Global Journal of Computer Science and Technology

discovering thoughts and inventing future

Volume 10 Issue 6 Version 1.0 Online ISSN: 0975-4172 Print ISSN: 0975-4350

15 Technology Reforming Ideas

highlights

- Synchronous Checkpointing Protocol
- Cloud Computing
- Security Log Management
- Coordinated Checkpointing Algorithm

July 2010

ENG

Global Journal of Computer Science and Technology

Global Journal of Computer Science and Technology

Volume 10 Issue 6 (Ver. 1.0)

Global Academy of Research and Development

License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027

Global Academy of Research and Development

Publisher's correspondence office

Global Journals, Headquarters Corporate Office, United States

Offset Typesetting

Global Journals, City Center Office, United States

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)

Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 500 USD (Color)

Editorial Board Members

Dr. Bart Lambrecht
Director of Research in Accounting and Finance Professor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology
Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training, New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management School Ph.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical Neurosciences
Northwestern University Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
New York-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo, School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, Taiwan University Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Chief Author

Dr. R.K. Dixit (HON.)
M.Sc., Ph.D., FICCT
Chief Author, India
Email: authorind@computerresearch.org

Dean & Editor-in-Chief (HON.)

Vivek Dubey(HON.)
MS (Industrial Engineering),
MS (Mechanical Engineering)
University of Wisconsin
FICCT
Editor-in-Chief, USA
editorusa@computerresearch.org

Er. Suyog Dixit
BE (HONS. in Computer Science), FICCT
SAP Certified Consultant
Technical Dean, India
Website: www.suyogdixit.com
Email:suyog@suyogdixit.com,
dean@computerresearch.org

Sangita Dixit
M.Sc., FICCT
Dean and Publisher, India
deanind@computerresearch.org

Contents of the Volume

From the Chief Author's Desk

We see a drastic momentum everywhere in all fields now a day. Which in turns, say a lot to everyone to excel with all possible way. The need of the hour is to pick the right key at the right time with all extras. Citing the computer versions, any automobile models, infrastructures, etc. It is not the result of any preplanning but the implementations of planning.

With these, we are constantly seeking to establish more formal links with researchers, scientists, engineers, specialists, technical experts, etc., associations, or other entities, particularly those who are active in the field of research, articles, research paper, etc. by inviting them to become affiliated with the Global Journals.

This Global Journal is like a banyan tree whose branches are many and each branch acts like a strong root itself.

Intentions are very clear to do best in all possible way with all care.

Dr. R. K. Dixit
Chief Author
chiefauthor@globaljournals.org

Security Provision for Miners Data Using Singular Value Decomposition in Privacy Preserving Data Mining

Narendar.Machha[1] M.Y.Babu[2]

GJCST Computing Classification
H.2.8, D.4.6, G.1.3, K.4.1

***Abstract*-Large repositories of data contain sensitive information that must be protected against unauthorized access. The protection of the confidentiality of this information has been a long-term goal for the database security research community and for the government statistical agencies. Recent advances in data mining and machine learning algorithms have increased the disclosure risks that one may encounter when releasing data to outside parties. It brings out a new branch of data mining, known as Privacy Preserving Data Mining (PPDM). Privacy-Preserving is a major concern in the application of data mining techniques to datasets containing personal, sensitive, or confidential information. Data distortion is a critical component to preserve privacy in security-related data mining applications; we propose a Singular Value Decomposition (SVD) method for data distortion. We focus primarily on privacy preserving data clustering. Our proposed method Singular Value Decomposition (SVD) distorts only confidential numerical attributes to meet privacy requirements.**

Keywords-Privacy-Preserving Data Mining, Matrix Decomposition, singular value decomposition, Nonnegative Matrix Factorization data distortion, data utility.

I. INTRODUCTION

Data mining technologies have now been used in commercial, industrial, and governmental businesses, for various purposes, ranging from increasing profitability to enhancing national security. The widespread applications of data mining technologies have raised concerns about trade secrecy of corporations and privacy of innocent people contained in the datasets collected and used for the data mining purpose. It is necessary that data mining technologies designed for knowledge discovery across corporations and for security purpose towards general population have sufficient privacy awareness to protect the corporate trade secrecy and individual private information. Unfortunately, most standard data mining algorithms are not very efficient in terms of privacy protection, as they were originally developed mainly for commercial applications, in which different organizations collect and own their private databases, and mine their private databases for specific commercial purposes. In the cases of inter-corporation and security data mining applications, data mining algorithms may be applied to datasets containing sensitive or private Information Data warehouses and government agencies may potentially have access to many databases collected from different sources and may extract any information from these databases. This potentially unlimited access to data and information raises the fear of possible abuse and promotes the call for privacy protection and due process of law. Privacy-preserving data mining techniques have been developed to address these concerns. The general goal of the privacy-preserving data mining techniques is defined as to hide sensitive individual data values from the outside world or from unauthorized persons, and simultaneously preserve the underlying data patterns and semantics so that a valid and efficient decision model based on the distorted data can be constructed. In the best scenarios, this new decision model should be equivalent to or even better than the model using the original data from the viewpoint of decision accuracy. There are currently at least two broad classes of approaches to achieving this goal. The first class of approaches attempts to distort the original data values so that the data miners (analysts) have no means (or greatly reduced ability) to derive the original values of the data. The second is to modify the data mining algorithms so that they allow data mining operations on distributed datasets without knowing the exact values of the data or without direct accessing the original datasets. This paper only discusses the first class of approaches. Interested readers may consult (Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., and Zhu, M., 2003) and the references therein for discussions on distributed data mining approaches.

II. BACKGROUND

The input to a data mining algorithm in many cases can be represented by a vector-space model, where a collection of records or objects is encoded as an n m × object-attribute matrix (Frankes, & Baeza-Yates, 1992). For example, the set of vocabulary (words or terms) in a dictionary can be the items forming the rows of the matrix, and the occurrence frequencies of all terms in a document are listed in a column of the matrix. A collection of documents thus forms a term-document matrix commonly used in information retrieval. In the context of privacy preserving data mining, each column of the data matrix can contain the attributes of a person, such as the person's name, income, social security number, address, telephone number, medical records, etc. Datasets of interest often lead to a very high dimensional matrix representation (Achlioptas, 2004). It is observable that many real-world datasets have nonnegative values for attributes. In fact, many of the existing data distortion

About-[1]Assistant Professor, HITS College Of Engineering. (e-mail:machha.narender@gmail.Com)
About-[2] Assistant Professor (e-mail;mannavababu@gmail.com) Aurora Engineering College

methods inevitably fall into the context of matrix computation. For instance, having the longest history in privacy protection area and by adding random noise to the data, additive noise method can be viewed as a random matrix and therefore its properties can be understood by studying the properties of random matrices (Kargupta, Sivakumar, & Ghosh, 2002; Mahta, 1991). Matrix decomposition in numerical linear algebra typically serves the purpose of finding a computationally convenient means to obtain a solution to a linear system. In the context of data mining, the main purpose of matrix decomposition is to obtain some form of simplified low-rank approximation to the original dataset for understanding the structure of the data, particularly the relationship within the objects and within the attributes and how the objects relate to the attributes (Hubert, Meulman, & Heiser, 2000). The study of matrix decomposition techniques in data mining, particularly in text mining, is not new, but the application of these techniques as data distortion methods in privacy-preserving data mining is a recent interest (Xu, Zhang, Han, & Wang, 2005). A unique characteristic of the matrix decomposition techniques, a compact representation with reduced-rank while preserving dominant data patterns, stimulates researchers' interest in utilizing them to achieve a win-win task both on high degree privacy preserving and high level data mining accuracy.

III. Main Focus

Data distortion is one of the most important parts in many privacy-preserving data mining tasks. The desired distortion methods must preserve data privacy, and at the same time, must keep the utility of the data after the distortion (Verykios, Bertino, Fovino, Provenza, Saygin, & Theodoridis, 2004). The classical data distortion methods are based on the random value perturbation (Agrawal, & Srikant, 2000). The more recent ones are based on the data matrix decomposition strategies (Wang, Zhong, & Zhang, 2006; Wang, Zhang, Zhong, & Xu, 2007; Xu, Zhang, Han, & Wang, 2006).

IV. Uniformly Distributed Noise

The original data matrix A is added with a uniformly distributed noise matrix E_u. Here E_u is of the same dimension as that of A, and its elements are random numbers generated from a continuous uniform distribution on the interval fromC1 to C2. The distorted data matrix A_u is denoted as: $A_u = A+E_u$.

V. Normally Distributed Noise

Similar to the previous method, here the original data matrix A is added with a normally distributed noise matrix E_n, which has the same dimension as that of A . The elements of E_n are random numbers generated from the normal distribution with a parameter mean μ and a standard deviation ρ. The distorted data matrix A_n is denoted as: $A_n = A+ E_n$.

VI. Singular Value Decomposition

Singular Value Decomposition (SVD) is a popular matrix factorization method in data mining and information retrieval. It has been used to reduce the dimensionality of, (and remove the noise in the noisy), datasets in practice (Berry, Drmac, & Jessup, 1999). The use of SVD technique in data distortion is proposed in (Xu, Zhang, Han, & Wang, 2005). In (Wang, Zhang, Zhong, & Xu, 2007), the SVD technique is used to distort portions of the datasets.

The SVD of the data matrix A is written as

$$A = U\Sigma V^T$$

where U is an nxn orthonormal matrix, $\Sigma = diag[\sigma_1, \sigma_2, \ldots. \sigma_s]$ (s= min{m, n}) is an n xm diagonal matrix whose nonnegative diagonal entries (the singular values) are in a descending order, and V^T is an mxm orthonormal matrix. The number of nonzero diagonal entries of Σ is equal to the rank of the matrix A.

Due to the arrangement of the singular values in the matrix Σ (in a descending order), the SVD transformation has the property that the maximum variation among the objects is captured in the first dimension, as $\sigma_1 \geq \sigma_i$ for i≥2. Similarly, much of the remaining variations is captured in the second dimension, and so on. Thus, a transformed matrix with a much lower dimension can be constructed to represent the structure of the original matrix faithfully. Define

$$A_k = U_k \Sigma_k V_k^T$$

Where Uk contains the first k columns of U, Σ_k contains the first k nonzero singular values, and V_k^T contains the first k rows of V^T. The rank of the matrix A_k is k. With k being usually small, the dimensionality of the dataset has been reduced dramatically from min{m, n} to k (assuming all attributes are linearly independent). It has been proved that A_k is the best k dimensional approximation of A in the sense of the Frobenius norm.

In data mining applications, the use of A_k to represent A has another important implication. The removed part $E_k = A - A_k$ can be considered as the noise in the original dataset (Xu, Zhang, Han, & Wang, 2006). Thus, in many situations, mining on the reduced dataset A_k may yield better results than mining on the original dataset A . When used for privacy-preserving purpose, the distorted dataset A_k can provide protection for data privacy, at the same time, it keeps the utility of the original data as it can faithfully represent the original data structure.

VII. Nonnegative Matrix Factorization

Given an nxm nonnegative matrix dataset A with Aij ≥ 0 and a prespecified positive integer k ≤min{n,m} , the nonnegative matrix factorization (NMF) finds two nonnegative matrices W Є Rnxk with Wij ≥ 0 and H Є

$$f(W, H) = \frac{1}{2}\|A-WH\|_F^2$$

Rkxm with Hij≥ 0, such that A ≈ WH and the objective function is minimized. Here is the Frobenius norm. The matrices W and H may have many other desirable properties in data mining applications. Several algorithms to compute nonnegative matrix factorizations for some applications of practical interests are proposed in (Lee, & Seung, 1999; Pascual-Montano, Carazo, Kochi, Lehmann, & Pascual-Marqui, 2006). Some of these algorithms are modified in (Wang, Zhong, & Zhang, 2006) to compute nonnegative matrix factorizations for enabling privacy-preserving in datasets for data mining applications. Similar to the sparsified SVD techniques, sparsification techniques can be used to drop small size entries from the computed matrix factors to further distort the data values (Wang, Zhong, & Zhang, 2006). In text mining, NMF has an advantage over SVD in the sense that if the data values are nonnegative in the original dataset, NMF maintains their nonnegative, but SVD does not. The nonnegative constraints can lead to a parts-based representation because they allow only additive, not subtractive, combinations of the original basis vectors (Lee, & Seung, 1999). Thus, dataset values from NMF have some meaningful interpretations in the original sense. On the contrary, data values from SVD are no longer guaranteed to be nonnegative. There has been no obvious meaning for the negative values in the SVD matrices. In the context of privacy preserving, on the other hand, the negative values in the dataset may actually be an advantage, as they further obscure the properties of the original datasets.

VIII. Utility Of The Distorted Data

Experimental results obtained in (Wang, Zhang, Zhong, & Xu, 2007; Wang, Zhong, & Zhang, 2006; Xu, Zhang, Han, & Wang, 2006; Xu, Zhang, Han, & Wang, 2005), using both synthetic and real-world datasets with a classification algorithm, show that both SVD and NMF techniques provide much higher degree of data distortion than the standard data distortion techniques based on adding uniformly distributed noise or normally distributed noise. In terms of the accuracy of the data mining algorithm, techniques based on adding uniformly distributed noise or normally distributed noise sometimes degrade the accuracy of the classification results, compared with applying the algorithm on the original, undistorted datasets. On the other hand, both SVD and NMF techniques can generate distorted datasets that are able to yield better classification results, compared with applying the algorithm directly on the original, undistorted datasets. This is amazing, as we intuitively expect that data mining algorithms applied on the distorted datasets may produce less accurate results, than applied on the original datasets. It is not clear why the distorted data from SVD and NMF are better for the data classification algorithm used to obtain the experimental results. The hypothesis is that both SVD and NMF may have some functionalities to remove the noise from the original datasets by removing small size matrix entries. Thus, the distorted datasets from SVD and NMF look like "cleaned" datasets. The distorted datasets from the techniques based on adding either uniformly distributed noise or normally distributed noise do not have this property. They actually generate "noisy" datasets in order to distort data values.

IX. Future trends

Using matrix decomposition-based techniques in data distortion for privacy-preserving data mining is a relatively new trend. This class of data privacy-preserving approaches has many desirable advantages over the more standard privacy-preserving data mining approaches. There are a lot of unanswered questions in this new research direction. For example, a classical problem in SVD-based dimensionality reduction techniques is to determine the optimal rank of the reduced dataset matrix. Although in the data distortion applications, the rank of the reduced matrix does not seem to sensitively affect the degree of the data distortion or the level of the accuracy of the data mining results (Wang, Zhang, Zhong, & Xu, 2007), it is still of both practical and theoretical interests to be able to choose a good rank size for the reduced data matrix. Unlike the data distortion techniques based on adding either uniformly distributed noise or normally distributed noise, SVD and NMF does not maintain some statistical properties of the original sestets, such as the mean of the data attributes. Such statistical properties may or may not be important in certain data mining applications. It would be desirable to design some matrix decomposition-based data distortion techniques that maintain these statistical properties. The SVD and NMF data distortion techniques have been used with the support vector machine based classification algorithms (Xu, Zhang, Han, & Wang, 2006). It is not clear if they are equally applicable to other data mining algorithms. It is certainly of interest for the research community to experiment these data distortion techniques with other data mining algorithms. There is also a need to develop certain techniques to quantify the level of data privacy preserved in the data distortion process. Although some measures for data distortion and data utility are defined in (Xu, Zhang, Han, & Wang, 2006), they are not directly related to the concept of privacy preserving in datasets.

X. Conclusion

We have presented two classes of matrix decomposition-based techniques for data distortion to achieve privacy-preserving in data mining applications. These techniques are based on matrix factorization techniques commonly practiced in matrix computation and numerical linear algebra. Although their application in text mining is not new, their application in data distortion with privacy-preserving data mining is a recent attempt. Previous experimental results have demonstrated that these data distortion techniques are highly effective for high accuracy privacy protection, in the sense that they can provide high degree of data distortion and maintain high level data utility with respect to the data mining algorithms. The computational methods for SVD and NMF are well developed in the matrix computation community. Very efficient software packages are available either in standard

matrix computation packages such as MATLAB or from several websites maintained by individual researchers. The availability of these software packages greatly accelerates the application of these and other matrix decomposition and factorization techniques in data mining and other application areas.

XI. References

1) Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining, Proceedings of the 2000
2) ACM SIGMOD International Conference on Management of Data, pp. 439-450, Dallas,TX.
3) Berry, M. W., Drmac, Z., & Jessup, E. R. (1999). Matrix, vector space, and information retrieval. SIAM Review, 41, 335-362.
4) Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., and Zhu, M. (2003). Tools for privacy preserving distributed data mining. ACM SIGKDD Explorations, 4(2), 1-7.
5) Gao, J., & Zhang, J. (2003). Sparsification strategies in latent semantic indexing. Proceedings of the 2003 Text Mining Workshop, pp. 93-103, San Francisco, CA.
6) Hubert, L., Meulman, J., & Heiser, W. (2000). Two purposes for matrix factorization: a historical appraisal. SIAM Review, 42(4), 68-82.
7) Kargupta, H., Sivakumar, K., & Ghosh, S. (2002). Dependency detection in mobimine and
8) random matrices. Proceedings of the 6th European Conference on Principles and Practice of Knowledge Discovery in Databases, pp. 250-262, Helsinki, Finland.
9) Lee, D. D., & Seung, H. S. (1999). Learning in parts of objects by non-negative matrix factorization. Nature, 401, 788-791.
10) Mahta, M. L. (1991). Random Matrices. 2nd edition. Academic, London.
11) Analysis and Machine Intelligence, 28, 403-415. Verykios, V.S., Bertino, E., Fovino, I. N., Provenza, L. P., Saygin, Y., & Theodoridis, Y. (2004).State-of-the-art in privacy preserving data mining. ACM SIGMOD Record, 3(1), 50-57.
12) Wang, J., Zhong, W. J., & Zhang, J. (2006). NNMF-based factorization techniques for highaccuracy privacy protection on non-negative-valued datasets. Proceedings of the IEEE Conference on Data Mining 2006, International Workshop on Privacy Aspects of Date Mining (PADM 2006), pp. 513-517, Hong Kong, China.
13) Xu, S., Zhang, J., Han, D., & Wang, J. (2006). Singular value decomposition based data distortion strategy for privacy protection. Knowledge and Information Systems, 10(3), 383-397.

An Efficient Synchronous Checkpointing Protocol for Mobile Distributed Systems

Parveen Kumar[1] Rachit Garg[2]

GJCST Computing Classification
C.2.2, C.2.1

***Abstract*-Recent years have witnessed rapid development of mobile communications and become part of everyday life for most people. In order to transparently adding fault tolerance in mobile distributed systems, Minimum-process coordinated checkpointing is preferable but it may require blocking of processes, extra synchronization messages or taking some useless checkpoints. All-process checkpointing may lead to exceedingly high checkpointing overhead. In order to balance the checkpointing overhead and the loss of computation on recovery, we propose a hybrid checkpointing algorithm, wherein an all-process coordinated checkpoint is taken after the execution of minimum-process coordinated checkpointing algorithm for a fixed number of times. In the minimum-process coordinated checkpointing algorithm; an effort has been made to optimize the number of useless checkpoints and blocking of processes using probabilistic approach and by computing an interacting set of processes at beginning. We try to reduce the loss of checkpointing effort when any process fails to take its checkpoint in coordination with others. We reduce the size of checkpoint sequence number piggybacked on each computation message**

I. Background

Recent years have witnessed rapid development of mobile communications and become part of everyday life for most people. In the future, we will expect more and more people will use some portable units such as notebooks or personal data assistants. With increasing use small portable computers, wireless networks and satellites, a trend to support "Computing of the move" has emerged. This trend is known as mobile computing or "anytime" or "anywhere" computing. This enables the user to access and exchange information while they travel, roam in their home environments, or work at their desktop computers. Mobile Hosts (MHs) are increasingly becoming common in distributed systems due to their availability, cost, and mobile connectivity. An MH is a computer that may retain its connectivity with the rest of the distributed system through a wireless network while on move. An MH communicates with the other nodes of the distributed system via a special node called mobile support station (MSS). A "cell" is a geographical area around an MSS in which it can support an MH. An MSS has both wired and wireless links and it acts as an interface between the static network and a part of the Mobile network. Static nodes are connected by a high speed wired network [1].

A checkpoint is a local state of a process saved on the stable storage. In a distributed system, since the processes in the system do not share memory, a global state of the system is defined as a set of local states, one from each process. The state of channels corresponding to a global state is the set of messages sent but not yet received. A global state is said to be "consistent" if it contains no orphan message; i.e., a message whose receive event is recorded, but its send event is lost [5]. To recover from a failure, the system restarts its execution from the previous consistent global state saved on the stable storage during fault-free execution. This saves all the computation done up to the last checkpointed state and only the computation done thereafter needs to be redone.

In independent checkpointing, processes do not synchronize their checkpointing activity and processes are allowed to records their local checkpoints in an independent way. After a failure, system will search a consistent global state by tracking the dependencies from the stable storage. The main advantage of this approach is that there is no need to exchange any control messages during checkpointing. But this requires each process to keep several checkpoints in stable storage and there is no certainty that a global consistent state can be built. It may require cascaded rollbacks that may lead to the initial state due to domino effect [6]. Acharya and Badrinath[1] were the first who present a uncoordinated checkpointing algorithm for mobile computing systems. In their algorithm, an MH takes a local checkpoint whenever a message reception is preceded by a message sent at that MH. If the send and receive of messages are interleaved, the number of local checkpoints will be equal to half of the number of computation messages, which may degrade the system performance.

In coordinated or synchronous checkpointing, processes take checkpoints in such a manner that the resulting global state is consistent. Mostly it follows the two-phase commit structure [2], [5], [6], [7], [10], [15]. In the first phase, processes take tentative checkpoints, and in the second phase, these are made permanent. The main advantage is that only one permanent checkpoint and at most one tentative checkpoint is required to be stored. In the case of a fault, processes rollback to the last checkpointed state [6]. The Chandy-Lamport [5] algorithm is the earliest non-blocking all-process coordinated checkpointing algorithm.

The existence of mobile nodes in a distributed system introduces new issues that need proper handling while designing a checkpointing algorithm for such systems [1], [4], [14], [16]. These issues are mobility, disconnections,

About-[1]Meerut Institute of Engineering & Technology, Meerut, India, Pin-125005(e-mail;pk223475@yahoo.com)
About-[2] Singhania University Pacheri Bari (Rajasthan) (e-mail:rachit.garg@yahoo.com)

finite power source, vulnerable to physical damage, lack of stable storage etc. Prakash and Singhal [14] proposed a nonblocking minimum-process coordinated checkpointing protocol for mobile distributed systems. They proposed that a good checkpointing protocol for mobile distributed systems should have low overheads on MHs and wireless channels; and it should avoid awakening of an MH in doze mode operation. The disconnection of an MH should not lead to infinite wait state. The algorithm should be non-intrusive and it should force minimum number of processes to take their local checkpoints. In minimum-process coordinated checkpointing algorithms, some blocking of the processes takes place [3], [10], [11], or some useless checkpoints are taken [4], [15].

In minimum-process coordinated checkpointing algorithms, a process Pi takes its checkpoint only if it a member of the minimum set (a subset of interacting process). A process Pi is in the minimum set only if the checkpoint initiator process is transitively dependent upon it. Pj is directly dependent upon Pk only if there exists m such that Pj receives m from Pk in the current checkpointing interval [CI] and Pk has not taken its permanent checkpoint after sending m. The ith CI of a process denotes all the computation performed between its ith and (i+1)th checkpoint, including the ith checkpoint but not the (i+1)th checkpoint.

The koo-Toueg[10] proposed a minimum process coordinated checkpointing algorithm for distributed systems with the cost of blocking of processes during checkpointing. However, this algorithm requires minimum number of synchronization message and number of checkpoints but each process uses monotonically increasing labels in its outgoing messages. The initiator process sends the checkpoint request to Pi only if it has received m from Pi in the current CI. Similarly, Pi sends the checkpoint request to other processes. In this way, a checkpointing tree is formed and at last the leaf node processes take checkpoints. The time taken to collect coordinated checkpoint in mobile systems may be too large due to mobility, disconnections and unreliable wireless channels. The extensive blocking of processes may degrade the system performance. Cao and Singhal [4] achieved non-intrusiveness in the minimum-process algorithm by introducing the concept of mutable checkpoints. Kumar and Kumar [21] proposed a minimum-process coordinated checkpointing algorithm for mobile distributed systems, where the number of useless checkpoints and the blocking of processes are reduced using a probabilistic approach. Singh and Cabillic [20] proposed a minimum-process non-intrusive coordinated checkpointing protocol for deterministic mobile systems, where anti-messages of selective messages are logged during checkpointing. Higaki and Takizawa [8], and Kumar et al [17] proposed hybrid checkpointing protocols where MHs checkpoint independently and MSSs checkpoint synchronously. Neves et al. [13] gave a time based loosely synchronized coordinated checkpointing protocol that removes the overhead of synchronization and piggybacks integer csn (checkpoint sequence number). Pradhan et al [19] had shown that asynchronous checkpointing with message logging is quite effective for checkpointing mobile systems.

Most of the proposed checkpointing algorithms do not addressing the multiple concurrent initiations in their algorithms, as it may exhaust the limited battery and congest the wireless channels. The authors claim in that their algorithm supports concurrent initiations [4]. But in[15] authors proves that the algorithm in[4] is designed to only handle the situation where the system has only one checkpoint initiator at a time and can cause inconsistency when there are multiple forced checkpoints or multiple concurrent checkpoint initiations. In[22], the author point out following problems in allowing concurrent initiations in minimum-process checkpointing protocols, particularly in case of mobile distributed systems:

i) If Pi and Pj concurrently initiate checkpointing and Pj belongs to the minimum set of Pi, then Pj's initiation will be redundant one. Some processes, in Pj's minimum set, will unnecessarily take multiple checkpoints by hardly advancing their recovery line. In other words, an MH may be asked to store multiple checkpoints in its local disk. It may also transfer multiple checkpoints to its local MSS.

ii) Sometimes, multiple triggers need to be piggybacked onto normal messages. Trigger contains the initiator process identification and its csn. Even if a process takes a checkpoint and no concurrent initiation is going on, it will piggyback its trigger, unnecessarily. If we do not allow concurrent initiation, no trigger is required to be piggybacked onto normal messages. Hence, concurrent initiations increase message size.

Authors [23] have proposed a minimum process coordinated checkpointing algorithm for mobile distributed system, where no useless checkpoints are taken and an effort is made to minimize the blocking of processes. . They captured the transitive dependencies during the normal execution. The Z-dependencies are well taken care of in this protocol. They also avoided collecting dependency vectors of all processes to compute the minimum set.

In this paper [24], authors propose a nonblocking coordinated checkpointing algorithm for mobile computing systems, which requires only a minimum number of processes to take permanent checkpoints. They reduce the message complexity as compared to the Cao-Singhal algorithm [4], while keeping the number of useless checkpoints unchanged.

II. Introduction

The system model is similar to [3], [4]. A mobile computing system consists of a large number of MH's and relatively fewer MSS's. The distributed computation we consider consists of n spatially separated sequential processes denoted by P0, P1, ..., Pn-1, running on fail-stop MH's or on MSS's. Each MH or MSS has one process running on it. The processes do no share common memory or common clock. Message passing is the only way for processes to communicate with each other. Each process progresses at its

own speed and messages are exchanged through reliable channels, whose transmission delays are finite but arbitrary. We assume the processes to be non-deterministic.

Similar to [3], [21], [22] initiator process collects the dependency vectors of all processes and computes the tentative minimum set. Suppose, during the execution of the checkpointing algorithm, Pi takes its checkpoint and sends m to Pj. Pj receives m such that it has not taken its checkpoint for the current initiation and it does not know whether it will get the checkpoint request. If Pj takes its checkpoint after processing m, m will become orphan. In order to avoid such orphan messages, we use the following technique as mentioned in [21].

If Pj has sent at least one message to a process, say Pk, and Pk is in the tentative minimum set, there is a good probability that Pj will get the checkpoint request. Therefore, Pj takes its mutable checkpoint before processing m [4]. In this case, most probably, Pj will get the checkpoint request and its mutable checkpoint will be converted into permanent one. Alternatively, this message is buffered Pj. Pj will process m only after taking its tentative checkpoint or after getting commit as in [22].

In minimum-process checkpointing, some processes may not be included in the minimum set for several checkpoint initiations due to typical dependency pattern; and they may starve for checkpointing. In the case of a recovery after a fault, the loss of computation at such processes may be unreasonably high [22]. In Mobile Systems, the checkpointing overhead is quite high in all-process checkpointing [14]. Thus, to balance the checkpointing overhead and the loss of computation on recovery, we design a hybrid checkpointing algorithm for mobile distributed systems, where an all-process checkpoint is taken after certain number of minimum-process checkpoints.

In coordinated checkpointing, if a single process fails to take its checkpoint; all the checkpointing effort goes waste, because, each process has to abort its tentative checkpoint. In order to take the tentative checkpoint, an MH needs to transfer large checkpoint data to its local MSS over wireless channels. Hence, the loss of checkpointing effort may be exceedingly high. Therefore, we propose that in the first phase, all concerned MHs will take soft checkpoint only. Soft checkpoint is similar to mutable checkpoint [4], which is stored on the memory of MH only. In this case, if some process fails to take checkpoint in the first phase, then MHs need to abort their soft checkpoints only. The effort of taking a soft checkpoint is negligible as compared to the tentative one. When the initiator comes to know that all relevant processes have taken their soft checkpoints, it asks all relevant processes to come into the second phase, in which, a process converts its soft checkpoint into tentative one. Finally, the initiator issues the commit request.

In the present study, we present a hybrid scheme, where an all process checkpoint is enforced after executing minimum-process algorithm for a fixed number of times as in [22]. In the first phase, the MHs in the minimum set are required to take soft checkpoint only. In the minimum-process algorithm, a process takes its forced checkpoint only if it is having a good probability of getting the checkpoint request as in [21].

III. The Proposed Checkpointing Scheme

A. An Example

We explain the minimum-process checkpointing algorithm with the help of an example. In Figure 1, at time t1, P1 initiates checkpointing process and sends request to all processes for their dependency vectors. At time t2, P1 receives the dependency vectors from all processes and computes the tentative minimum (mset) set as in [21], which in case of Figure 1 is {P0, P1, P2}]. P1 sends this tentative minimum set to all processes. A process takes its soft checkpoint if it is a member of the tentative minimum set. When P0 and P2 get the mset, they find themselves in the mset; therefore, they take their soft checkpoints. When P3, P4 and P5 get the mset, they find that they are not its members ; therefore, they do not take their checkpoints.

P1 sends m8 after taking its checkpoint and P0 receives m8 before getting the mset. In this case, P0 buffers m8 and processes it only after taking its soft checkpoint. After taking its soft checkpoint, P1 sends m11 to P3. At the time of receiving m11, P4 has received the mset and it has not taken its checkpoint, therefore, P4 takes bitwise logical AND of sendv4 and mset and finds that the resultant vector is not all zeroes [sendv3[1]=1 due to m3; mset[2]=1]. P3 concludes that most probably, it will get the checkpoint request in the current initiation; therefore, it takes its mutable checkpoint before processing m11. When P2 takes its soft checkpoint, it finds that it is dependent upon P3 and P3 is not in the minimum set [known locally]; therefore, P2 sends checkpoint request to P3. On receiving the checkpoint request, P3 converts its mutable checkpoint into soft one.

After taking its checkpoint, P2 sends m13 to P4. P4 takes the bitwise logical AND of sendv4 and mset and finds the resultant vector to be all zeroes (sendv4=[000001]; mset=[111000]). P4 concludes that most probably, it will not get the checkpoint request in the current initiation; therefore, P4 does not take mutable checkpoint but buffers m13. P4 processes m13 only after getting commit request. P5 processes m14, because, it has not sent any message since last permanent checkpoint. After taking its checkpoint, P1 sends m12 to P2. P2 processes m12, because, it has already taken its checkpoint in the current initiation. At time t3, P1 receives responses from all relevant processes and issues tentative checkpoint request along with the exact minimum set [P0, P1, P2, P3] to all processes. On receiving tentative checkpoint request, all relevant processes convert their soft checkpoints into tentative ones and inform the initiator. Finally, at time t4, initiator P2 issues commit. On receiving commit following actions are taken. A process, in the minimum set, converts its tentative checkpoint into permanent one and discards its earlier permanent checkpoint, if any. A process, not in the minimum set, discards its mutable checkpoint, if any, or processes the buffered messages, if any.

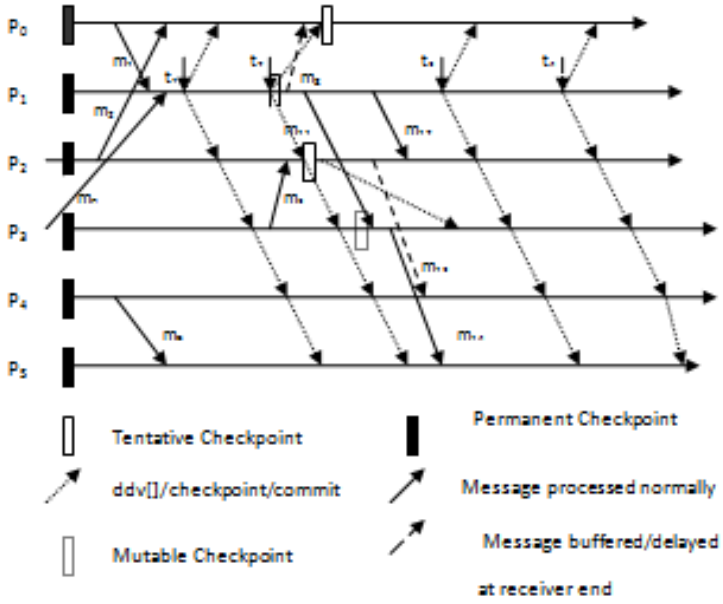


Figure 1 An Example of the proposed Protocol

B. *Handling Node Mobility and Disconnections*

Suppose, an MH, say MHi, disconnects from an MSS, say MSSk, it stores its own checkpoint, say disconnect_ckpti, and other support information, e.g. ddv, at MSSk. During disconnection period, MSSk acts on behalf of MHi as follows. If checkpointing process is initiated and MHi is in cell of MSSj, it is connected to the MSSj, if g_chkpt is reset. Otherwise, it waits for the g_chkpt to be reset. Before connection, MSSj collects its ddv, buffered messages from MSSk; and MSSk discards MHi's support information and disconnect_ckpti. The buffered messages are processed by MHi, in the order of their receipt at the MSSk. MHi's ddv is updated on the processing of buffered messages.

Comparison with existing non-blocking algorithm In Cao-Singhal algorithm [20], suppose, Pi receives m from Pj before taking its checkpoint and Pi is in the minimum set. In this case, after taking its checkpoint, Pi sends checkpoint request to Pj due to m. If Pj has taken some permanent checkpoint request after sending m, the checkpoint request to Pj is useless. To enable P_j to decide whether the checkpoint request is useful, P_i also piggybacks $csn_i[j]$ and a huge data structure MR along with the checkpoint request to P_j. These useless checkpoint requests and piggybacked data structures increase the message complexity of the algorithm. Whereas, in our algorithm, no such useless checkpoint requests are sent and no such information is piggybacked onto checkpoint requests. The $csn_i[j]$ is integer; its size is 4 bytes. In worst case the size of MR is (4n +n/8) bytes (n is the number of processes in the distributed system). Intuitively, we can say that the number of useless checkpoints in the proposed algorithm will be negligibly small as compared to the algorithm [20].

the minimum set, MSSk converts its disconnected checkpoint into permanent one. On global checkpoint commit, MSSk also updates MHi's ddv, as if, it is a normal process. On the receipt of messages for MHi, MSSk stores them in a queue without updating ddv. When MHi, enters in the.

The proposed protocol suffers from the following limitations with respect to the existing algorithm [20]. Initiator MSS collects dependencies of all processes, computes the tentative minimum set, and broadcasts the tentative minimum set along with the checkpoint request to all MSS's. Initiator MSS broadcasts exact minimum set along with the commit request on the static network. Blocking of processes also takes place. Concurrent executions of the algorithm are avoided.

IV. Conclusions

We propose a hybrid checkpointing algorithm, wherein an all-process coordinated checkpoint is taken after the execution of minimum-process coordinated checkpointing algorithm for a fixed number of times. In minimum-process checkpointing, we try to reduce number of useless checkpoints and blocking of processes. We have proposed a probabilistic approach to reduce the number of useless checkpoints. Thus, the proposed protocol is simultaneously able to reduce the useless checkpoints and blocking of processes at very less cost of maintaining and collecting dependencies and piggybacking checkpoint sequence numbers onto normal messages. Concurrent initiations of the proposed protocol do not cause its concurrent executions. We try to reduce the loss of checkpointing effort when any process fails to take its checkpoint in coordination with others.

V. References

1) Acharya A. and Badrinath B. R., "Checkpointing Distributed Applications on Mobile Computers," Proceedings of the 3rd International Conference on Parallel and Distributed Information Systems, pp. 73-80, September 1994.
2) Cao G. and Singhal M., "On coordinated checkpointing in Distributed Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 9, no.12, pp. 1213-1225, Dec 1998.
3) Cao G. and Singhal M., "On the Impossibility of Min-process Non-blocking Checkpointing and an Efficient Checkpointing Algorithm for Mobile Computing Systems," Proceedings of International Conference on Parallel Processing, pp. 37-44, August 1998.
4) Cao G. and Singhal M., "Mutable Checkpoints: A New Checkpointing Approach for Mobile Computing systems," IEEE Transaction On Parallel and Distributed Systems, vol. 12, no. 2, pp. 157-172, February 2001.
5) Chandy K. M. and Lamport L., "Distributed Snapshots: Determining Global State of Distributed Systems," ACM Transaction on Computing Systems, vol. 3, No. 1, pp. 63-75, February 1985.
6) Elnozahy E.N., Alvisi L., Wang Y.M. and Johnson D.B., "A Survey of Rollback-Recovery Protocols in Message-Passing Systems," ACM Computing Surveys, vol. 34, no. 3, pp. 375-408, 2002.
7) Elnozahy E.N., Johnson D.B. and Zwaenepoel W., "The Performance of Consistent Checkpointing," Proceedings of the 11th Symposium on Reliable Distributed Systems, pp. 39-47, October 1992.
8) Higaki H. and Takizawa M., "Checkpoint-recovery Protocol for Reliable Mobile Systems," Trans. of Information processing Japan, vol. 40, no.1, pp. 236-244, Jan. 1999.
9) J.L. Kim, T. Park, "An efficient Protocol for checkpointing Recovery in Distributed Systems," IEEE Trans. Parallel and Distributed Systems, pp. 955-960, Aug. 1993.
10) Koo R. and Toueg S., "Checkpointing and Roll-Back Recovery for Distributed Systems," IEEE Trans. on Software Engineering, vol. 13, no. 1, pp. 23-31, January 1987.
11) Parveen Kumar, R K Chauhan, "A Coordinated Checkpointing Protocol for Mobile Computing Systems", International Journal of Information and Computing Science, Vol. 9, No. 1, pp. 18-27, 2006.
12) Lalit Kumar, M. Misra, R.C. Joshi, "Low overhead optimal checkpointing for mobile distributed systems" Proceedings. 19th International Conference on IEEE Data Engineering, pp 686 – 88, 2003.
13) Neves N. and Fuchs W. K., "Adaptive Recovery for Mobile Environments," Communications of the ACM, vol. 40, no. 1, pp. 68-74, January 1997.
14) Prakash R. and Singhal M., "Low-Cost Checkpointing and Failure Recovery in Mobile Computing Systems," IEEE Transaction On Parallel and Distributed Systems, vol. 7, no. 10, pp. 1035-1048, October1996.
15) Weigang Ni, Susan V. Vrbsky and Sibabrata Ray, " Pitfalls in nonblocking checkpointing" World Science's journal of Interconnected Networks. Vol. 1 No. 5, pp. 47-78, March 2004.
16) Parveen Kumar, Lalit Kumar, R K Chauhan, "A low overhead Non-intrusive Hybrid Synchronous checkpointing protocol for mobile systems", Journal of Multidisciplinary Engineering Technologies, Vol.1, No. 1, pp 40-50, 2005.
17) Lalit Kumar, Parveen Kumar, R K chauhan "Logging based Coordinated Checkpointing in Mobile Distributed Computing Systems", IETE journal of research, vol. 51, no. 6, 2005.
18) Lamports L., "Time, clocks and ordering of events in distributed systems" Comm. ACM, 21(7), 1978, pp 558-565.
19) Pradhan D.K., Krishana P.P. and Vaidya N.H., "Recovery in Mobile Wireless Environment: Design and Trade-off Analysis," Proceedings 26th International Symposium on Fault-Tolerant Computing, pp. 16-25, 1996.
20) Pushpendra Singh, Gilbert Cabillic, "A Checkpointing Algorithm for Mobile Computing Environment", LNCS, No. 2775, pp 65-74, 2003.
21) Lalit Kumar Awasthi, P.Kumar, "A Synchronous Checkpointing Protocol for Mobile Distributed Systems: Probabilistic Approach" International Journal of Information and Computer Security, Vol.1, No.3 pp 298-314, 2007.
22) Parveen Kumar, "A Low-Cost Hybrid Coordinated Checkpointing Protocol for Mobile Distributed Systems", Mobile Information Systems pp 13-32, Vol. 4, No. 1, 2007.
23) [23] Kumar, P., & Khunteta, A. A Minimum-Process Coordinated Checkpointing Protocol For Mobile Distributed System. International Journal of Computer Science issues, Vol. 7, Issue 3, 2010.
24) [24] Garg, R., & Kumar, P.(2010). A Nonblocking Coordinated Checkpointing Algorithm for Mobile Computing Systems. International Journal of Computer Science issues, Vol. 7, Issue 3, 2010.

A Fuzzy Co-Clustering approach for Clickstream Data Pattern

GJCST Computing Classification
I.5.1, I.5.3, J.1, H.2.8

R.Rathipriya[1] Dr. K.Thangavel[2]

***Abstract*-Web Usage mining is a very important tool to extract the hidden business intelligence data from large databases. The extracted information provides the organizations with the ability to produce results more effectively to improve their businesses and increasing of sales. Co-clustering is a powerful bipartition technique which identifies group of users associated to group of web pages. These associations are quantified to reveal the users' interest in the different web pages' clusters. In this paper, Fuzzy Co-Clustering algorithm is proposed for clickstream data to identify the subset of users of similar navigational behavior /interest over a subset of web pages of a website. Targeting the users group for various promotional activities is an important aspect of marketing practices. Experiments are conducted on real dataset to prove the efficiency of proposed algorithm. The results and findings of this algorithm could be used to enhance the marketing strategy for directing marketing, advertisements for web based businesses and so on.**

Keywords-Web usage mining, Fuzzy Co-Clustering, Target marketing, Clickstream data

I. INTRODUCTION

Nowdays, internet is a very fast communication media between business organizations' services and their customers with very low cost. Web Data mining [1] is an intelligent data mining technique to analyze web data. It includes web content data, web structure data and web usage data. Analysis of usage data provides the organizations with the required information to improve their performances. In general, Web clustering techniques are used to discover the group of users or group of pages called clusters which are similar between them and dissimilar to the users /pages in the other cluster. User clustering approaches of usage data create groups with similar browsing pattern. Web page's content data, structure data and usage data are used to cluster the web pages of a web site. Clustering results may be beneficial for wide range of application such as web site personalization, system improvement, web caching and pre-fetching, recommendation system, design of collaborative filtering and target marketing. These clustering techniques are one dimensional where as Co-Clustering is the bi-dimensional clustering technique. The combination of user cluster with set of its significant web pages of a web site is called a Co-Cluster.

There are many applications for Co-clustering[7] such as recommendations systems, direct marketing, text mining identifying the web communities and election analysis [1][2]. Co-Clustering techniques can be used in, collaborative filtering to identify subgroups of customers with similar preferences or behaviors towards a subset of products with the goal of performing target marketing. Recommendation systems and Marketing are important applications in E-commerce area. The main goal for the above applications is to identify group of web users or customers with similar behavior/ interest so that one can predict the customer's interest and make proper recommendations to improve their sale Generally, Co-clustering is a form of two-way clustering in which both dimensions are clustered simultaneously Target and generated Co-Clusters are refined using some techniques like fuzzy approach. The goal of this paper is to provide fuzzy Co-Clustering algorithm for clickstream data to quantify the discovered Co-Clusters .Users' clusters with their members are related in a different degree with pages' clusters. The relation between these clusters is quantified using fuzzy membership function to show the distribution of users' interest over the web page clusters.

The organization of the paper is as follows. Section 2 summarizes some of the existing web clustering techniques and co-clustering approaches. Section 3 describes the problem statements. The proposed Fuzzy Co-clustering algorithm is described briefly in Section 4. The experimental results of the proposed algorithm are discussed in the Section 5. Section 6 concludes this paper.

II. BACKGROUND

A. *Related work*

Web mining was first proposed by Etzioni in 1996.Web mining techniques automatically discover and extract information from World Wide Web documents and services. Cooley et al.[1,6] did in-depth research in web usage mining. Approaches proposed in [3,10] extend the one dimensional clustering problem and focus on the simultaneous grouping of both users and web pages by exploiting their relations. Its goal is to identify groups of related web users and pages, which has similar interest across the same subset of pages. This behavior reveals users' interests as similar and highly related to the topic that the specific set of pages involves. The obtained results are particularly useful for applications such as e-commerce and recommendation engines, since relations between clients and products may be revealed. These relations are more meaningful than the one dimensional clustering of users or pages.

Co-Clustering algorithms fall into three categories. First category models each type of object as a random variable, clustering the objects of different types simultaneously while preserving the mutual information between the

About-[1]Department of Computer Science, Periyar University, Salem,Tamilnadu,India.
(e-mail;[1]rathi_priyar@yahoo.co.in ,[2]drktvelu@yahoo.com)

random variables that model these objects. The second category models the relationship between different types of objects as a (nonnegative) matrix. This matrix is *approximately* decomposed into several matrices, which indicate the cluster memberships for the objects . The third category treats the relationship between different types of objects as a graph and performs co-clustering by graph partitioning based on spectral analysis [2].Fuzzy biclustering approach to correlate the web users and web pages based on spectral clustering technique was proposed in[2].

B. Co-Clustering Approach

By definition Co-Clustering[9] is the process of simultaneous categorization of user and web pages into user cluster and page cluster respectively. The term co-cluster refers to each pair of user cluster and page cluster. Using the matrix illustration, a co-cluster is represented by a sub-matrix of A where the aij values of all its elements are similar to one another. Thus co-clustering is the task of finding these coherent sub-matrices of A. One illustration of co-clustering is shown in the following matrix. The six square matrices represent the six co-clusters (i.e. A11 to A32).

$$A = \begin{pmatrix} 5 & 5 & 5 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 5 & 7 \\ 0 & 0 & 0 & 1 & 5 & 7 \\ 4 & 4 & 0 & 4 & 4 & 4 \\ 4 & 4 & 0 & 4 & 4 & 4 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \\ A_{31} & A_{32} \end{pmatrix}$$

This paper aims to provide a framework for the simultaneous clustering of web pages and users called Fuzzy Co-Clustering. The relations between web users and pages in a co-cluster will be identified and quantified. Here, users grouped in the same users' cluster may be related to more than one web pages' cluster with different degree of fuzzy membership value and vice versa.

III. PROBLEM STATEMENT

This section gives the formal definitions of the problem and describes how the clickstream data from web server log file converted into matrix form.

Let A(U , P) be an 'n x m' user associated matrix where U={U1,U2 ,……,Un} be a set of users and P={ P1,P2,……,Pm} be a set of pages of a web site. It is used to describe the relationship between web pages and users who access these web pages. Let 'n' be the number of web user and 'm' be the number of web pages. The element aij of A(U,P) represents frequency of the user Ui of U visit the page Pj of P during a given period of time

$$a_{ij} = \begin{cases} \text{Hits}(U_i, P_j) & \text{, if } P_j \text{ is visited by } U_i \\ 0 & \text{, otherwise} \end{cases} \quad (1)$$

where Hits(Ui ,Pj) is the count/frequency of the user Ui accesses the page Pj during a given period of time.

A **user cluster** is a group of users that have similar behavior when navigating through a web site during a given period of time. A **page cluster** is a group of web pages that are related according to user's perception, specifically they are accessed by similar users during a given period of time. Similarity measure used in this paper is **Fuzzy similarity**. Fuzzy similarity measure between two fuzzy subsets $X_1=\{x_{11},x_{12} ,…….,x_{1n}\}$ and $X_2=\{x_{21},xu_{22} ,…….,x_{2n}\}$ is defined as

$$\text{fsim}(X_1, X_2) = \frac{\sum_{k=1}^{m} X_{1k} \wedge X_{2k}}{\sum_{k=1}^{m} X_{1k} \vee X_{2k}} \quad (2)$$

This ratio defines the similarity between two fuzzy subsets, with values between 0 and 1. Using this similarity measure, compute similarity matrix for user vector and page vector of user associated matrix A.

Fuzzy co-clustering is a technique that performs simultaneous clustering of objects and features using fuzzy membership function to correlate their relations. It allows user clusters to belong to several page clusters simultaneously with different degree of membership value. The membership value lies between 0 and 1.

A. Clustering algorithm : K-Means

In this paper, K-Means clustering technique[12] is used to create user cluster and page cluster. K-means is one of the simplest unsupervised learning algorithms for clustering problem. The procedure is simple and easy way to classify a given data set through a certain fixed number of clusters (assume K clusters).

The algorithm is composed of the following steps:

Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.

Assign each object to the group that has the closest centroid.

When all objects have been assigned, recalculate the positions of the K centroids.

Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.

The K-Means algorithm is significantly sensitive to the initial randomly selected cluster centers. Run K-Means algorithm repeatedly with different random cluster centers(called centriods)approximately for ten times. Choose the best centriod whose Davis Bouldin Index value is minimum.

B. Web Server Log File

Web server log file[3,5] is a log file automatically created and maintained by server of activity performed by it. Default log file format is Common log File format. It contains information about the request, client IP address, request date/time, page requested, HTTP code, bytes served, user agent, and referrer. These data can be combined into a single file, or separated into distinct logs, such as an access log, error log, or referrer log. From web server log file, which user access which web page of a web site during a specified period of time can be obtained easily.

C. Clickstream Data

Clickstream data[4] is a natural by-product of a user accessing world wide web pages, and refers to the sequence of pages visited and the time these pages were viewed. Clickstream data is to Internet marketers and advertisers. An instance of real clickstream records is the MSNBC dataset, which describes the page visits of users who visited msnbc.com on a single day. There are 989,818 users and only 17 distinct items, because these items are recorded at the level of URL category, not at
page level, which greatly reduces the dimensionality. The 17 categories are tabulated with their category number.

Frontpage	1	News	2
Tech	3	Local	4
Opinion	5	On-air	6
Misc	7	Weather	8
Health	9	Living	10
Business	11	Sports	12
Summary	13	Bbs	14
Travel	15	msn-news	16
msn-sports	17		

Sample Sequences

1 1
2
3 2 2 4 2 2 2 3 3
6 7 7 7 6 6 8 8 8 8
6 9 4 4 4 10 3 10 5 10 4 4 4

Each row describes the hits of a single user. For example, the first user hits "frontpage" twice, and the second user hits "news" once.

D. User fuzzy subset

For each user U_i , use the user accessing information on each web page P_j to describe the visiting pattern. Then user fuzzy subset μ_{Ui} of i^{th} user that reflects the user's visiting behavior is defined as

$$\mu_{U_i} = \left\{ \left(P_j, f\mu_{U_i}(P_j) \right) \mid P_j \grave{o} P \right\}$$

where $f\mu_{Ui}(P_j)$ is the membership function which is defined as

$$f\mu_{U_i}(P_j) = \frac{\text{Hits}(U_i, P_j)}{\sum_{k=1}^{m} \text{Hits}(U_i, P_k)} \quad (3)$$

and m is the number of web pages of a web site.

E. Page Fuzzy subset

For each page Pj , use the all user accessing information on the web page Pj to describe the web page itself. Then page fuzzy subset μPj that reflects all users' visiting behavior on the jth page is defined as

$$\mu_{P_j} = \left\{ \left(U_i, f\mu_{P_j}(U_i) \right) \mid U_i \grave{o} U \right\}$$

where $f\mu_{Pj}(U_i)$ is the membership function which is defined as

$$f\mu_{Pj}(U_i) = \frac{\text{Hits}(U_i, P_j)}{\sum_{k=1}^{n} \text{Hits}(U_k, P_j)} \quad (4)$$

and n is the number of web users.

IV. FUZZY CO-CLUSTERING ALGORITHM FOR CLICKSTREAM DATA

In this paper, K-Means clustering method is applied on the user(row) and page(column) dimensions of the user access matrix A(U,P) separately and, then combine the results to obtain small co-regulated submatrices called Co-Clusters. Given a user access matrix A, let ku be the number of clusters on user dimension and kp be the number of clusters on page dimension after K-Means clustering is applied. Cu is the family of user clusters and Cp is the family of page clusters. Let ciu be a subset of users and ciu ϵ Cu (1≤ i≥ ku). Let cjp be a subset of pages and cjp ϵ Cp (1≤ j≥ kp). The pair (ciu,cjp) denotes a Co-Cluster of A . By combining the results of user dimensional clustering and page dimensional clustering, ku × kp Co-clusters are obtained. The objective of the paper is to quantify these Co-clusters in different degree using fuzzy membership function. The proposed Fuzzy Co-Clustering algorithm has three phases

A. First Phase: User Clustering

1. Compute user fuzzy subset of the user associated $A(U,P)_{nxm}$ using equation 3.
2. Compute user similarity matrix of size 'n x n' using fuzzy similarity measure as defined in equation2.
3. Apply K-Means to user similarity matrix and generate k_u user groups.

B. Second Phase: Page Clustering

1. Compute page fuzzy subset of the user associated $A(U,P)_{nxm}$ using equation 4.
2. Compute page fuzzy similarity matrix of size 'm x m' using equation2.
3. Apply K-Means to page similarity matrix and generate k_p page groups.

C. Third Phase: Fuzzy Relation Coefficients

1. Combining the results of user dimensional clustering and page dimensional clustering, to obtain $k_u \times k_p$ Co-clusters .
2. Calculate relation coefficients between user cluster and page cluster of each Co-Cluster using equation5 that indicates the distribution of related users' interest over the page clusters.
3. Calculate relation coefficients between user cluster and page cluster of each Co-Cluster using equation6 that shows which user cluster has more interest in that page cluster.

After performing one dimensional clustering on user fuzzy subset and page fuzzy subset, k_u user clusters and k_p page clusters are related and quantified user clusters' interest in the different degree to different page clusters. It reveals the group of related users' interest in the different group of related web pages. The fuzzy relation co-efficient between user cluster and web page cluster is defined in two ways as

$$f\left(c_i^u, c_j^p\right) = \frac{\sum_{ui \in c_i^u} \sum_{pj \in c_j^p} \text{Hits}\left(u_i, p_j\right)}{\sum_{k=1..n} \sum_{pj \in c_j^p} \text{Hits}\left(u_i, p_k\right)} \quad (5)$$

$$f\left(c_i^u, c_j^p\right) = \frac{\sum_{ui \in c_i^u} \sum_{pj \in c_j^p} \text{Hits}\left(u_i, p_j\right)}{\sum_{k=1..m} \sum_{ui \in c_i^u} \text{Hits}\left(u_k, p_j\right)} \quad (6)$$

Equation5 quantifies the each user clusters' interest for different related web page clusters. Equation 6 quantifies the different users' clusters interest for each web page clusters. The interpretation of the fuzzy co-clustering result can be used to improve direct and target marketing strategy and also used to improve the quality of recommendation systems.

V. Experimentation and Results

Inorder to evaluate performance of the proposed algorithm, experiment is conducted on the benchmark clickstream dataset of MSNBC.com which describes the sequence of page visits of users on 28 September 1999.

A. Data Preprocessing

Data preprocessing[8] transforms the data into a format that will be more easily and effectively processed for the purpose of the user. The techniques to preprocess data include data cleaning, data integration, data transformation and data reduction. Clickstream records in the MSNBC dataset is converted into matrix format where elements aij of A(U,P) represents the frequency of the user Ui accesses the web page Pj of a web site during a given period of time. During the user session, the user visited web page categories are marked with the frequency of that page accessed and otherwise 0.

B. Data filtering

Data filtering is the task of extracting only those records of weblog files, which are essential for the analysis, thus reducing significantly data necessary for further processing. In this paper, data filtering aims to filter out the users who have visited less than 9 page categories of web site. Initially there are 989818 users, after this step number of users are reduced to 1720 users.

C. Results

K-Means algorithm is applied to the resultant user associated matrix of size 1720 X 17 where k_u=10 and k_p= 3 was fixed to create ten user clusters and three page clusters. Using equation 4 and equation 5, the relations between user clusters and page clusters were quantified as shown in Fuzzy Relation Coefficient Matrix 1and Matrix 2

VI. Fuzzy Relation Co-efficient

Table 1 shows which user and page clusters are more related and it indicate the way of users' clusters interest distribution over all pages' clusters. From the Table1, User Cluster $\mathbf{c_2^u}$ has more interest in the page cluster $\mathbf{c_3^p}$ because that Co-Cluster 's fuzzy relation value is high. Similarly, interested pages for each user cluster can be found easily and efficiently

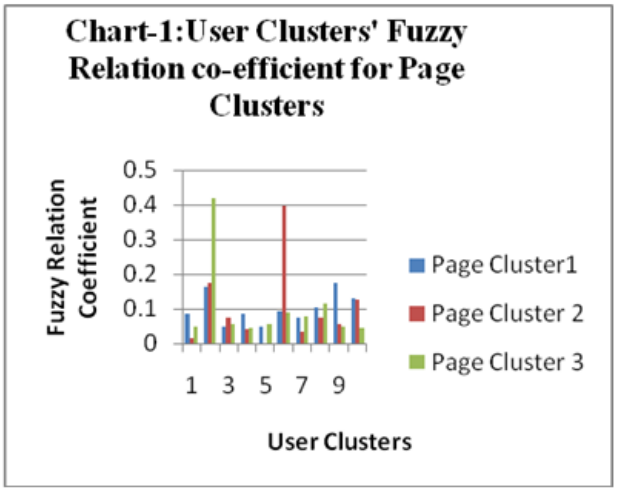


Table 2 shows Co-Cluster's fuzzy relation value by relating user and page clusters. It clearly pictures out which user cluster has more interest for a page cluster. By this way it is

easy to identify target related user group for each page cluster and which is useful for target marketing to make recommendations according to their frequent access of web pages during a given period of time.

Clusters	c_1^p	c_2^p	c_3^p
c_1^u	0.0839	0.0162	0.0489
c_2^u	0.1615	0.1739	0.4192
c_3^u	0.0466	0.0763	0.0574
c_4	0.0847	0.0423	0.0456
c_5^u	0.0485	0.0019	0.0549
c_6^u	0.0921	0.3978	0.0877
c_7^u	0.0739	0.0346	0.0792
c_8^u	0.1049	0.0752	0.1165
c_9^u	0.1734	0.0562	0.0475
c_{10}^u	0.1305	0.1256	0.0431

Table 1 : Users' Cluster Fuzzy Relation Coefficient for Page Clusters

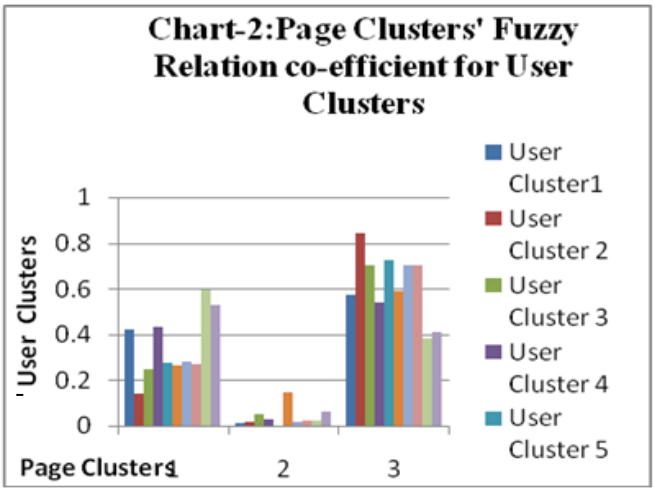


Table 2 shows Co-Cluster's fuzzy relation value by relating user and page clusters. It clearly pictures out which user cluster has more interest for a page cluster. By this way it is easy to identify target related user group for each page cluster and which is useful for target marketing to make recommendations according to their frequent access of web pages during a given period of time.

Interpretation of Co-Cluster result with fuzzy relation value is very helpful to realize how and with which patterns the web site page categories are visited more by the which user cluster. Such information's are useful to the web administrators for web site evaluation or reorganization. Recommend set of related web page category for users group based on the fuzzy relation value also possible.

Clusters	c_1^u	c_2^u	c_3^u	c_4^u	c_5^u	c_6^u	c_7^u	c_8^u	c_9^u
c_1^p	0.4192	0.1389	0.2445	0.4309	0.274	0.2652	0.2805	0.2712	0.595
c_2^p	0.0103	0.0189	0.0507	0.0273	0.0014	0.1451	0.0167	0.0246	0.0244
c_3^p	0.5705	0.8422	0.7048	0.5419	0.7246	0.5898	0.7028	0.7041	0.3806

VII. Conclusion

This paper proposed Fuzzy Co-Clustering algorithm for Cliskstream data and evaluated it with real dataset. The results proved its efficiency in correlating the relevant users and web pages of a web site. Thus, interpretation of Co-cluster results are used by the company for focalized marketing campaigns to an interesting target user cluster. This is a key feature in target marketing. Our Fuzzy Co-Clustering algorithm produces non-overlapping co-clusters. In future it is extended to generate overlapping clusters.

VIII. References

1) Cooley.R ,Srivastava.J, Deshpande.M, , "Data preparation for mining world wide web browsing patterns", Knowledge and Information Systems ,Vol 1,No.1,pp.5–32,1999.
2) Koutsonikola, V.A. and Vakali, A. ,"A fuzzy bi-clustering approach to correlate web users and
3) pages", Int. J. Knowledge and Web Intelligence, Vol. 1, No. 1/2, pp.3–23, 2009.
4) Liu, X., He, P. and Yang, Q. 'Mining user access patterns based on Web logs', Canadian Conference on Electrical and Computer Engineering, May, Saskatoon Inn Saskatoon,Saskatchewan Canada, pp.2280–2283, 2005.
5) Panagiotis Antonellis, Christos Makris, Nikos Tsirakis,"Algorithms for Clustering ClickStream Data", Information Processing Letters, Vol- 109, Issue 8, pp. 381-385,2009
6) Qinbao Song , Martin Shepperd ," Mining web browsing patterns for E-commerce", Computers in Industry 57,pp. 622–630,2006.
7) Srivastava.J, Cooley.R, Deshpande.M, and P.-N. Tan, "Web usage mining: Discovery and applications of usage patterns from web data," SIGKDD Explorations, Vol. 1, No. 2, pp. 12-23, 2000.
8) Stanislav Busygina, Oleg Prokopyevb, and Panos M. Pardalos," Biclustering in data mining", Computers & Operations Research 35 ,pp.2964 – 2987,2008.
9) Suneetha K.R, Dr. R. Krishnamoorthi,"Data Preprocessing and Easy Access Retrieval of Data through Data Ware House ",Proceedings of the

World Congress on Engineering and Computer Science 2009, USA, Vol. 1,2009.

10) Tjhi.W.C and L. Chen ," Minimum sum-squared residue for fuzzy co-clustering" Intelligent Data Analysis 9 pp.1–13,2006.
11) Zeng, H-J., Chen, Z. and Ma, Y-M. "A unified framework for clustering heterogeneous web objects", Proceedings of the 3rd International Conference on Web Information Systems Engineering, December, Singapore, pp.161–172, 2002.

A Survey on Topology for Bluetooth Based Personal Area Networks

Prof. Anuradha.V[1] Dr. Sivaprakasam. P[2]

GJCST Computing Classification
C.2.1

***Abstract*-Bluetooth is a proficient technology for short range wireless communication and networking, fundamentally used as a alternate for connected cables. Bluetooth is a Wireless Personal Area Network (WPAN) technology, which enables devices to connect and communicate by means of short-range ad-hoc networks. Topology formation remains to be challenging problem in most of the Bluetooth based Wireless Personal Area Networks (BT-WPANs). The problem of topology creation in WPANs can be divided I nto two sub problems: the election of the nodes that have to act as master, and the assignment of the slaves to the piconets. Topology creation is the procedure of defining the piconets, and the interconnection of the nodes organized in the network area. Traffic load distribution and energy consumption by the nodes are the two major factors that are affected by improper topology design. Many researchers have been conceded on topology study for Bluetooth WPANs. These researches decide to develop an efficient topology for BT-WPANs that may consume less energy for communication between the master and the slave. This paper presents a survey on various network topology distribution techniques for Bluetooth based WPANs. Additionally, as a part of future research, this paper also discusses some of the limitations of the available topologies and the probable solutions to overcome the limitations**

Keywords- Bluetooth, Bridges, Topology, Wireless Personal Area Network (WPAN), Nodes, Master, Slave, Piconets, Scatternets, Slots, Frequency Hopping

I. Introduction

In recent years, wireless ad-hoc networks have acquired significant importance. Correspondingly, a great deal of attention is offered towards short range radio systems that are operated using Bluetooth technology [1], [2] and IEEE 802.15[3]Wireless Personal Area Networks (WPAN). Piconets form the fundamental architectural unit in WPANs. Bluetooth is a Wireless Personal Area Network (WPAN) technology, which enables devices to connect and communicate via short-range ad-hoc networks [4]. Bluetooth WPANs (BT-WPANs) are characteristically used to twist stand-alone devices located in the range of about 10 m into networked equipment. In general, a piconet comprises of a master device and a maximum of seven slave devices. The slave devices are limited in operation as they are permitted to communicate only with their master device. Additionally, a piconet can have unlimited number of nodes, provided that they remain inactive. In other words, the excess nodes will not participate in piconet transmissions.

A different frequency hopping sequence may be utilized by each piconet. This frequency hopping sequence is normally derived from the master address. Because of the exercise of different hopping sequences, a bridge cannot be active in more than one piconet at a time; thus, bridges have to switch between piconets on a time division basis, and, while switching, they must re-synchronize with the current piconet. An intended full duplex connection can be established between the master and the slave by sending and receiving the traffic alternatively. A master or a slave involved in the activity of more than one piconet can act as a bridge allowing piconets to form a larger network, a so-called scatternet. A slave is allowed to start transmission in a given slot, if the master has addressed it in the preceding slot. In Bluetooth technology, frequency hopping or time division duplex (FH/TDD) is used for time division into 625- μsec intervals, termed as slots. The master uses intra-piconet scheduling algorithms to schedule the traffic within a piconet. Inter-piconet scheduling algorithms are used to schedule the existence of the bridges in diverse piconets [8]. Abundant intra and inter-piconet scheduling algorithms have been proposed [5] [6] [7].

Network topology creation remains to be a most important aspect in WPANs. Topology creation is the process of defining the piconets, and the interconnection of the nodes deployed in the network area. Certainly, topology design has an essential impact on the traffic load distribution within the WPAN, and on the nodes energy consumption. One of the most demanding problems in deploying a BT-WPAN consists in forming a scatternet that meets the constraints posed by the system specifications and the traffic requirements. This paper presents a survey on various network topology distribution techniques for Bluetooth based WPANs. Additionally, as a part of future research, this paper also discusses some of the limitations of the available topologies and the probable solutions to overcome the limitations.

The remainder of this paper is organized as follows. Section II of this paper provides an insight view on different topologies for Bluetooth based wireless personal area networks that were proposed earlier in literature. Section III gives directions for future research. Section IV concludes the paper with fewer discussions.

II. Literature Review

Numerous researches have been carried on topology study for Bluetooth WPANs. These researches determine to develop an efficient topology for BT-WPANs that may consume less energy for communication between the master and the slave. This section of the paper provides a close study on different topologies for Bluetooth based wireless personal area networks that were proposed earlier in literature.

An effective topology for Bluetooth scatternet was proposed by Huang et al. in [9]. Bluetooth is a capable technology for

short-range wireless communication and networking, essentially used as a replacement for connected cables. Since the Bluetooth specification only defines how to build piconet, several solutions have been proposed to construct a scatternet from the piconets in the literatures. A tree shaped scatternet is called the bluetree. In their paper, they proposed an approach to generate the bluetree hierarchically; namely, the nodes are added into the bluetree level by level. This kind of Hierarchical Grown Bluetree (HGB) topology resolves the defects of the conventional bluetree. During growing up, HGB always remains balanced so as to maintain shorter routing paths. Besides, the links between siblings provide alternative paths for routing. As a result, the traffic load at parent nodes can be significantly improved and only two separate parts will be induced if a parent node is lost. The Bluetooth network therefore achieves better reliability.

L. Huang et al. in [10] described the impact of topology on multi-hop Bluetooth personal area network. Their paper concentrates on the impact of topology on Bluetooth personal area network. They initially described some observations on performance degradations of Bluetooth PAN due to network topologies, and then analyzed its reason. Based on their analysis, they described a lithe scatternet formation algorithm under conference scenario for multi-hop communication. By using proposed method, scatternet can be formed flexibly with different topologies under a controlled way. In order to utilize topology information in multi-hop communication, they proposed new link metric Load Metric (LM) information in multi-hop communication; they proposed a new link metric Load Metric (LM) instead of number of hops. LM is derived from estimation of nodes link bandwidth, which reflects different roles of nodes in Bluetooth scatternet. Furthermore, their proposal helped routing protocol to bypass heavily loaded nodes, and find route with larger bandwidth. They presented some experimental results based on implementation, which proved the effectiveness of their protocols.

Hsu et al. in [11] put forth a method of topology formation with the assistance of ns. Bluetooth is a promising technology in wireless applications, and many associated issues are however to be explored both in academia and industry. Because of the complexity and the dynamics of computer networks, a good simulation tool plays an imperative role in the development stage. Of the existing simulation tools, ns is an accepted, open-source package that has a considerable support for simulation of TCP, routing, and multicast protocols over wired and wireless networks. It also has BlueHoc as its extension for Bluetooth. Although BlueHoc offers many simulation functions for Bluetooth, all simulations must be done in a practically fixed topology. Hence simulation about dynamic topology construction-the first and an important step in establishing a Bluetooth network-cannot be conducted. Besides, BlueHoc offers only a restricted support for building a network. It also lacks flexibility in device control, in animated presentation, and in modeling mobility. The main contribution of their paper is therefore to enhance BlueHoc to support the aforementioned functions.

Optimal topology for Bluetooth was projected by Melodia et al. in [12]. As we all know, Bluetooth is a hopeful technology for personal/local area wireless communications. A Bluetooth scatternet is composed of overlapping piconets, each with a low number of devices sharing the same radio channel. Their paper discusses the scatternet formation problem by analyzing topological characteristics of the scatternet formed. A matrix-based representation of the network topology is used to define metrics that are applied to estimate the key cost parameters and the scatternet performance. Numerical examples are presented and discussed, highlighting the impact of metric selection on scatternet performance. Then, a distributed algorithm for scatternet topology optimization is introduced, that supports the formation of a locally optimal scatternet based on a selected metric. Numerical results obtained by adopting this distributed approach to optimize the network topology are shown to be close to the global optimum.

Lin et al. in [13] proposed the formation of a new BlueRing scatternet topology for Bluetooth WPANs. It is recommendable to have uncomplicated yet competent scatternet topologies with good supports of routing protocols, considering that Bluetooth are to be used for personal area networks with design goals of simplicity and compactness. In the literature, even though many routing protocols have been proposed for mobile ad hoc networks, directly applying them poses a difficulty due to Bluetooth's special base band and MAC-layer features. In their work, they proposed an attractive scatternet topology called BlueRing, which connects piconets as a ring interleaved by bridges between piconets, and address its formation, routing, and topology-maintenance protocols. The BlueRing architecture enjoys the following fine features. First, routing on BlueRing is stateless in the sense that no routing information needs to be kept by any host once the ring is formed. This would be favorable for environments such as Smart Homes where computing capability is limited. Second, the architecture is scalable to median-size scatternets easily (e.g. around 50 ~ 70 Bluetooth units). In comparison, most star- or treelike scatternet topologies can easily form a communication bottleneck at the root of the tree as the network enlarges. Third, maintaining a BlueRing is a trouble-free task as some Bluetooth units join or leave the network. To endure single-point failure, they proposed a protocol-level solution mechanism. To tolerate multipoint failure, they proposed a recovery mechanism to reconnect the BlueRing. Graceful failure is tolerable as long as no two or more critical points fail at the same time. In addition, they also evaluated the ideal network throughput at different BlueRing sizes and configurations by mathematical analysis. Simulation results are presented, which demonstrated that BlueRing outperforms other scatternet structures with higher network throughput and moderate packet delay.

A feasible topology formation algorithm for Bluetooth based WPANs was presented by Carla et al. in [14]. In their paper, they begin with the problem of topology formation in

Bluetooth Wireless Personal Area Networks (BT-WPANs). They initially overviewed and extended a previously proposed centralized optimization approach, and discussed its results. Then they outlined the main steps of two procedures that can lead to feasible distributed algorithms for the incremental construction of the topology of a BT-WPAN. The centralized optimization approach has the advantage of producing topologies that reduce the traffic load of the most congested node in the network while meeting the limitations on the BT-WPAN structure and capacity. On the other hand, the centralized nature and the high complexity of the optimization are a strong limitation of the proposed approach. Distributed algorithms for the topology formation of BT-WPANs are much more attractive, provided their algorithmic complexity and energy cost are sufficiently low to allow implementation in large BT-WPANs. Moreover, they discussed the distributed procedures for the insertion and the removal of a node in/from a BT-WPAN, which are easily implementable and able to cooperate between the system efficiency and its ability to rapidly recover from topology changes. These procedures are the key building blocks for a distributed solution approach to the BT-WPAN topology formation problem.

Roy et al. in [15] proposed a new topology construction technique for Bluetooth WPANs. They proposed a Bluetooth topology construction protocol that works in combination with a priority-based polling scheme. A master assigns a priority to its slaves including bridges for each polling cycle and then polls them as many times as the assigned priority. The slaves can splurge their idle time either in a power-saving mode or execute new node discovery. The topology construction algorithm works in a bottom-up manner in which isolated nodes join to form small piconets. These small piconets can come together to form larger piconets. Larger piconets can establish sharing bridge nodes to form a scatternet. Individual piconets can also discover new nodes while participating in the master-driven polling process. The shutting down of master and slave nodes is detected for dynamic restructuring of the scatternet. The protocol can handle situations when all the Bluetooth nodes are not within radio range of each other.

Scatternet formation of Bluetooth wireless networks was projected by Zhen et al. in [16]. In their paper, a protocol stack of Bluetooth group ad hoc network and a "blue-star island" network formation algorithm are proposed. The network formation locates within Bluetooth Network Encapsulation Protocol (BNEP) layer and is underneath the routing protocol. The most important task of network formation is to establish and maintain Bluetooth network topology with better performance and in a fast and economic way. The routing protocol is generally to find the best routes among the existing network topology. The network formation communicates with routing protocol and management entity using "Routing Trigger" mechanism. The "blue-star island" algorithm is a distributed 2-stages scheme. First, a group of neighbor nodes are self-organized into "blue-star Island," where the joint node is slave in scatternet. Then, initiated by "Routing Trigger" from routing protocol, blue-star islands are bridged together. The "Routing trigger" can be "Route REQuest" message or "HELLO" message. The design has no assumption on number, distribution and mobility of nodes. In addition, they presented discussion and simulation results that showed the proposed algorithm has lower formation latency, maintained consume and generated an efficient and good quality of topology for forwarding packet.

A self-routing topology for Bluetooth WPANs was put forth by Sun et al. in [17]. The emerging Bluetooth standard is considered to be the most promising technology to construct ad-hoc networks. It contains specifications on how to build a piconet but left out the details on how to automatically construct a scatternet from the piconets. Existing solutions only discussed the scatternet formation concern without considering the ease of routing in such a scatternet. They presented algorithms to embed b-trees into a scatternet which enables such a network to become self-routing. It requires only fix-sized message header and no routing table at each node regardless of the size of the scatternet. These properties made their solution scalable to deal with networks of large sizes. Their solutions are of distributed control and asynchronous. They also proved that their algorithm preserves the b-tree property when devices join or leave the scatternet and when one scatternet is merged into another.

Salonidis et al. in [18] proposed a distributed topology formation technique for Bluetooth personal area networks. In their paper they introduced and analyzed a randomized symmetric protocol that yields link establishment delay with predictable statistical properties. They then proposed the Bluetooth Topology Construction Protocol (BTCP), an asynchronous distributed protocol that extends the point-to-point symmetric mechanism to the case of several nodes. BTCP is based on a distributed leader election process where closeness information is discovered in a progressive way and ultimately accumulated to an elected coordinator node. BTCP consists on three important phases. They are Coordinator election, role determination, connection establishment and leader election termination. Bluetooth link establishment is a two-step process that involves the Inquiry and Paging procedures. Leader election is an important tool for breaking symmetry in a distributed system. They have implemented BTCP on top of an existing prototype implementation that emulates the Bluetooth environment on a Linux platform.

A distributed Bluetooth scatternet formation method was presented by Chang et al. in [19]. They devised a distributed Bluetooth scatternet formation algorithm using the parking property. This parking mechanism allows the master to manage more than seven slaves in its piconet. When a master slave pair is formed, the slave is immediately parked such that the master will not be restricted by already having seven active slaves. This method is effortless and valuable and is well-matched with current Bluetooth specification. As we all know that straight line is the shortest way to connect to points in space, they named their algorithm Blueline to indicate that the communicating path between two Bluetooth nodes is shorter compared to other scatternets. Their proposed scatternet formation algorithm will allow two

Bluetooth nodes to form a connection and communicate directly if they are within each other's transmission range. The important purpose is to form a topology with the minimum number of hops for routes. One thing not described in the above algorithm is the switching policy of a bridge in the scatternet. In order to evaluate the performance of Blueline, they have developed a Bluetooth extension to the VINT project network simulator.

Metin et al. in [20] discussed the construction of energy efficient Bluetooth scatternets. Bluetooth networks can be constructed as piconets or scatternets depending on the number of nodes in the network. Though piconet construction is a distinct process specified in Bluetooth standards, scatternet formation policies and algorithms are not well specified. Among many solution proposals for this problem, only a few of them focus on efficient usage of bandwidth in the resulting scatternets. In their paper, they proposed a distributed algorithm for the scatternet formation problem that dynamically constructs and maintains a scatternet based on estimated traffic flow rates between nodes. The algorithm is adaptive to changes and maintains a constructed scatternet for bandwidth-efficiency when nodes come and go or when traffic flow rates change. Based on simulations, the paper also presented the improvements in bandwidth-efficiency and reduction in energy consumption provided by the proposed algorithm.

An algorithm for connected topologies in Bluetooth WPANs was described by Guerin et al. in [21]. They first described the fundamental characteristics of the Bluetooth technology that are appropriate to topology formation. They formulated a mathematical model for the system objectives and constraints, as an initial step towards a systematic investigation of the connectivity issue. They mainly focused on designing a topology where a node's degree does not exceed 7. They presented a topology design procedure based on an approximation algorithm guaranteed to generate a spanning tree with degree at most one more than the minimum possible value in any arbitrary graph. The Minimum weighted spanning tree algorithm does not give any analytical guarantee on the degrees of the nodes in the 3-dimensional case. Therefore they utilized MST algorithm to form connected topologies for Bluetooth networks.

Marsan et al. in [22] projected an approach for optimal topology design in WPANs. In their paper, they deal with the master election and the assignment of the slaves to the piconets, while they do not address the election of the bridge nodes. They defined an intention function to be optimized in the course of the network topology design, which represents the above requirements on traffic load distribution and energy consumption at the network nodes. Then, they devised topology design algorithms for WPAN systems, that both maximize the objective function, and satisfy the constraints on the maximum number of active slaves allowed per piconet and on the maximum transmission range of the radio devices. They initially assumed that a centralized procedure can be performed, and they found the optimal set of masters as well as the optimal assignment of slaves to piconets. Then, by maintaining the set of masters identified via the centralized algorithm, they developed a distributed assignment scheme, which well approximates the performance of the centralized solution. Tabu search algorithms can be seen as an evolution of the classical local optimum solution search called Steepest Descent (SD). The approach they proposed to find the optimal network topology in a centralized manner completely relies on the use of the tabu search (TS) methodology. Numerical results showed that the distributed algorithm closely approximates the performance of the centralized solution for almost any number of nodes in the network area.

In order to optimize the topology in Bluetooth PANs Marsan et al. proposed a method in [23]. Their optimization approach is based on a model resultant from constrictions that are unambiguous to the BT-WPAN technology, but the level of abstraction of the model is such that it can be related to the more general field of ad hoc networking. By using a min-max formulation, they determined the optimal topology that provides full network connectivity, fulfills the traffic requirements and the constraints posed by the system specification, and minimizes the traffic load of the most congested node in the network, or equivalently its energy consumption. Results showed that a topology optimized for some traffic requirements is also remarkably robust to changes in the traffic pattern. Due to the problem complexity, the optimal solution is attained in a centralized manner. Although this implies severe limitations, a centralized solution can be applied whenever a network coordinator is elected, and provides a useful term of comparison for any distributed heuristics.

III. Future Enhancement

In recent years, wireless ad hoc networks have been a growing area of research. While there has been considerable research on the topic of routing in such networks, the topic of topology creation has received due attention. Bluetooth is a promising new wireless technology, which enables portable devices to form short-range wireless ad hoc networks and is based on a frequency

hopping physical layer. However, the network topology construction at present requires that devices are pairwise in range of each other. The issue of determining an optimal topology specifically for BT-WPANs is discussed in [18] but is not actually addressed there. The first attempt at finding a solution to the problem is represented by the work in [24]. Further research is needed to conquer this strong requirement while maintaining an easy construction process. In addition, it would be interesting to perform simulation studies in order to estimate the parameters of real schedules that yield a good tradeoff between achievable throughput, average path length and medium access delay caused by the scheduling. The mobility support of the algorithm is not discussed in [19]. Therefore, the future work may take steps to make the algorithm to support mobility by turning the neighbors discover time to infinity. The future study may determine to find a mathematical framework for Bluetooth scatternets, in order to allow the design of efficient scatternet topologies

IV. Conclusion

Wireless networks are implemented in a variety of real time applications. Bluetooth is a capable technology in wireless applications, and many associated issues are however to be explored both in academia and industry. Therefore, the Bluetooth technology that is used to interface the devices within a short range is widely used in recent years. The communication between the connected devices takes place by means of a network, which has to be assigned a topology. Topology determination for a Bluetooth based WPANs are a serious problem in most of the applications. Topology creation resides on election of a master and assignment of the slaves to that particular elected master. A lot of techniques and methods have been proposed earlier in literature for topology formation in Bluetooth wireless personal area networks. This paper presents a survey on various network topology distribution techniques for Bluetooth based WPANs. The future work mainly focuses on developing an approach for topology creation that accounts for minimum energy consumption between the master and slave node. The development of an approach also considers the traffic load between the nodes

V. References

1) Haartsen, "The Bluetooth radio system," IEEE Personal Communications Magazine, pp. 28–36, February 2000.
2) "The Bluetooth core specification," 2001, http://www.bluetooth.com.
3) "IEEE 802.15 Working Group," 2001, http://www.ieee802.org/15/pub/TG2.html.
4) Bluetooth Special Interest Group, "Specification of the Bluetooth System – Version 2.0," Nov. 2004.
5) Baatz, M. Frank, C. Kuhl, P. Martini, and C. Scholz, "Bluetooth Scatternet: An Enhanced Adaptive Scheduling Scheme," in Proceedings of IEEE INFOCOM'02, pp. 782-790, 2002.
6) A .Capone, M. Gerla, and R. Kapoor, "An Efficient Polling Schemes for Bluetooth Picocells," in Proceedings of IEEE ICC'01, vol. 7, pp. 1990-1994, 2001.
7) Har-Shai, R. Kofman, A. Segall, and G. Zussman, "Load Adaptive Inter-piconet Scheduling in Small-scale Bluetooth Scatternets," IEEE Communications Magazine, vol. 42, pp. 136–142, July 2004.
8) Gil Zussman, Adrian Segall and Uri Yechiali, "On the Analysis of the Bluetooth Time Division Duplex Mechanism," IEEE Transactions on Wireless Communications, vol. 6, no. 6, pp. 2149-2161, 2007.
9) Tsung-Chuan Huang, Chu-Sing Yang, Chao-Chieh Huang and Sheng-Wen Bai, "Hierarchical Grown Bluetrees (HGB): an effective topology for Bluetooth scatternets," International Journal of Computational Science and Engineering, vol. 2, no. 2, pp. 23-31, 2006.
10) Leping Huang, Hongyuan Chen, V. L. N. Sivakumar, Tsuyoshi Kashima and Kaoru Sezaki, "Impact of Topology on Multi-hop Bluetooth Personal Area Network," Book Chapter, Springer link, pp. 131-138, 2004.
11) Chia-Jui Hsu and Yuh-Jzer Joung, "An ns-based Bluetooth Topology Construction Simulation Environment," Proceedings of the 36th annual symposium on Simulation, p. 145, 2003.
12) Tommaso Melodia and Francesca Cuomo, "Locally Optimal Scatternet Topologies for Bluetooth Ad Hoc Networks," Book Chapter on Wireless On-Demand Network Systems, Springer link, pp. 19-24, 2004.
13) Ting-Yu Lin, Yu-Chee Tseng and Keng-Ming Chang, "A new BlueRing scatternet topology for Bluetooth with its formation, routing, and maintenance protocols," Research in Ad Hoc Networking, Smart Sensing and Pervasive Computing, vol. 3, no. 4, pp. 517-537, 2003.
14) Carla F. Chiasserini, Marco Ajmone Marsan, Elena Baralis and Paolo Garza, "Towards Feasible Topology Formation Algorithms for Bluetooth-based WPANs," 36th Annual Hawaii International Conference on System Sciences (HICSS'03), vol. 9, p. 313, 2003.
15) Rajarshi Roy, Mukesh Kumar, Navin K. Sharma and Shamik Sural, "Bottom-Up Construction of Bluetooth Topology under a Traffic-Aware Scheduling Scheme," IEEE Transactions on Mobile Computing, vol. 6, no. 1, pp. 72-86, January, 2007.
16) Bin Zhen, Jonghun Park, and Yongsuk Kim, "Scatternet Formation of Bluetooth Ad Hoc Networks," 36th Annual Hawaii International Conference on System Sciences (HICSS'03), vol. 9, p. 312, 2003.
17) Min-Te Sun, Chung-Kuo Chang and Ten-Hwang Lai, "A Self-Routing Topology for Bluetooth Scatternets," International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN '02), p. 17, 2002.
18) Theodoros Salonidis and Leandros Tassiulas, "Distributed Topology Construction of Bluetooth Wireless Personal Area Networks," In Proceedings of IEEE INFOCOM, 2001.
19) Ruay-Shiung Chang and Ming-Te Chou, "Blueline: A Distributed Bluetooth Scatternet Formation and Routing Algorithm," Journal of Information Science and Engineering, vol. 21, pp. 479-494, 2005.
20) Metin Tekkalmaz, Hasan Sozer and Ibrahim Korpeoglu, "Distributed Construction and Maintenance of Bandwidth and Energy Efficient Bluetooth Scatternets," IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 9, pp. 963-974, 2006.
21) Guerin, J. Rank, S. Sarkar and E. Vergetis, "Forming Connected Topologies in Bluetooth Ad-

hoc Networks - An Algorithmic Perspective," 2003.

22) Ajmone Marsan, C. F. Chiasserini, and A. Nucci, "Optimal Topology Design in Wireless Personal AreaNetworks," www.cercom.polito.it/Publication/Pdf/114.pdf.
23) Marco Ajmone Marsan, Carla F. Chiasserini, Antonio Nucci, Giuliana Carello, and Luigi De Giovanni, "Optimizing the Topology of Bluetooth Wireless Personal Area Networks," 2005.
24) O. Miklos, A. Racz, Z. Turanyi, A.Valko, and P. Johansson, "Performance Aspects of Bluetooth Scatternet Formation," First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHoc), pp. 147–148, August 2000.

Identification of Most Desirable Parameters in SIGN Language Tools: A Comparative Study

Yousef Al-Ohali

GJCST Computing Classification
H.5.2, H.5.1, I.6.5

***Abstract*-Symbolic languages have gained popularity to undertake communication within community of people with special needs. The languages are used to help the individuals with special needs. Research exporting the possibilities for suggesting better communication symbols can not only be taken as a scientific achievement but also as great services to humanity. This paper focuses on the identification and comparison of tools that have been developed to present the words in symbols. The careful selection of tool has been made so that the competitors are of adequate standard to generate the valuable results. The comparative study has focused on most desirable parameters, e.g. 3D animation, video based representation, sign Editor, Education tool, dictionary, text analysis and speech recognition. An ample amount of tools have been discussed and their merits and de-merits have been explored. In light of the discussion the choice of appropriate tool can be made based on the customized requirements.**

I. Introduction

A sign language uses visual sign patterns to convey meanings by combining the hand shapes, movements and orientations of the diversified shapes of hands, arms and other associated parts of the body. The facial expressions are also used to fully express the thoughts of the speaker. The sign languages are basically developed to help the deaf understand the message without listening. Diversity in the expressions has been observed throughout the world that is governed by the culture, traditions, symbolic signal representation and inter-symbol sequencing. Hundreds of sign languages are being used throughout the world simultaneously and have been greatly admired by the deaf culture.

The sign languages have been observed to be existing since 5th century BC. In 1620 Juan Pablo published "Reduction of letters and art for teaching mute people to speak" in Madrid which is considered to be the first symbolic representation of the words and phonetics enabling deaf to learn and present themselves by using the signs. Charles-Michel's work has been revolutionary in this domain and is used in France and North America until the present time.

With the passage of time, the need to develop computerized systems that can help the deaf in conveying and understanding the message has increased. In the consequent sections we discuss the available tools that can help in Translating the words into symbols, we also find the merits and de-merits of each tool, and finally a tabular view is Provided to summarize and facilitate the easy choice of tool for translating the words and punctuations into their symbolic equality.

About-Deanship Of E-Transactions And Communication King Saud University, Riyadh, Saudi Arabia
(e-mail;yousef@ccis.edu.sa)

II. Sign Language Tools

In this section, we survey available tools that help designers and developers to develop new systems for sign language translation.

A. Vsign

Vsign [1] is a 3-D animation tool implemented in Macromedia ShockWave. It is sponsored by EMMA (European Media Masters of Art) 2001/2002. It models the sign animations by means of an editor. Vsign consists of two parts:

Vsign Builder: The builder is an editor that facilitates a way to setup the beginning, end and intermediate states of signs (Figure 1). It provides separate modeling for hands, body and arms. The animation is saved to text files (with special file extension "gbr").

Vsign Player: This part facilitates playback of the animation file from a properly stored text file.

Vsign is a good tool that can be utilized to implement sign language translation since it contains a 3D capability along with the sign language editor. Fortunately, it does not have an extra hardware requirement. Furthermore, Vsign uses a simple file format to store animation information. However, this tool has some drawbacks. It does not have a user-friendly interface, for instance. In addition, it produces unrealistic (far from natural) 3D viewing.

Figure 1: Vsign Builder

B. The DeaulP University American Sign Language Project

This is a large scaled and professional academic 3-D project that aims to translate English to the American Sign Language (ASL) [2]. In order to improve quality of the animation, the project emphasizes on shadows and naturalness. Shadows and different light sources are implemented to make animations look normal. To achieve naturalness, every animation is repeated hundreds of times to detect and correct sharp/unrealistic movement transitions. Furthermore, the project aims towards comprehensible finger spelling. Thus, translation from every letter to a proper sign is kept in video file as AVI format.

The produced animations seem descriptive and realistic. However, there are only a few sample animations in the website (Figure 2) which does not give a concrete idea about the educational aspect and user interface of the project

Figure 2: The DePaul University American Sign Language example

C. Reading Power

Reading Power [3] is an educational software product for native signers focused on literacy and reading comprehension. The software includes storytelling, interactive conversation, and tools to build comprehension and vocabulary. Reading Power uses 3-D signing characters to unlock the power of reading and to add fun to the learning process. Reading Power also includes teacher support materials, activities, a starter dictionary and ideas for integrating technology into learning. Reading Power uses 3-D signing characters which avoid the disadvantages of video based applications. Reading Power has a big advantage with its 3-D virtual environment.

D. Ready Set Sign

Ready Set Sign (RSS) [4] is an online portal for teaching American Sign Language, but the main product is published and sold via CD. The portal has many lessons and many video clips for each lesson. The courses are organized as if they are intended to teach a foreign language. The site is easily understandable. Iconic explanations are widely used in videos which are helpful for reminding the user of the words. The site and the product use video clips to show motions and icons but as the quality increases it gets harder to process and download those videos. The portal has many lessons that are educationally well-organized. It includes some games that are simultaneously educational and entertaining, thus providing an enjoyable user experience.

E. Sign

The eSIGN [5] project aims to provide sign language on websites with small software installed to clients. It uses both 3-D animations and videos as the expression medium. It animates original BBC news simultaneously with a smart avatar near the news video. Moreover, eSIGN provides a user friendly interface (Figure 3). The animations are created with an intelligent sign language editor. The animations are based on motion-capture data and so they are more realistic than synthetic ones. Nevertheless, the hand shapes are not caught easily since the avatar is small.

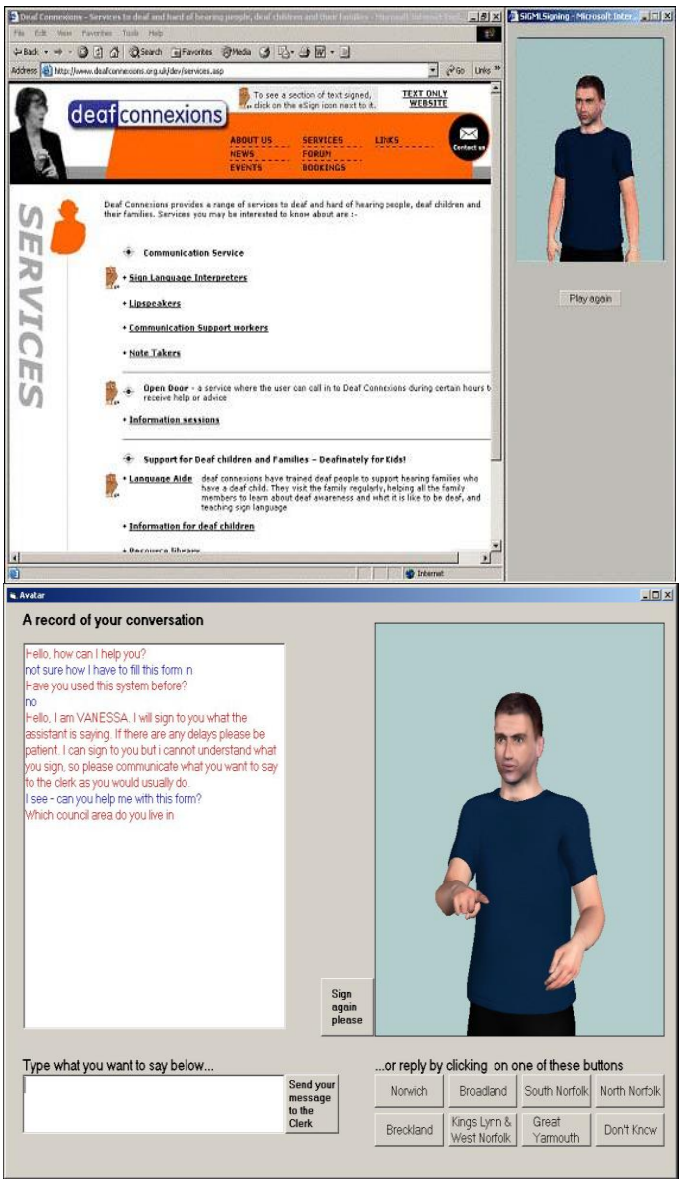


Figure 3: eSIGN (a- provide sign language on websites, b- sign language translator)

F. SignGenius

SignGenius [6] is a fast, interactive software package to learn Sign Language developed by Moving Hand Enterprises and accredited by DEAFSA (South African National Council for the Deaf). It uses video clips to demonstrate sign language. SignGenius is composed of six sections (Figure 4):

- Tips: Overview of the basic hand shapes and movements that a user may need to know in order to use sign language correctly.
- Tutor: 2197 video clips grouped into 65 categories.
- Test: test feature to test the ability to associate the video clips with the correct words.
- Score: For parents, teachers and students, measure progressing medium.
- Info: Comprehensive list of addresses of Deaf organizations, support groups etc.
- Game: A built-in Hangman game.

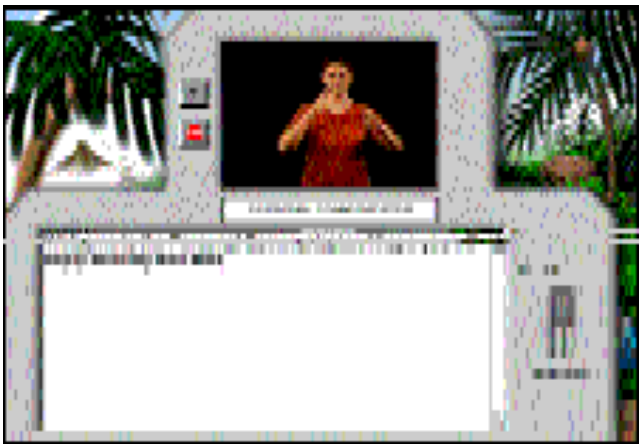
SignGenius is not an animation sign language tool but it has a numbers of features like advanced search function, user friendly interface, and good categorization for the tutor. However, SignGenius has some shortcomings e.g. low video quality, and insufficient educational perspective.

Figure 4: SignGenius

G. Personal Communicator

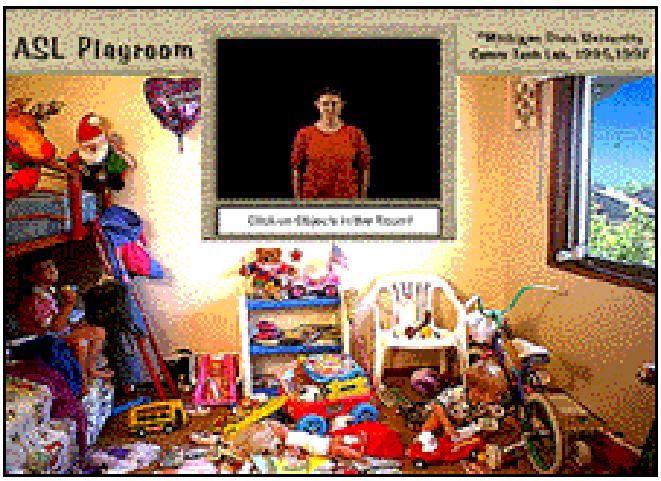
Personal communicator [7] is a tool for learning and communicating in American Sign Language (ASL) developed by Comm. Tech Lab in MSU. Personal Communicator uses digital video and compression technology for presenting sign language features. It has four components: word processor, text to sign/speech converter, an English-ASL dictionary and the ASL playroom.

The target audience is not limited to people who want to learn new signs, but extends to those who look for fun along the way. Interaction with the objects is provided in a user friendly and clever manner (Figure 5). This is digital video oriented tool, and is not a 3-D based environment



(a) Word Processor

(a) English-ASL Dictionary



(b) ASL Playroom

(d) ASL Browser
Figure 5: Personal Communicator

H. Visicast

ViSiCAST [8] is a project funded under the European Union Fifth Framework which is part of the Information Society Technologies (IST) program. It is a large project consisting of three main parts:
Multimedia and WWW Applications: which enables authors of web pages to provide signed material as part of the page's content.
Face-to-Face Transactions: this part provides a basis for dialogue between customer and clerk, through the incorporation of available moving image recognition technology to 'read' simple signs made by the deaf customer, which can then be translated into text or speech for the benefit of the clerk.
Television & Broadcast Transmission: this part concerns the provision of virtual human synthetic signing capabilities in the context of broadcast television, and has two related aspects: development of the necessary transmission technology and the incorporation of ViSiCAST work into the relevant broadcast standards.

Figure 6: ViSiCAST

I. Auslan Tuition System

Auslan Tuition System [9] is a 3-D animation of Australian Sign Language. It is created by the School of Computer Science & Software Engineering, University of Western Australia. It consists of two parts: Auslan Tuition System and Auslan Sign Editor. The Auslan tuition system is made up of several modes:
Tutorial mode that allows the user to select an Auslan phrase and learn the sign.
Finger-spelling mode where user enters words that are then finger spelled.
Dialogue mode that has two avatars signing dialogue together. This mode is designed for the sake of phrases learning in conversations.
Numbers mode which is used for number signing.
The Auslan Sign Editor software concentrates on building the signs, whereas the tuition part is the front end of the system and is used to display the constructed signs in a tutorial manner (Figure 7). Only Auslan Tuition System is available for download from the web. Shown animation demos seem detailed and realistic.

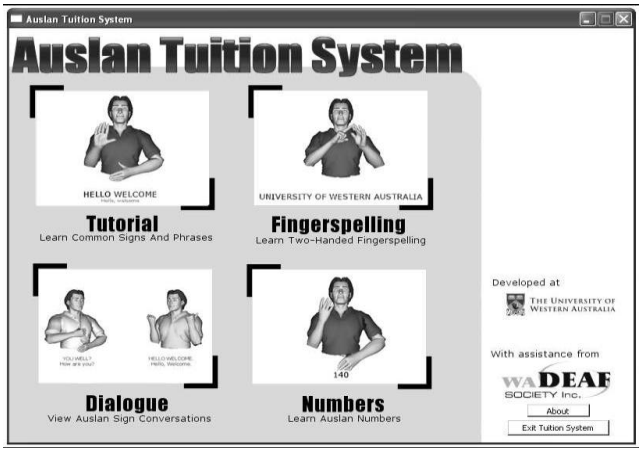


Figure 7: Auslan Tuition System

J. Sign Smith Studio & Gesture Builder

The Sign Smith Studio authoring tool from Vcom3D allows individuals to rapidly create Signing Avatar scripts for creating sign enabled content. Studio offers many powerful features for changing coordinated facial expression, eye gaze, role shifting and speech [10]. It contains over 2,500 ready to use signs in its dictionary. Sign Builder allows users of Studio to "spatially inflect" signs such as pronouns, verbs and classifiers. Sign Builder also allows users to create other signs that may not be a part of Studio's core dictionary. These include: Specialized technical and science vocabulary.
Signs which are standard in certain regions of the U.S.
Contextualized name signs for people and places.
Foreign sign languages such as British Sign Language (BSL), etc.
A key feature of this tool is Inverse Kinematics (IK) technology. It allows the user to focus on the hand position. Once the user selects a hand shape and properly positions

the hand, the IK software automatically places the joints of the wrist, elbow and shoulder in natural positions. These features give full power of creativity to the user. It is an easy tool to learn and use (Figure 8).

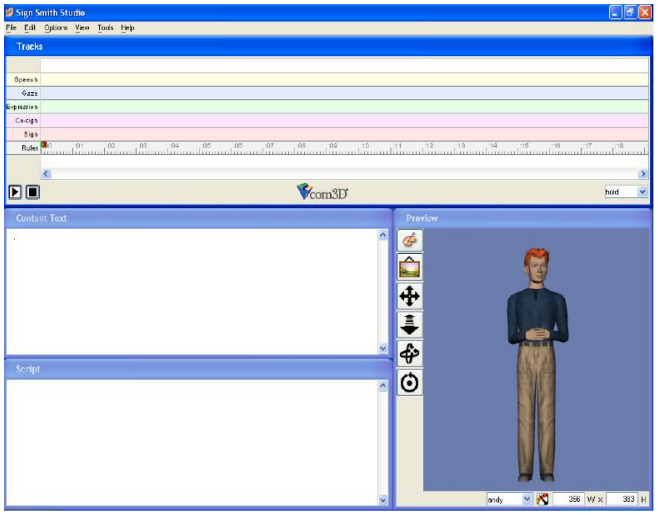


Figure 8: Sign Smith Studio

K. SiSi (Say It Sign It) System

It is 3D animation tool developed by researchers at IBM [11]. SiSi translates spoken or written words to the British Sign Language (BSL). In case of spoken words SiSi first translate the words to text then to 3D animations (Figure 9). The system is useful in many situations when there's no sign language interpreter like radio, telephone calls, some television shows.

Figure 9: The 3D character of SiSi system

L. Tawasoul

Tawasoul [12] is a research project conducted by the Computer Sciences Department in King Saud University. It was developed as an Arabic Sign Language (ARSL) educational tool for hearing impaired children, their parents, and others who are interested in learning ARSL. The system is comprised of four key features: namely, 3D Animations of ARSL expressions such as hand-signs, mouth and eyes expressions, morphological Analyzers which analyze the Arabic text to show the related ARSL animation, categorized ARSL vocabulary dictionary, and a sign language text editor (Figure 10). It consists of three parts:

Translator: It provides text to translate signs. It allows users to enter an Arabic text and view the Arabic signs that are related to the entered text.

Dictionary: Dictionary of Tawasoul is a basic vocabulary guide for users who want to learn Arabic Sign Language. It consists of a number of categories; each one contains a related group of words.

Finger Spelling: it can be utilized as a sign language editor to help users to write documents in sign alphabetic letters by converting the entered Arabic text to sign language text

Figure 10: Tawasoul

M. 3D-Sign

It is Malaysian sign language project [13]. It aims to develop a package to assist the learning of Malaysian sign language in 3D format using the 3D Poser Artist 4.0 which allows creating animations using 3D characters; the interface is easy to use (Figure 11). The package consists of the following functions:

One of three human characters can be selected: male, female and child.

Learners can select between different levels: beginner, intermediate and advanced.

The 3D animation enables learners to view hand/finger signing from different angles.

Different ways of learning such as chatting & puzzles' games.

Figure 11: 3D Sign

N. Sign to me

Simon Harvey developed British sign language tool and introduced the 'Sign to me' tool [14]. It provides videos of everyday signs aimed at adults and children who have difficulties with their reading and pre-reading age. It consists of many functions:

Find a Sign (Alphabetical Dictionary): by writing the word or the phrase then the video demonstrates the corresponding symbol (Figure 12)

Picture Signs (Picture Dictionary): Each sign is represented by a symbol in clear categories, when the cursor is rolled over the symbol, a video clip of the sign for that symbol appears and the word is also spoken.

Games: by showing a video clip of a sign, then letting the player choose the correct picture that represents that sign.

The main advantages is the ease of use and colorful symbols which make it an attractive way to learn.

Figure 12: Sign to me

O. Hand Speak

Hand Speak [14] is American Sign Language (ASL) site that produced an online dictionary, grammar, storytelling and poetry, manual alphabet (finger spelling), manual numeral, tutorials, articles. Hand speak consist ASL words in the constantly growing dictionary. All images after September 2007 are video-based, the rest of the older images are gif-animation (which will be replaced continually). A teacher can vocally speak a word and the child fingerspells out a word in spelling lessons. (Figure 13)

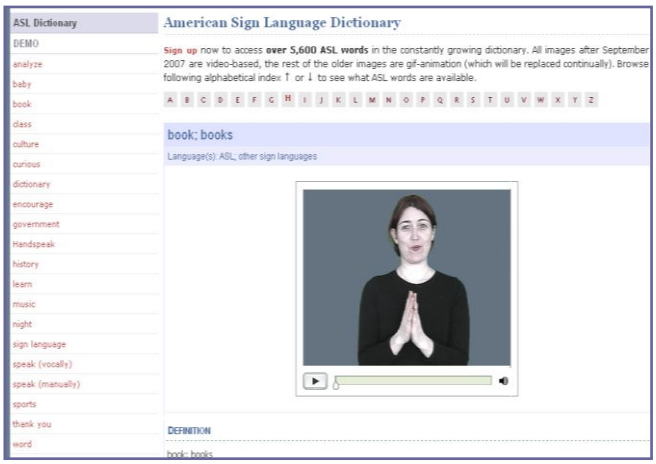


Figure 13: Hand Speak

P. Comparison of various tools

Examining these fifteen notable products gives a good overview of the technology solutions in this domain. Table 1 presents the whole ten products along with main features of each one.

Q. Comparison of various tools

Examining these fifteen notable products gives a good overview of the technology solutions in this domain. Table 1 presents the whole ten products along with main features of each one.

Tool/ Feature	3D Animation	Video Based	Sign Editor	Education Tool	Dictionary	Free Text Analyzer	Speech Recognition
Vsign	Yes	No	Yes	No	No	No	No
ASL Project	Yes	No	Yes	No	Yes	No	No
eSIGN	Yes	Yes	Yes	Yes	Yes	Yes	No
Reading Power	Yes	No	No	Yes	Yes	No	No
SignGenius	No	Yes	No	No	Yes	No	No
Ready Set Sign	No	Yes	No	Yes	Yes	No	Yes
ViSiCAST	Yes	No	No	No	No	Yes	Yes
Personal Communicator	No	Yes	No	Yes	Yes	Yes	No
Auslan Tuition	Yes	No	Yes	Yes	Yes	No	No
Sign Smith Studio	Yes	No	Yes	Yes	Yes	Yes	No

SiSi	Yes	No	No	Yes	No	Yes	Yes
Tawasoul	Yes	No	No	Yes	Yes	Yes	No
3D-Sign	Yes	Yes	No	Yes	Yes	No	No
Sign to me	No	Yes	No	Yes	Yes	No	No
Hand Speak	No	Yes	No	No	Yes	No	No

Table 2: Comparison of sign language products

III. Conclusion

This paper highlights certain parameters that are essential for evaluating the effectiveness of sign language tools. The parameters include but not limited to 3-D animation, video based features, sign editor, education tool, dictionary, text analyzer and speech recognition component. After comprehensive discussion of ten different sign language tools based on the mentioned parameters it has been observed that none of the existing tools meets all the parameters. Comparing all the available tools against known parameters we can identify the extent to which each tool supports these essential features. 'VSign', 'SignGenius', and 'Hand Speak' support only two features each, 'Ready Set Sign' and 'Auslan Tuition' and few other support three or four features respectively. 'Sign Smith Studio' support the five major features required in a sign language tool. The SiSi tools has the support for animation, text analyzer and speech recognition but lacks the valuable features like video base and sign editor. Tawasol also lack the features that SiSi lacks. '3D-Sign' and 'Sign to me' are very well video based but lack the features like animation, editor, text analyzer and speech analyzer. 'Hand Speak' also suffers from the facts that it does not support 3D-animation, Sign Editor, Education Tool, Text and speech analyzer. The result of the study support that eSIGN tool provides the best functionality with respect to the features used for evaluation.

IV. References

1) Vsign, Vsign Project, http://www.vsign.nl/EN/vsignEN.htm.
2) DePaul ASL Synthesizer, The DePaul University American Sign Language Project., "http://asl.cs.depaul.edu".
3) Reading Power, "http://voisales.com/items/sign-language-software/vcom3d/reading-power-detail.html".
4) Ready! Set! Sign! "http://www.readysetsign.com/index2.html".
5) eSIGN at UEA, eSign, "http://www.visicast.cmp.uea.ac.uk/eSIGN/Introduction.html".
6) Sign Language Software by SignGenius, "http://www.signgenius.com/".
7) Comm Tech Lab @ MSU, Personal Communicator., "http://commtechlab.msu.edu/index.php".
8) ViSiCAST Project, "http://www.visicast.sys.uea.ac.uk/Publications.html".
9) Auslan Tuition System, "http://auslantuition.csse.uwa.edu.au/".
10) Vcom3D, Sign Smith Studio & Gesture Builder., "http://www.vcom3d.com/".
11) IBM Recruitment , SiSi software, "http://www-05.ibm.com/employment/uk/extreme-blue/cool-projects/sisi.html"
12) Tawasoul, "http://tawasoul4arsl.ksu.edu.sa/"
13) DSpace@UM, 3D-Sign, "http://dspace.fsktm.um.edu.my/handle/1812/200"
14) British sign language, Sing to me, http://www.britishsign.co.uk/product_info.php?pName=sign-to-me-cdrom
15) Handspeak: http://www.handspeak.com/tour
16) Ahmad Mukhtar Omer, Muhammad Hamassa Abdul Latif, Mustafa Zahran, „Basic Language „„ Bachelors degree thesis, Feb. 2000
17) A tool for analysis of the Arabic sentence," twitter Aallissan, Samia geek, Maha Al-Rabiah and Faten Al-Qahtani, a graduation project for a bachelor's degree, Riyadh, Feb. 2000
18) Francik, J. and P. Fabian, "Animating Sign Language in the Real Time, 20th IASTED International Multi-Conference Applied Informatics, Innsbruck, Austria, pp. 276-281, 2002.
19) Holden, E. J. and G. G. Roy, "The Graphical Translation of English Text into Signed English in the Hand Sign Translator System", Computer Graphics Forum (Eurographics'92), vol. 11, no. 3, pp. C357-C366, 1992.

A Low-Overhead Minimum Process Coordinated Checkpointing Algorithm for Mobile Distributed System

GJCST Computing Classification
C.2.4, C.1.4, C.4

Parveen Kumar[1] Poonam Gahlan[2]

***Abstract*-A distributed system is a collection of independent entities that cooperate to solve a problem that cannot be individually solved. A mobile computing system is a distributed system where some of processes are running on mobile hosts (MHs), whose location in the network changes with time. The number of processes that take checkpoints is minimized to 1) avoid awakening of MHs in doze mode of operation, 2) minimize thrashing of MHs with checkpointing activity, 3) save limited battery life of MHs and low bandwidth of wireless channels. In minimum-process checkpointing protocols, some useless checkpoints are taken or blocking of processes takes place. In this paper, we propose a minimum-process coordinated checkpointing algorithm for non-deterministic mobile distributed systems, where no useless checkpoints are taken. An effort has been made to minimize the blocking of processes and synchronization message overhead. We try to reduce the loss of checkpointing effort when any process fails to take its checkpoint in coordination with others.**

Keywords-Checkpointing algorithms; parallel & distributed computing; rollback recovery; fault-tolerant system; mobile computing

I. INTRODUCTION

Parallel computing with clusters of workstations is being used extensively as they are cost-effective and scalable, and are able to meet the demands of high performance computing. Increase in the number of components in such systems increases the failure probability. It is, thus, necessary to examine both hardware and software solutions to ensure fault tolerance of such parallel computers. To provide fault tolerance, it is essential to understand the nature of the faults that occur in these systems. There are mainly two kinds of faults: permanent and transient. Permanent faults are caused by permanent damage to one or more components and transient faults are caused by changes in environmental conditions. Permanent faults can be rectified by repair or replacement of components. Transient faults remain for a short duration of time and are difficult to detect and deal with. Hence it is necessary to provide fault tolerance particularly for transient failures in parallel computers. Fault-tolerant techniques enable a system to perform tasks in the presence of faults. It is easier and more Cost effective to provide software fault tolerance solutions than hardware solutions to cope with transient failures [25].

A distributed system is a collection of independent entities that cooperate to solve a problem that cannot be individually solved. With the widespread proliferation of the Internet and the emerging global village, the notion of distributed computing systems as a useful and widely deployed tool is becoming a reality [24]. A distributed system can be characterized as a collection of mostly autonomous processors communicating over a communication network and having the following features [25]

No common physical clock; This is an important assumption because it introduces the element of "distribution" in the system and gives rise to the inherent asynchrony amongst the processors.

No shared memory; This is a key feature that requires message-passing for communication. It may be noted that a distributed system may still provide the abstraction of a common address space via the distributed shared memory abstraction.

***Geographical separation*;** It is not necessary for the processors to be on a wide-area network (WAN). Recently, the network/cluster of workstations (NOW/COW) configuration connecting processors on a LAN is also being increasingly regarded as a small distributed system. This NOW configuration is becoming popular because of the low-cost high-speed off-the-shelf processors now available. The Google search engine is based on the NOW architecture.

Autonomy and heterogeneity; The processors are "loosely coupled in that they have different speeds and each can be running a different operating system. They are usually not part of a dedicated system, but cooperate with one another by offering services or solving a problem [25].

Local checkpoint is the saved state of a process at a processor at a given instance. Global checkpoint is a collection of local checkpoints, one from each process. A global state is said to be "consistent" if it contains no orphan message; i.e., a message whose receive event is recorded, but its send event is lost. To recover from a failure, the system restarts its execution from a previous consistent global state saved on the stable storage during fault-free execution. In distributed systems, checkpointing can be independent, coordinated, or quasi-synchronous. Message Logging is also used for fault tolerance in distributed systems [14]. Most of the existing coordinated checkpointing algorithms [9, 19] rely on the two-phase protocol and save two kinds of checkpoints on the stable

About-[1]Department of Computer Science & Engineering Meerut Institute of Engineering & Technology, Meerut, India, -250005
(e-mail: pk223475@yahoo.com)
About-[2]Department of Computer Sc & Engg, Singhania University, Pacheri Bari (Rajasthan) India;(e-mail: swastikaarya83@gmail.com)

storage: tentative and permanent. In the first phase, the initiator process takes a tentative checkpoint and requests all or selective processes to take their tentative checkpoints. If all processes are asked to take their checkpoints, it is called all-process coordinated checkpointing [5, 7, 19]. Alternatively, if selective communicating processes are required to take checkpoints, it is called minimum-process checkpointing. Each process informs the initiator whether it succeeded in taking a tentative checkpoint. After the initiator has received positive acknowledgments from all relevant processes, the algorithm enters the second phase. Alternatively, if a process fails to take its tentative checkpoint in the first phase, the initiator process requests all processes to abort their tentative checkpoint.

If the initiator learns that all concerned processes have successfully taken their tentative checkpoints, the algorithm enters in the second phase and the initiator asks the relevant processes to make their tentative checkpoints permanent.

In order to record a consistent global checkpoint, when a process takes a checkpoint, it asks (by sending checkpoint requests to) all relevant processes to take checkpoints. Therefore, coordinated checkpointing suffers from high overhead associated with the checkpointing process [20], [21], [22], [23]. Much of the previous work [2, 3, 4, 20, 21, 22, 23] in coordinated checkpointing has focused on minimizing the number of synchronization messages and the number of checkpoints during the checkpointing process. However, some algorithms (called blocking algorithm) force all relevant processes in the system to block their computations during the checkpointing process [3, 9, 21, 22, 23]. Checkpointing includes the time to trace the dependency tree and to save the states of processes on the stable storage, which may be long. Moreover, in mobile computing systems, due to the mobility of MHs, a message may be routed several times before reaching its destination. Therefore, blocking algorithms may dramatically reduce the performance of these systems [7]. Recently, non-blocking algorithms [7, 19] have received considerable attention. In these algorithms, processes need not block during the checkpointing by using a checkpointing sequence number to identify orphan messages. Moreover, these algorithms [4, 10] require all processes in the system to take checkpoints during checkpointing, even though many of them may not be necessary.

A mobile computing system is a distributed system where some of processes are running on mobile hosts (MHs), whose location in the network changes with time. To communicate with MHs, mobile support stations (MSSs) act as access points for the MHs by wireless networks. Features that make traditional checkpointing algorithms for distributed systems unsuitable for mobile computing systems are: locating processes that have to take their checkpoints, energy consumption constraints, lack of stable storage in MHs, and low bandwidth for communication with MHs [1]. Minimum-process coordinated checkpointing is an attractive approach for transparently adding fault tolerance to distributed applications, since it avoids domino effect, minimizes the stable storage requirement and also forces only interacting processes to checkpoint.

In coordinated or synchronous checkpointing, processes coordinate their local checkpointing actions such that the set of all recent checkpoints in the system is guaranteed to be consistent [add reference list……]. In case of a fault, every process restarts from its most recent permanent/committed checkpoint. Hence, this approach simplifies recovery and it does not suffer from domino-effect. Furthermore, coordinated checkpointing requires each process to maintain only one permanent checkpoint on stable storage, reducing storage overhead and eliminating the need for garbage collection. Its main disadvantage is the large latency involved in output commit.

A straightforward approach to coordinate checkpointing is to block communications while the checkpointing process executes. A coordinator takes a checkpoint and broadcasts a request message to all processes, asking them to take a checkpoint. When a process receives a message, it stops its execution, flushes all the communication channels, takes a tentative checkpoint, and sends an acknowledgement message back to the coordinator. After the coordinator receives acknowledgement from all processes, it broadcasts a commit message that completes the two phase checkpointing protocol. After receiving the commit message, each process receives the old permanent checkpoint and makes the tentative checkpoint permanent. The process is then free to resume execution and exchange messages with other processes. The coordinated checkpointing algorithms can also be classified into following two categories: minimum-process and all process algorithms.

Prakash-Singhal algorithm [13] forces only a minimum number of processes to take checkpoints and does not block the underlying computation during checkpointing. However, it was proved that their algorithm may result in an inconsistency [3]. Cao and Singhal [4] achieved non-intrusiveness in the minimum-process algorithm by introducing the concept of mutable checkpoints. The number of useless checkpoints in [4] may be exceedingly high in some situations [16]. Kumar et. al [16] and Kumar et. al [11] reduced the height of the checkpointing tree and the number of useless checkpoints by keeping non-intrusiveness intact, at the extra cost of maintaining and collecting dependency vectors, computing the minimum set and broadcasting the same on the static network along with the checkpoint request. Some minimum-process blocking algorithms are also proposed in literature [3, 9, 21, 23].

In this paper, we propose an efficient checkpointing algorithm for mobile computing systems that forces only a minimum number of processes to take checkpoints. An effort has been made to minimize the blocking of processes and synchronization message overhead.

We capture the partial transitive dependencies during the normal execution by piggybacking dependency vectors onto computation messages. The Z-dependencies are well taken care of in this protocol. In order to reduce the message overhead, we also avoid collecting dependency vectors of all processes to find the minimum set as in [3], [11], [21]. We also try to minimize the loss of checkpointing effort when any process fails to take its checkpoint.

II. Proposed Checkpointing Algorithm

Our system model is similar to [4, 21]. We propose to handle node mobility and failures during checkpointing as proposed in [21].

A. The Proposed Algorithm

First phase of the algorithm: When a process, say Pi, running on an MH, say MHi, initiates a checkpointing, it sends a checkpoint initiation request to its local MSS, which will be the proxy MSS (if the initiator runs on an MSS, then the MSS is the proxy MSS). The proxy MSS maintains the dependency vector of Pi say Ri. On the basis of Ri, the set of dependent processes of Pi is formed, say Sminset. The proxy MSS broadcasts ckpt (Sminset) to all MSSs. When an MSS receive ckpt (Sminset) message, it checks, if any processes in Sminset are in its cell. If so, the MSS sends mutable checkpoint request message to them. Any process receiving a mutable checkpoint request takes a mutable checkpoint and sends a response to its local MSS. After an MSS received all response messages from the processes to which it sent mutable checkpoint request messages, it sends a response to the proxy MSS. It should be noted that in the first phase, all processes take the mutable checkpoints. For a process running on a static host, mutable checkpoint is equivalent to tentative checkpoint. But, for an MH, mutable checkpoint is different from tentative checkpoint. In order to take a tentative checkpoint, an MH has to record its local state and has to transfer it to its local MSS. But, the mutable checkpoint is stored on the local disk of the MH. It should be noted that the effort of taking a mutable checkpoint is very small as compared to the tentative one[4]. For a disconnected MH that is a member of minimum set, the MSS that has its disconnected checkpoint, considers its disconnected checkpoint as the required come.

Second Phase of the Algorithm; After the proxy MSS has received the response from every MSS, the algorithm enters the second phase. If the proxy MSS learns that all relevant processes have taken their mutable checkpoints successfully, it asks them to convert their mutable checkpoints into tentative ones and also sends the exact minimum set along with this request. Alternatively, if initiator MSS comes to know that some process has failed to take its checkpoint in the first phase, it issues abort request to all MSS. In this way the MHs need to abort only the mutable checkpoints, and not the tentative ones. In this way we try to reduce the loss of checkpointing effort in case of abort of checkpointing algorithm in first phase.

When an MSS receives the tentative checkpoint request, it asks all the process in the minimum set, which are also running in itself, to convert their mutable checkpoints into tentative ones. When an MSS learns that all relevant process in its cell have taken their tentative checkpoints successfully, it sends response to proxy MSS.

Third Phase of the Algorithm; Finally, when the proxy MSS learns that all processes in the minimum set have taken their tentative checkpoints successfully, it issues commit request to all MSSs. When a process in the minimum set gets the commit request, it converts its tentative checkpoint into permanent one and discards its earlier permanent checkpoint, if any.

B. Massage Handling During Checkpointing

When a process takes its mutable checkpoint, it does not send any massage till it receives the tentative checkpoint request. Suppose, Pi sends m to Pj after taking its mutable checkpoint and Pj has not taken its mutable checkpoint at the time of receiving m. In this case, if Pj takes its mutable checkpoint after processing m, then m will become orphan. Therefore, we do not allow Pi to send any massage unless and until every process in the minimum set have taken its mutable checkpoint in the first phase. Pi can send massages when it receives the tentative checkpoint request; because, at this moment every concerned process has taken its mutable checkpoint and m cannot become orphan. The massages to be sent are buffered at senders end. In this duration, a process is allowed to continue its normal computations and receive massages.

Suppose, Pj gets the mutable checkpoint request at MSSp. Now, we find any process Pk such that Pk does not belong to Sminset and Pk belongs to Rj. In this case, Pk is also included in the minimum set; and Pj sends mutable checkpoint request to Pk. It should be noted that the Sminset, computed on the basis of dependency vector of initiator process is only a subset of the minimum set. Due to zigzag dependencies, initiator process may be transitively dependent upon some more process which is not included in the $S_{minset.}$

C. An Example

The proposed Algorithm can be better understood by the example shown in Figure 2. There are six processes (P0 to P5) denoted by straight lines. Each process is assumed to have initial permanent checkpoints with csn equal to "0". Cix denotes the xth checkpoints of Pi. Initial dependency vectors of P0, P1, P2, P3, P4, P5 are [000001], [000010] [000100], [001000], [010000], and [100000], respectively. The dependency vectors are maintained as explained in Section 2.1.

P0 sends m2 to P1 along with its dependency vector [000001]. When P1 receives m2, it computes its dependency vector by taking bitwise logical OR of dependency vectors of P_0 and P_1, which comes out to be [000011]. Similarly, P_2 updates its dependency vector on receiving m_3 and it comes out to be [000111]. At time t_1, P_2 initiates checkpointing algorithm with its dependency vector is [000111]. At time t_1, P_2 finds that it is transitively dependent upon P_0 and P_1. Therefore, P_2 computes the tentative minimum set [S_{minset}= {P_0, P_1, P_2}]. P_2 sends the mutable checkpoint request to P_1 and P_0 and takes its own mutable checkpoint C_{21}. For an MH the mutable checkpoint is stored on the disk of MH. It should be noted that S_{minset} is only a subset of the minimum set. When P_1 takes its mutable checkpoint C_{11}, it finds that it is dependent upon P_3 due to m_4, but P_3 is not a member of After taking its mutable checkpoint C21, P2 generates m8 for P3. As P2 has already taken its mutable checkpoint for

the current initiation and it has not received the tentative checkpoint request from the initiator; therefore P2 buffers m8 on its local disk. We define this duration as the uncertainty period of a process during which a process is not allowed to send any massage. The massages generated for sending are buffered at the local disk of the sender's process. P2 can sends m8 only after getting tentative checkpoint request or abort massages from the initiator process. Similarly, after taking its mutable checkpoint P0 buffers m10 for its uncertainty period. It should be noted that P1 receives m10 only after taking its mutable checkpoint. Similarly, P3 receives m8 only after taking its mutable checkpoint C31.A process receives all the massages during its uncertainty period for example P3 receives m11. A process is also allowed to perform its normal computations during its uncertainty period.

At time t2, P2 receives responses to mutable checkpoints requests from all process in the minimum set (not shown in the Figure 2) and finds that they have taken their mutable checkpoints successfully, therefore, P2 issues tentative checkpoint request to all processes. On getting tentative checkpoint request, processes in the minimum set [P0, P1, P2, P3] convert their mutable checkpoints into tentative ones and send the response to initiator process P2; these process also send the massages, buffered at their local disks, to the destination processes For example, P0 sends m10 to P1 after getting tentative checkpoint request [not shown in the figure]. Similarly, P_2 sends m_8 to P_3 after getting tentative checkpoint request. At time t_3, P_2 receives responses from the process in minimum set [not shown in the figure] and finds that they have taken their tentative checkpoints successfully, therefore, P_2 issues commit request to all process. A process in the minimum set converts its tentative checkpoint into permanent checkpoint and discards it old permanent checkpoint if any.

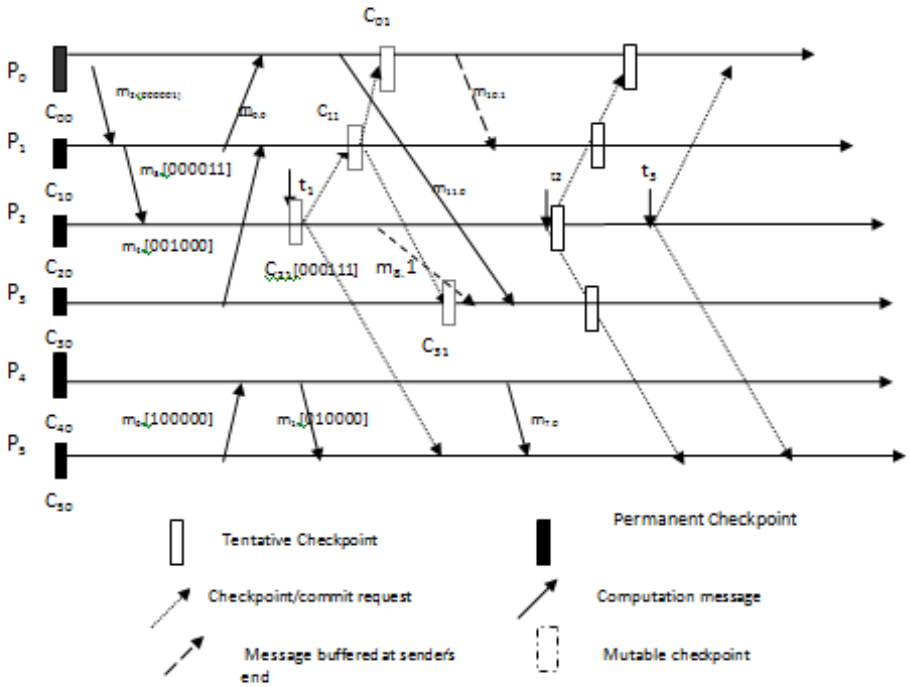


Figure 2

D. *Correctness Proof*

We can show that global state collected by the proposed protocol will be consistent. We can prove the result by contradiction. Suppose there is some orphan message in the recorded global state. We explore different possibilities with the help of Figure 2. Suppose, P0 sends m10 after taking its mutable checkpoint and P1 receives m10 before taking its mutable checkpoint. This situation is not possible, because, after taking its mutable checkpoint P0 comes into its uncertainty period and it cannot send any message unless and until it receives the tentative checkpoint request. P2 can issue the tentative checkpoint request only after getting confirmed that every concerned process (including P1) has taken its mutable check point. Hence P1 cannot receive m10 before taking its mutable checkpoint C11. Suppose, P5 sends m13 to P3 after C50 and P3 gets m13 before C31 (not show in the Figure 2). In this case, when P3 takes its mutable checkpoint C31, it will find that P5 does not belong to Sminset and P3 is dependent upon P5; therefore, P3 will send mutable checkpoint request to P5 and send (m13) will also be included in the global state the other possibilities can be proved by obviousness [21].

III. Comparative Analysis of the Proposed Algorithms with Other Algorithms

We use following notations to compare our algorithm with other algorithms:

N_{mss}: number of MSSs.

N_{mh}: number of MHs.

C_{pp}: cost of sending a message from one process to another

C_{st}: cost of sending a message between any two MSSs.

C_{wl}: cost of sending a message from an MH to its local MSS (or vice versa).

$C_{broadcast}$: cost of broadcasting a message over static network.

C_{search}: cost incurred to locate an MH and forward a message to its current local MSS, from a source MSS.

T_{st}: average message delay in static network.

T_{wl}: average message delay in the wireless network.

T_{ch}: average delay to save a checkpoint on the stable storage. It also includes the time to transfer the checkpoint from an MH to its local MSS.

N: total number of processes

N_{min}: number of minimum processes required to take checkpoints.

N_{mut}: number of useless mutable checkpoints [4].

T_{search}: average delay incurred to locate an MH and forward a message to its current local MSS.

N_{ucr}: average number of useless checkpoint requests in [4].

N_{dep}: average number of processes on which a process depends.

h_1 : height of the checkpointing tree in Koo-Toueg algorithm [9].

h_2 : height of the checkpointing tree in the proposed algorithm.

IV. Message Overhead of the Proposed Algorithm

A. Message overhead in the first phase

Initiator process sends mutable checkpoint request to the local MSS and (say MSS_{in}) and gets response from the MSS_{in}: 2 C_{wl}

MSS in broadcasts mutable checkpoint request over the static network: $C_{broadcast}$

We suppose that all the process are running on MHs.

All the process in the minimum set get the mutable checkpoint request from the local MSS and sends response to the local MSS: $2*N_{min}*C_{wl}$

Every MSS sends response to MSS_{in}: $N_{mss}*C_{st}$

process is blocked when it takes its mutable checkpoint and it waits for the other concerned process to take their mutable checkpoints to come out of blocking state. In KT algorithm [9], a process is blocked when it takes its tentative checkpoint and it waits for the other concerned process to take their tentative checkpoints to come out of blocking state. In mobile distributed systems, the time to take a mutable

B. Message overhead in the second phase

MSSin broadcasts tentative checkpoint request over static network:Cbroadcast

Every process in the minimum set receives tentative checkpoint request, and sends response to these requests to local MSS: 2*Nmin*Cwl

Every MSS sends response to MSSin: Nmss*Cst

C. Message Overhead In The Third Phase

MSS_{in} broadcasts commit request over static network: $C_{broadcast}$

Total Average message overhead: $2Cwl+3\ C_{broadcast} +4*N_{min}*C_{wl} + 2*N_{mss}*C_{st}$

Our algorithm is a three phase algorithm; therefore it suffers from extra message overhead of $C_{broadcast} +4*N_{min}*C_{wl}$. By doing so, we are able to reduce the loss of checkpointing effort in case of abort of the checkpointing procedure in the first phase. In other algorithms [2, 3, 4, 9], in case of abort in the first phase, all concerned processes are forced to abort their tentative checkpoint whereas in the proposed scheme, all relevant processes abort their mutable checkpoints only. The effort of taking a mutable checkpoint is negligible as compared to tentative one in the mobile distributed system [4]. Frequent abort of checkpointing algorithms, due to exhausted battery power, abrupt disconnections etc., may significantly increase the checkpointing overhead in two-phase algorithms [2, 3, 4, 9]. We try to minimize the same by designing the three phase algorithm.

In our algorithm, only minimum number of processes is required to take their checkpoints.

The blocking time of the Koo-Toueg [11] protocol is highest, followed by Cao-Singhal [4] algorithm. We claim that the blocking time in the proposed scheme will be significantly smaller as compared to the KT Algorithm [9]. Because, in algorithm [9], transitive dependencies are collected by direct dependencies. The checkpoint initiator process, say Pin, sends the checkpoint request to any process Pi if Pin is causally dependent upon Pi. Similarly, Pi sends the checkpoint request to any process Pj if Pi is causally dependent upon Pj. In this way, a checkpointing tree is formed. In the proposed algorithm, transitive dependencies are captured during normal execution as described in Section 2.1. Some zigzag dependencies may not be captured in the proposed scheme during normal execution and they may form low order checkpointing tree in some typical situations. But, in general, the checkpointing tree formed in the proposed scheme will be negligibly small as compared to KT algorithm [9] and hence the blocking time of processes will be small in the proposed scheme as compared to KT algorithm [9]. Furthermore, in the proposed scheme, a checkpoint may be negligibly small as compared to tentative checkpoint. Hence, in the proposed scheme, the blocking period of a process will be significantly small as compared to the KT algorithm [9]. Our blocking period is larger than CS algorithm [3], but it suffers from extra message overhead of collecting dependency vectors from all processes and moreover, it forces all the processes to block for a short duration. In our scheme, a process is blocked only if it is a

member of the minimum set. Furthermore, a process is allowed to perform its normal computations and receive messages during its blocking period

In the algorithms proposed in [4], [20], no blocking of processes takes place, but some useless checkpoints are taken, which are discarded on commit. In Elnozahy et al [7] algorithm, all processes take checkpoints. In the protocols [3], [9], and in the proposed one, only minimum numbers of processes record their checkpoints. In algorithm [4], concurrent executions of the algorithm are allowed, but it may lead to inconsistencies in doing so [17]. We avoid the concurrent executions of the proposed algorithm..

Table 1. A Comparison of System Performance

	Cao-Singhal [4]	**Cao-Singhal [5]**	**Koo-Toeg Algorithm [11]**	**Elnozahy et al [8]**	**Proposed Algorithm**
Avg. blocking Time	$2T_{st}$	0	h_1*T_{ch}	0	h_2*T_{ch}
Average No. of checkpoints	N_{min}	$N_{min}+N_{mut}$	N_{min}	N	N_{min}
Average Message Overhead	$3C_{broadcast}+2C_{wl}+2N_{mss}*C_{st}+3N_{mh}*C_{wl}$	$2*N_{min}*C_{pp}+C_{broadcast}+N_{ucr}*C_{pp}$	$3*N_{min}*C_{pp}*N_{dep}$	$2*C_{broadcast}+N*C_{pp}$	$2Cwl+3+C_{broadcast}+4*N_{min}*C_{wl}+2*N_{mss}*C_{st}$

V. Conclusion

In this paper, we have proposed a minimum-process checkpointing protocol for deterministic mobile distributed systems, where no useless checkpoints are taken and an effort has been made to minimize the blocking of processes. We try to reduce the checkpointing time and blocking time of processes by limiting checkpointing tree which may be formed in other algorithms [4, 9]. We captured the transitive dependencies during the normal execution by piggybacking dependency vectors onto computation messages. The Z-dependencies are well taken care of in this protocol. We also try to reduce the loss of checkpointing effort when any process fails to take its checkpoint in coordination with others

VI. References

1) Acharya A. and Badrinath B. R., "Checkpointing Distributed Applications on Mobile Computers," Proceedings of the 3rd International Conference on Parallel and Distributed Information Systems, pp. 73-80, September 1994.
2) Cao G. and Singhal M., "On coordinated checkpointing in Distributed Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 9, no.12, pp. 1213-1225, Dec 1998.
3) Cao G. and Singhal M., "On the Impossibility of Min-process Non-blocking Checkpointing and an Efficient Checkpointing Algorithm for Mobile Computing Systems," Proceedings of International Conference on Parallel Processing, pp. 37-44, August 1998.
4) Cao G. and Singhal M., "Mutable Checkpoints: A New Checkpointing Approach for Mobile Computing systems," IEEE Transaction On Parallel and Distributed Systems, vol. 12, no. 2, pp. 157-172, February 2001.
5) Chandy K. M. and Lamport L., "Distributed Snapshots: Determining Global State of Distributed Systems," ACM Transaction on Computing Systems, vol. 3, No. 1, pp. 63-75, February 1985.
6) Elnozahy E.N., Alvisi L., Wang Y.M. and Johnson D.B., "A Survey of Rollback-Recovery Protocols in Message-Passing Systems," ACM Computing Surveys, vol. 34, no. 3, pp. 375-408, 2002.
7) Elnozahy E.N., Johnson D.B. and Zwaenepoel W., "The Performance of Consistent Checkpointing," Proceedings of the 11th Symposium on Reliable Distributed Systems, pp. 39-47, October 1992.
8) Higaki H. and Takizawa M., "Checkpoint-recovery Protocol for Reliable Mobile Systems," Trans. of Information processing Japan, vol. 40, no.1, pp. 236-244, Jan. 1999.
9) Koo R. and Toueg S., "Checkpointing and Roll-Back Recovery for Distributed Systems," IEEE Trans. on Software Engineering, vol. 13, no. 1, pp. 23-31, January 1987.

12) Neves N. and Fuchs W. K., "Adaptive Recovery for Mobile Environments," Communications of the ACM, vol. 40, no. 1, pp. 68-74, January 1997.
13) Parveen Kumar, Lalit Kumar, R K Chauhan, V K Gupta "A Non-Intrusive Minimum Process Synchronous Checkpointing Protocol for Mobile Distributed Systems" Proceedings of IEEE ICPWC-2005, pp 491-95, January 2005.
14) Pradhan D.K., Krishana P.P. and Vaidya N.H., "Recovery in Mobile Wireless Environment: Design and Trade-off Analysis," Proceedings 26th International Symposium on Fault-Tolerant Computing, pp. 16-25, 1996.
15) Prakash R. and Singhal M., "Low-Cost Checkpointing and Failure Recovery in Mobile Computing Systems," IEEE Transaction On Parallel and Distributed Systems, vol. 7, no. 10, pp. 1035-1048, October1996.
16) Ssu K.F., Yao B., Fuchs W.K. and Neves N. F., "Adaptive Checkpointing with Storage Management for Mobile Environments," IEEE Transactions on Reliability, vol. 48, no. 4, pp. 315-324, December 1999.
17) J.L. Kim, T. Park, "An efficient Protocol for checkpointing Recovery in Distributed Systems," IEEE Trans. Parallel and Distributed Systems, pp. 955-960, Aug. 1993.
18) L. Kumar, M. Misra, R.C. Joshi, "Low overhead optimal checkpointing for mobile distributed systems" Proceedings. 19th IEEE International Conference on Data Engineering, pp 686 – 88, 2003.
19) Ni, W., S. Vrbsky and S. Ray, "Pitfalls in Distributed Nonblocking Checkpointing", Journal of Interconnection Networks, Vol. 1 No. 5, pp. 47-78, March 2004.
20) L. Lamport, "Time, clocks and ordering of events in a distributed system" Comm. ACM, vol.21, no.7, pp. 558-565, July 1978.
21) Silva, L.M. and J.G. Silva, "Global checkpointing for distributed programs", Proc. 11th symp. Reliable Distributed Systems, pp. 155-62, Oct. 1992.
22) Parveen Kumar, Lalit Kumar, R K Chauhan, "A Non-intrusive Hybrid Synchronous Checkpointing Protocol for Mobile Systems", IETE Journal of Research, Vol. 52 No. 2&3, 2006.
23) Parveen Kumar, "A Low-Cost Hybrid Coordinated Checkpointing Protocol for mobile distributed systems", Mobile Information Systems. pp 13-32, Vol. 4, No. 1, 2007.
24) Lalit Kumar Awasthi, Parveen Kumar, "A Synchronous Checkpointing Protocol for Mobile Distributed Systems: Probabilistic Approach" International Journal of Information and Computer Security, Vol.1, No.3 pp 298-314.
25) Sunil Kumar, R K Chauhan, Parveen Kumar, "A Minimum-process Coordinated Checkpointing Protocol for Mobile Computing Systems", International Journal of Foundations of Computer science,Vol 19, No. 4, pp 1015-1038 (2008).
26) [24] A. Tanenbaum and M. Van Steen, Distributed Systems: Principles and Paradigms, Upper Saddle River, NJ, Prentice-Hall, 2003.
27) [25] M. Singhal and N. Shivaratri, Advanced Concepts in Operating Systems, New York, McGraw Hill, 1994.

The Establishment of an AR-based Interactive Digital Artworks

GJCST Computing Classification I.3.7

Min-Chai Hsieh[1] Hao-Chiang Koong Lin[2] Jin-Wei Lin[3] Mei-Chi Chen[4]

***Abstract*-This work attempts to declare the background of personal contemporary state through an immersion of "digital vacancy". The work is stacked on the identical digital space with concurrent portrait and enjoyment. Moreover, the work describes the doubt and depression in life, combining with humor of predicament and absurdities of senses. We employ augmented reality to create digital artworks to present interactive poem. This work is established where the digital poem is generated via the interaction between a video film and a text-based poem. After establishing the digital artwork, we exhibited the digital work at Digital Art Center (DAC), Taipei, Taiwan. The audiences can interactive with digital poem in real time. In comparison to the other AR equipment, the cost of this work is quite low. In the future, some usability evaluation will be performed on this work.**

Keywords- Augmented reality, Digital artworks, Interactive poem.

I. INTRODUCTION

In the past, the artists present the creation of domain and private space. The most artworks are based on non-interactive visual creative expression. With the progress of information technology development, people can create art by using the digital multimedia rather than just doing in a traditional manner. That is, the way of art-creating has changed dramatically. Thus, the digital art creation becomes more lively and interesting. Furthermore, these materials/technologies enhance the artists' creativity. Artists are able to create artworks via technology and multimedia; that is to say, they can create artworks with the multimedia besides the traditional way of creating arts, so they can create in more fashions to express their thoughts. Today, the ideas of artists can be implemented in real time via the powerful computation abilities of various computers.

The process of artworks creation is charmingly. Because it no longer a phenomenon of the slice, but a manifestation of the experience. Interaction has been considered as an important characteristic of digital artworks. But the evolution of the aesthetic point of view is seldom mentioned. Participate in the experience during the construction is the significance of create all of the works. It formed the "interactive aesthetics" gradually. These are important concepts in new media art [1][2].

In "The End of Art", Arthur C. Danto said/mentioned that the function of art imitation and reappear has already disappeared. From now emphasizing that the verisimilitude imitation is also redefined in the art history [3]. The text should be opened to and created by the readers. The meaning of text is interpreted by the readers instead of the author. This is the well-known "writable text" concept [4].

In this work, we will employ Augmented Reality (AR) technology to create digital artworks to present a series of interactive poem. The audience can interact with the digital poem via pre-designed postcards. Notice that the postcard is real object, while the digital poem is virtual sight. Interestingly, the real lies in the virtual; vice versa, virtual scenes render in the real environment. Therefore, audience can feel themselves in an environment, both virtual and real.

II. RELATEDWORK

In recent years, many scholars and institutes have been carrying out the research on Augmented Reality, one of the techniques of computer vision application. AR is also called Mixed Reality (MR), the extension of Virtual Reality (VR). By setting up the scene via Computer Graphics, VR can simulate objects in the real world and create the environment where users can interact with the simulated objects. AR is the images, objects or scenes generated by the computer that blend into the real environment to strengthen our visual feelings. In sum, it adds virtual objects to our real environment. The technology has to possess three qualities, the combination of virtual objects and the real world, real time interaction, 3D space only.

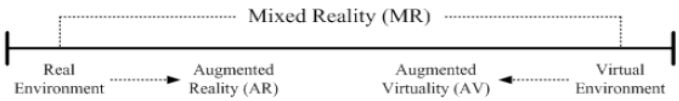


Fig.1. Reality and Virtuality(RV) continuum

Milgram et al. [5] treats the real environment and the virtual one as a closed union. We can find it in Fig 1. On the left side is merely real environment while on the right side is only virtual environment. VR is inclined to take place of the real world; AR is to augment the virtual image produced by the computer to the real environment. Presently, AR is being applied very extensively to such as education, medical technology, military training, engineering, industrial design, art, entertainment and so on [6][7][8][9][10][11][12].

AR combines virtual objects with the real environment and displays the virtual object generated by computers in front of users' eyes. Milgram et al. [5] defines two displaying ways of AR. One is See-Through AR. Users can directly see the surrounding environment through the monitor and the monitor also display the virtual image in it. Accordingly, the

About-[1] Dept. of Information and Learning Technology, National University of Tainan, Tainan, Taiwan.
(telephone: +886-6-2133111#771 email: shiehminchai@gmail.com)
About-[2]Dept. of Information and Learning Technology, National University of Tainan, Tainan, Taiwan.
(telephone: +886-6-2133111#771 email: koonglin@gmail.com)

effect of augmented environment can be the greatest via See-through AR. The other is Monitor Based AR. The computer combines the images captured by the webcam with the virtual images. The final image after combination will show up on Head Mounted Display (HMD) or computer monitor. There are two kinds of HMD, one is pure HMD and the other is HMD with a small webcam. The former has small volume and can be equipped with the head mounted tracking instrument, which can track the present angle as well as direction ahead of user's head. It is more suitable for research and application of AR. The latter has immersion effect.

III. Concept ofwork

This work attempts to declare the background of personal contemporary state through an immersion of "digital vacancy," the work is stacked on the identical digital space with concurrent portrait and enjoyment. The author allows the audience to generate engagement of ideas from past created videos and poetry using interactive media, which further pushes the audience to wonder what they are expecting and the kind of attention they involve in while waiting. Such as life, the crowd passes each other in the city, alternating and switching consciousness and predicament. Perhaps the image of dust generally contains an ingenious meaning due to naturally-born vision and wisdom; while the condensation of air, image and signs symbolize the endless vacancy. Perhaps the audience has fallen into a conventional mindset. Often times, the audience needs to think again before understanding the definition to his or herself.

Our thinking can be both naive and profound. Therefore, this work attempts to expand fragments of a series of identify from the phenomenology of inconspicuous things. The work describes the doubt and depression in life, combining with humor of predicament and absurdities of senses. We are the city wanderers who observe various surrounding symbols through constantly muttering without probing into its significance.

After we enter the kingdom of other dimension, we often start immersing in the beauty of ambiguity while thinking about the multilevel of possibility. Such pattern forms cognitive approach to reflect the nature and details of things, while estimating the length and scale of seemingly familiar yet strange surrounding sceneries, giving a little taste of such inspiration. As Claude Levi-Strauss said, "Our eyes have lost the ability to distinguish and we no longer know how to treat things." Subjective regularity helps us gain insight to streamer and freeze in true cleverness. Our creation no longer belongs to part of theories and we can unlimitedly slow down our pace.

IV. Digital poem

A system (written in the Processing programming language) is established where the digital poem is generated via the interaction between a video film and a text-based poem. In other words, the system acquires two kinds of inputs: (1) a video file which was produced by the artist before, and (2) a modem poem which was written by the artist. The poem consists of a sequence of Chinese characters. Fig. 2 is the transformation program written in Processing.

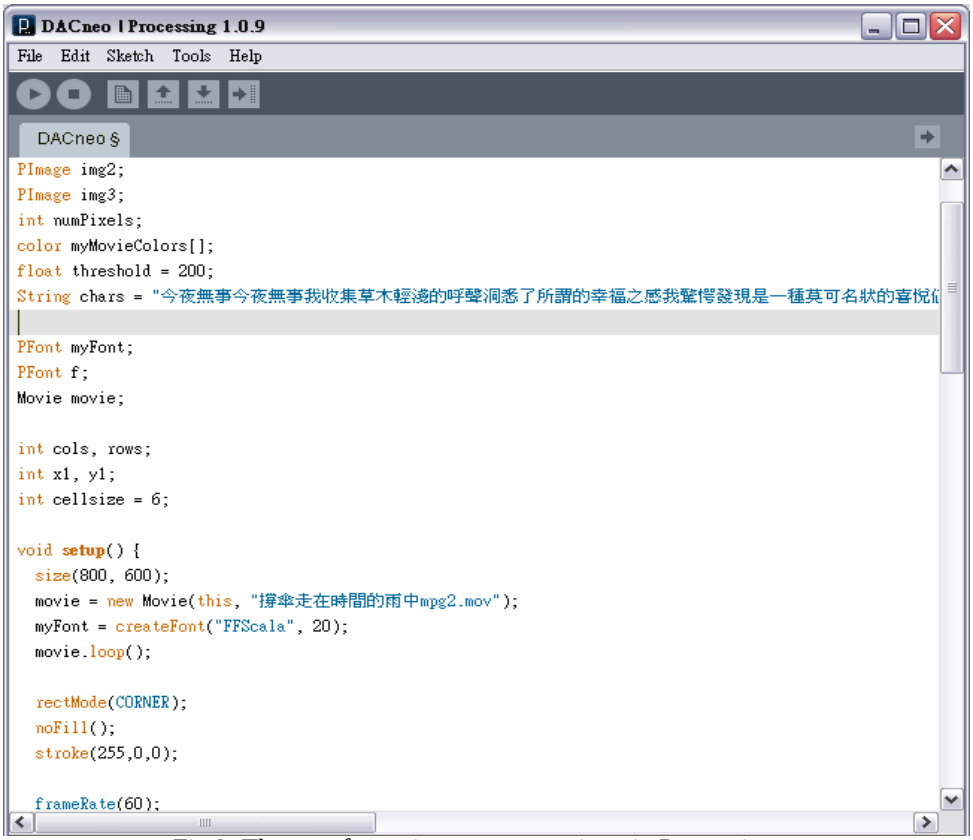


Fig.2. The transformation program written in Processing.

After these two inputs are fed to the system, each frame in the video is transformed to an image constructed by texts. The transformation process is depicted as follows. A "cell size" is defined in the program, and each cell contains several pixels, for example, four pixels. The number of the cell size determines the style of the resulting image. For each cell in the frame, we replace the content by the character in the poem. The orders for the characters to be applied depend on their positions in the poem.

Moreover, the color of the character is based on the color of the cell on the same position. Notice that the font size of the character can also be defined by the designer. Therefore, if the font size is larger than the cell size, characters on the image may overlap with each other's so that the colors will blur to embellish the frame to be "draw-like".

When all the frames are generated and be filled with colors via the above process, an interactive "digital poem" with a video form is thus produced. Fig. 3 is the video file before transformation, play with Quick Time. And Fig. 4 is the frame after transformation

Fig.3. The video file before transformation.

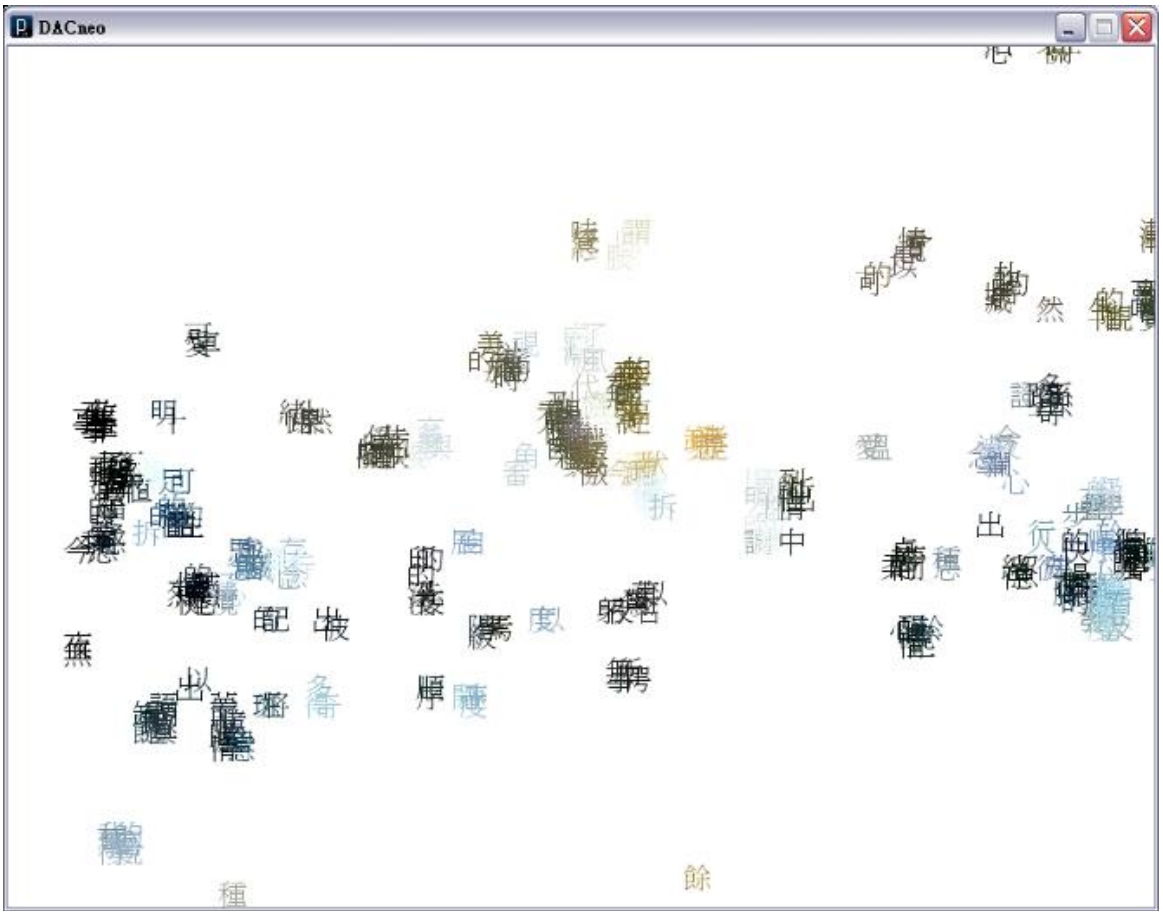


Fig.4. The frame after transformation (Pixels in this frame were replaced by texts in poem).

V. Implementation

We create digital artworks to present interactive poem by taking advantage of the Augmented Reality technology.

This work is implemented in Processing programming language and developed based on ARToolKit [13]. Figure 5 depicts the flowchart of digital poem presentation.

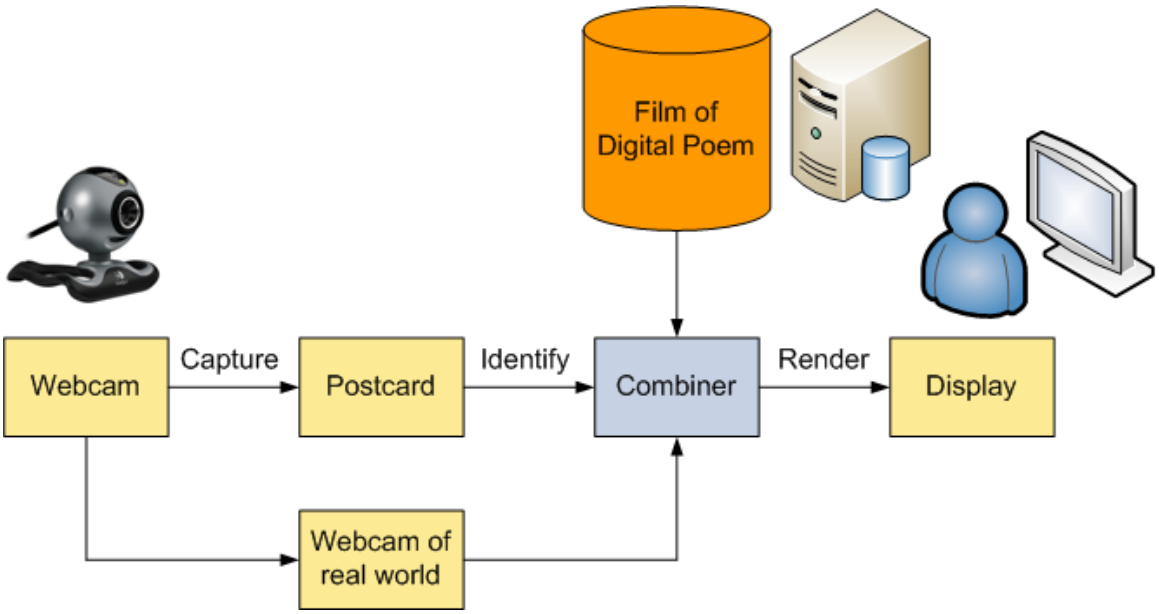


Fig.5. The flowchart of digital poem presentation

The webcam captures video of the real world and sends it to the computer. The system searches through each video frame for any square shapes of black color. If a square is found, the system uses some mathematics to calculate the position of the webcam relative to the black square. Once the position of the webcam is determined, a film of digital poem is drawn from that same position. This film of digital poem is drawn on top of the video of the real world and so appears stuck on the square marker. The final output is shown back, and displayed via the projector. Therefore, when the audience looks through the display they see film of digital poem overlaid on the real world.

Figure 6 shows the digital poem presentation based on our system written in Processing language. We create image textures and corresponding vertices. Then, the four vertexes of film will match the four ones of Image Texture and film will be drawn on the Image Texture. There are four vertices in Image Texture. They are expressed as vertex (x, y, u, v). The x is coordinate of the vertex, the y is coordinate of the vertex, the u is horizontal coordinate for the texture mapping and the y is vertical coordinate for the texture mapping.

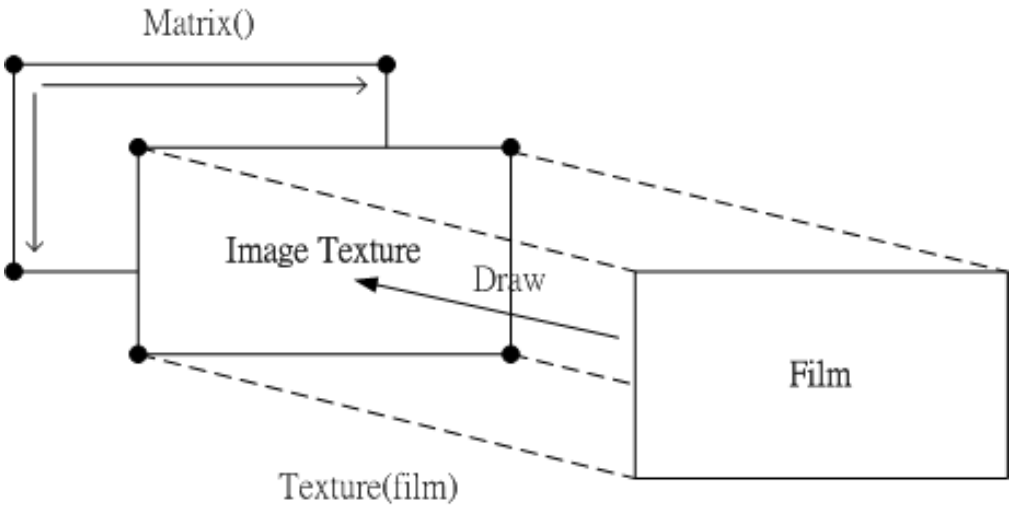


Fig.6. The film draws on image texture.

About the development environment, we use a PC with Pentium(R) Dual-Core 2.6GHz CPU, Logitech Orbit as the webcam, which captures 30 frames per second. The frame size is 640×480. The distance between the webcam and the postcard is 50 centimeters. The AR marker on postcard is 4.55 cm in length and width respectively.

The interactive content of the work contains video. Each poem from postcard matches a virtual digital poem. Then, the audience can interact with postcard by directly manipulating it. Figure 7 is the example of postcard. Each postcard corresponds to a video of digital poem. The total numbers of postcards and videos are both 12. Shown in figure 8 are all of the 12 postcards.

Fig.2. (1) The postcard of back is AR marker. (2) The postcard of front is poem


這只是我在弱勢團體中的一種姿態罷了


第二天
上演
的
情節


第二天上演的情節


無從界定


無從界定

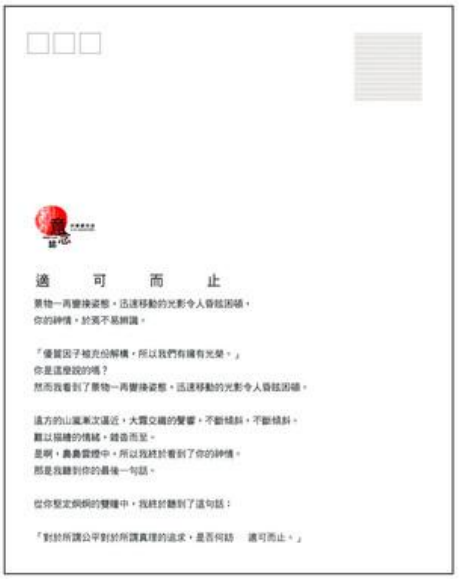
不該煽情

有些眼神，藏匿於解構後的心情中
無從重組。
所以夜色的身姿總是有些呆滯
所以翻不完的書頁　有凝重的破裂景趣。

強力搭建意念的圖騰。
所以拱凑出的所謂等寂
所以析辨出的所謂落寞
僅不足採信。

字句中的枯槁面容
不時為驚怖所吸引
揉揉我們的疲憊，折疊我們的憔悴
教唆那，錯綜疊疊的光陰
追逐冷冽的無形無數的氣息
夢囈式的抒情。

所以不該。



適　可　而　止

景物一再變換姿態，迅速移動的光影令人昏眩困頓，
你的神情，於焉不易辨識。

「優質因子被充份解構，所以我們有擁有光榮。」
你是這麼說的嗎？
然而我看到了景物一再變換姿態，迅速移動的光影令人昏眩困頓。

遠方的山嵐漸次逼近，大雲交織的聲響，不斷傾斜，不斷傾斜。
難以描繪的情緒，錯雜而至。
是啊，農農雲煙中，所以我終於看到了你的神情。
那是我聽到你的最後一句話。

從你堅定炯炯的雙瞳中，我終於聽到了這句話：

「對於所謂公平對於所謂真理的追求，是否何妨　適可而止。」

我，以及其他

邏輯羅於一夜風雨解構的格局中。
（其實不必對自己表達秘密而假釋那刺骨的寒。）

「一個人嗎？」
句法及語意皆適於觀諒，一時令我啞然無從回答。
「一個人嗎？」
口氣的佈局顯然鬱塞，我強口大笑
所有感覺都和我的聲帶制離。
是孤單麗，我想。

所以圍執，關於一切優柔寡斷及其他等等。
而忘了防範：夢遺後
疲憊與光榮般般跌落我錯裂糾結的思緒中，
而彼此排擠。

我們只能這麼說了。心靈角隅一端
優越與其突變的劣等基因
錯綜盤據在意識的刮面
我只能這麼說了
無須重組本質及無法為心情命名，
並且風雨纏繞。
如此而已。

不修邊幅

我甚至清對鏡相依的呼吸節奏都如此輕忽
其實並非漠視自己。
清澈照映自我之後的審慎付諸
決意將關心焦距全對準這綺麗景。

即便是十分認真地收藏了一罐子所有的遺憾與心碎
儘管哭時誰是如何地給氣雜音。

縞紵是否不修邊幅
於焉甚不重要。

停格之二

我的夢境。從內心的體形到最遠不可見的完整結構
諸多真誠而又模糊的想念
終於看見。綽綽於潔淨山澤中的芳蹤。
你來了

「然至此我仍尚未理清回憶與明日種種無關緊要的往事
　究竟牽扯著什麼或疏或密的關聯時，」(註一)
我靜待自己的睿智的甦醒。

所以我在這裏
所以你在那裏

(註一)：改編自田運良詩人之「生生：世苦」

中傷我吧

以曖昧的言語勾引你：
中傷我吧。
揮身而出的姿態是否與天氣有關　不用管
中傷我吧。

中傷我吧
藉此我厚衛心情
釋放繽紛的愉悅與憂傷。
中傷我吧
因為感動是不需要的　傷懷是不需要的
因為回憶是不需要的　珍惜是不需要的
摧毀所有鍵結吧
可以如同他們般　轉眼型圖的流光歲月。

而預期的話與不該
當它們擺躍欲試迫不及待想見識你的歡息不斷你的遇於晶瑩的夢
那麼將情何以堪。

所以，還是中傷我吧

Fig. 8. The total postcards

The element of presentation includes the webcam embedded to the lamp, reading-desk, projector and white wall in exhibition. Figure 9 is the presentation of artworks. There are several postcards on reading-desk and the lamp is installed at a higher position in order to present a broader view. The audience "read" the content of these poem by manipulating the postcards, so that the digital films "hidden" behind the AR markers will be displayed. The installation of this artwork is show in figure 10.

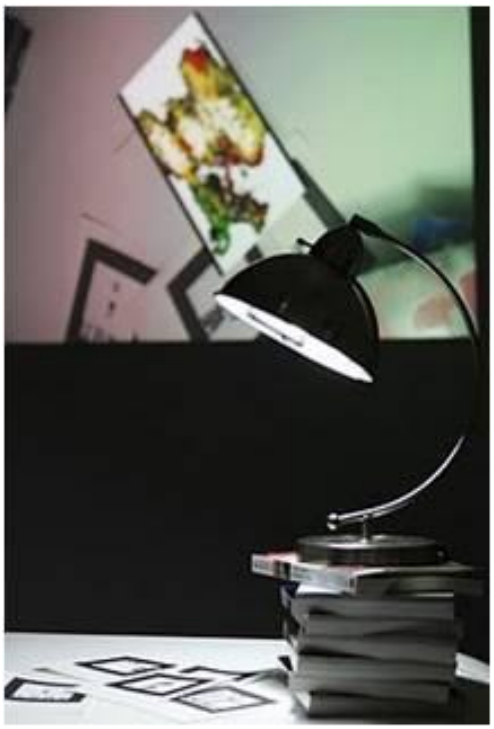


Fig.9. The presentation of artworks

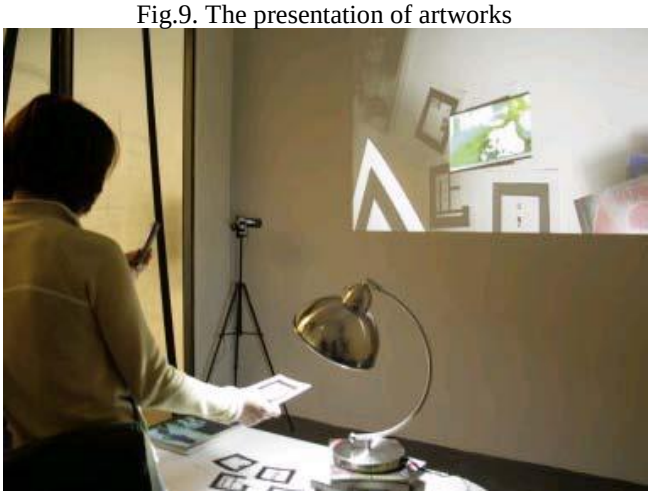


Fig.10. The audience interacts with AR digital poem..

VI. Conclusion

In this work, we employ augmented reality technologies to create digital artworks to present interactive poem. This artwork was exhibited in Digital Art Center, Taipei, Taiwan, and the exhibition duration is from March 6, 2010 to April 11, 2010. We will extend this work so that the audiences can interact with the AR digital poem via internet. The artwork setting and operation is easy. Audiences only need to set up a webcam, with no additional hardware requirement. In comparison to other AR equipment, the cost of this work is quite low. In the future, some usability evaluation will be performed on this work.

III. References

1) Lev, M. (2001). The Language of New Media. Massachusetts: MIT Press.
2) Kirk, V., and Gopnik, A. (1990). High and Low: Modern Art and Popular Culture. New York: Museum of Modern Art.
3) Oliver, G. (2003).Virtual Art. Massachusetts: MIT Press.
4) Zucker, S. D. (1997). The Arts of Interaction: Interactivity, Performativity and Computers, Journal of Aesthetics and Art Criticism (Special Issue on Art and Technology), 55(2), 17-127.
5) Milgram, P., and Kishino, F. (1994). A Taxonomy of Mixed Reality Visual Displays. IEICE Trans. Information Systems, E77-D(12), 1321-1329.
6) Azuma, R.(1997). A Survey of Augmented Reality. Presence: Teleoperators and Virtual Environments, 6, 355-385.
7) Azuma, R., Baillot, Y., and Behringer, R. (2001). Recent advances in augmented reality. IEEE Computers and Graphic, 21, 34–47.
8) Dünser, A., and Hornecker, E. (2007). Lessons from an AR book study. In: Proceedings of the First International Conference on Tangible and Embedded Interaction, 179-182.
9) Liarokapis, F., Petridis, P., Lister P.F., and White, M. (2002). Multimedia Augmented Reality Interface for E-learning (MARIE). World Trans. on Engineering and Technology Education, 1(2), 173-176.
10) Billinghurst, M., Kato, H., and Poupyrev, I. (2001). The MagicBook: A transitional AR interface. Computer and Graphic, 25, 745-753.
11) Kirner, C., and Zorzal, E.R. (2005). Educational applications of augmented reality collaborative environments. Proceedings of sixteenth Brazilian Symposium on Informatics in Education, 114-124.
12) Hsieh, M.C., and Lee, J.S. (2008). AR marker capacity increasing for kindergarten English learning. International Multiconference of Engineerings and Computer Scientists, 663-666.
13) Kato, H., Billinghurst, M., Blanding, B., and May, R. (1999). ARToolKit. Technical Report (Hiroshima City University).

AUTOCLUS: A Proposed Automated Cluster Generation Algorithm

Samarjeet Borah[1] Mrinal Kanti Ghose[2]

GJCST Computing Classification
I.5.3, I.4.6

***Abstract*-Among all kind of clustering algorithms partition based and hierarchical based methods have gained more popularity among the researchers. Both of the methods have their own advantages and disadvantages. In this paper an attempt has been made to propose a new clustering algorithm which includes the selected features of both of the algorithms. While developing the proposed methodology, emphasis has been given on some of the disadvantages of both categories of algorithms. The proposed algorithm is tested with various datasets and found satisfactory results**

Keywords-Clustering, Partition, Hierarchical, Automatic, Distance Measure.

I. Introduction

There is huge amount of data in the world and it is increasing day by day. Everyday new data are collected and stored in the databases. To obtain implicit meaningful information from the data the requirement of efficient analysis methods [1] arises. If a data set has thousands of entries and hundreds of attributes, it is impossible for a human being to extract meaningful information from it by means of visual inspection only. Computer-based data mining techniques are essential in order to reveal a more complicated inner structure of the data. Such techniques are the clustering solutions which help in extracting information from the large dataset

II. Clustering

Clustering [2][3][4] is a type of unsupervised learning method in which a set of elements is separated into homogeneous groups. Intuitively, patterns within a valid cluster are more similar to each other than they are to a pattern belonging to a different cluster. The variety of techniques for representing data, measuring similarity between data elements, and grouping data elements has produced a rich and often confusing assortment of clustering methods. Clustering is useful in several exploratory pattern-analysis, grouping, decision-making, and machine-learning situations, including data mining, document retrieval, image segmentation, and pattern classification [5][3]. Data clustering algorithms can be *hierarchical* or *partitional* [6]. Within each of the types, there exists a wealth of subtypes and different algorithms for finding the clusters

A. Partition Based Clustering Methods

Given a database of n objects, a partition based [5] clustering algorithm constructs k partitions of the data, so that an objective function is optimized. Partition based clustering algorithms try to locally improve a certain criterion. The majority of them could be considered as greedy algorithms, i.e., algorithms that at each step choose the best solution and may not lead to optimal results in the end. The best solution at each step is the placement of a certain object in the cluster for which the representative point is nearest to the object. This family of clustering algorithms includes the first ones that appeared in the Data Mining Community. The most commonly used are K-means [7], PAM (Partitioning Around Medoids), CLARA (Clustering LARge Applications) and CLARANS (Clustering LARge ApplicatioNS). All of them are applicable to data sets with numerical attributes.

B. Hierarchical Clustering Algorithms

Hierarchical algorithms can be agglomerative (bottom-up) or divisive (top-down). Agglomerative algorithms begin with each element as a separate cluster and merge them in successively larger clusters. Divisive algorithms begin with the whole set and proceed to divide it into successively smaller clusters. Hierarchical algorithms have two basic advantages [4]. First, the number of classes need not be specified a priori, and second, they are independent of the initial conditions. However, the main drawback of hierarchical clustering techniques is that they are static; that is, data points assigned to a cluster cannot move to another cluster. In addition to that, they may fail to separate overlapping clusters due to lack of information about the global shape or size of the clusters [8]. In hierarchical clustering, the output is a tree showing a sequence of clustering, with each cluster being a partition of the data set [9].

III. Automated Clustering (AUTOCLUS)

This work has been motivated by the issues mentioned above. Although the above algorithms are well established and quite efficient one but their particular drawbacks may affect the clustering result. For example, many of these algorithms require the user to specify input parameters where wrong input parameter may result in bad clustering. The algorithm AUTOCLUS has been proposed keeping some of the issues in mind faced in the above algorithms. It's a hybrid kind of algorithm which includes some features of both partition based and hierarchical based algorithms.

A. Proposed Methodology "Autoclus"

Let the data set be given as $\boldsymbol{X} = \{\boldsymbol{x_i}, \boldsymbol{i} = \boldsymbol{1}, \boldsymbol{2} \ldots \boldsymbol{N}\}$ which consists of N data objects $\boldsymbol{x_1}, \boldsymbol{x_2} \ldots \boldsymbol{x_N}$., where each object has *M* different attribute values corresponding to the *M*

*About-*Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology Majitar, Rangpo, East Sikkim-737136, India (e-mail;[1]samarjeetborah@gmail.com [2]mkghose2000@yahoo.com)*

different attributes. The value of *i*-th object can be given by:

$$\boldsymbol{X_i} = \{\boldsymbol{x_{i1}}, \boldsymbol{x_{i2}} \dots \boldsymbol{x_{iM}}\}$$

Let the relation $\boldsymbol{x_i} = \boldsymbol{x_k}$ does not mean that $\boldsymbol{x_i}$ and $\boldsymbol{x_k}$ are the same objects but that the two objects has equal values for the attribute set $\boldsymbol{A} = \{\boldsymbol{a_1}, \boldsymbol{a_2}, \dots, \boldsymbol{a_m}\}$. The main objective of the algorithm is to partition the dataset into *k* disjoint subsets where $\boldsymbol{k} \leq \boldsymbol{N}$. The algorithm tries to minimize the inter-cluster similarity and maximize the intra-cluster similarity.

B. Distance Measure

While searching a certain structure from given data sets, the important thing is to find an appropriate distance function. In this context the most important question is what should be the criterion for selecting an appropriate distance function. For distance calculation the distance measure sum of square Euclidian distance is used in this algorithm. It aims at minimizing the average square error criterion which is a good measure of the within cluster variation across all the partitions. Thus the average square error criterion tries to make the k-clusters as compact and separated as possible.

The algorithm combines the features of both hierarchical and partition based clustering. It creates a hierarchical decomposition of the given set of data objects. At the same time it tries to group the objects based on a mean value. It is a simple algorithm which applies a top-down or divisive approach. Initially all the objects of the dataset will be assumed as a single cluster. The algorithm applies an iterative process to divide the given dataset into a set of clusters until the termination condition converges. The classification is done based on the popular clustering criterion within-group sum of squared error (WGSSE) function.

$$WGSSE = \sum_{i=1}^{n} \sum_{j=1}^{M} \left(x_{ij} - \overline{x_i}\right)^2$$

The classical WGSSE function was originally designed to define the traditional hard c-means and ISODATA algorithms. With the emergence of fuzzy sets theory, Dunn [10] firstly generalized WGSSE to square weighting WGSSE function. Later, Bezdek [11] extended it to an infinite family of criterion functions which formed a universal clustering objective function of fuzzy c-means (FCM) type algorithms. The studies on criterion functions have mainly been focused on the measurements of similarity or distortion D (.), which are often expressed by the distances between the samples and prototypes. Different distance measurements are used to detect various structural subsets.

C. Phases of the Algorithm

The algorithm works in two different phases. One is the cluster generation phase and the other is the cluster validation phase. The various phases of the algorithm work as follows:

D. Cluster Generation Phase

This phase involves in the formation of new clusters by grouping the objects around a new mean value. The algorithm follows the reproduction process of amoeba, which is a tiny, one celled organism. Amoebas reproduce by binary fission. A parent cell divides the nucleus also divides in a process called fission and produces two smaller copies of it.

The same phenomenon has been followed here. A cluster will be divided into two smaller clusters selecting a new mean value. This new means value will be selected at the furthest Euclidian distance of the current mean. Then the rest of the objects will be redistributed among the two means (the old mean and the newly selected mean).

E. Cluster Validation Phase

This is the most important part of the algorithm. Whether the newly generated cluster is a stable cluster or not will be checked by this Cluster validation phase. Within group sum of square has been taken as the criteria for cluster validation. If the total WGSSE of the newly generated clusters is smaller than the parent cluster's WGSSE, then the clusters are valid. Otherwise the newly generated clusters will be discarded and the clustering process will be stopped here.

F. The pseudo code for AUTOCLUS

1. Take an initial data set D.
2. Compute Grand Mean: CALCULATE_GM(D).
3. Find the object with mean value closest to GM and call it Cluster_Head1.
4. Assign points to the cluster ASSIGN_PT (X, C)
   // $X = \{x_i, i = 1, 2 \dots N\}$,
   // $C = \{c_1, c_2 \dots c_k\}$ where $k \leq N$
5. SS := CALCULATE_WGSS (M, C).
   // $M = \{m_1, m_2 \dots m_k\}$where $k \leq n$
6. Repeat the following steps while WGSSE_of_Parent > $(Total\_WGSSE\_of\_Childs)$
   a. Obtain Euclidian Distance(ED) from all other objects to Cluster_Head1.
   b. Select the object at the largest Euclidian distance of Cluster_Head1.
   c. Name the object at largest distance as Cluster_Head2.
   d. Rename the Cluster_Head1 as Cluster_Head1.1
   e. Reassign objects around Cluster_Head1.1 and Cluster_Head2.
   f. Calculate WGSSE for the Cluster_Head1.1 and Cluster_Head2 (SS1 & $SS2$).
   g. If WGSSE_of_Parent > $(Total\_WGSSE\_of\_Childs)$ then the

child clusters will be accepted else discarded.

h. Go to step 6 and repeat the whole process for accepted new clusters.

IV. Implementation & Results

The algorithm has been implemented in C using a synthetic data set having 10 dimensions. The data set consists of real values including both positive and negative. It is almost similar to a gene expression data set. The program has different procedures for the implementation of various elements of the algorithm. For example the procedure compute_mean_grandmean() has been used to compute the grand mean of the dataset. Again the procedure wgsse_cal() has been used to calculate the within group sum of square of a cluster and computationss() has been used to generate the clusters. It's a top-down approach. The clusters that have been generated are uniquely identified by a cluster number. The numbering of the clusters have been done in such a way that the level of the cluster in the sub-tree can be found out from the number itself. For example 0 is the number assigned to the root of the tree, which is the cluster containing all the nodes of the dataset, 00 is assigned to the left sub-tree, 01 is assigned to the right sub-tree and so on. Applying the algorithm on the given dataset finally six clusters have been found. The tree of the clusters generated can be shown as below:

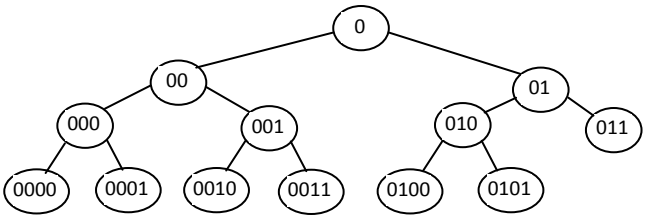


Fig 1: The Tree of the Clusters Generated by AUTOCLUS

A small portion of the result of AUTOCLUS is given in the following figure. The pair of centroids mentioned there are those which will be considered for the next decomposition of the cluster.

Cluster No. 0:
0 8.00 4.30 9.00 7.10 9.10 6.00 2.30) (2.00 5.00 11.00 88.00 3.00 5.00 66.00 22.00 7.77 4.30) (-3.00 9.00 -2.00 -4.00 0.90 5.00 6.00 1.00 1.10 4.50) (5.00 1.00 0.20 9.00 0.40 -8.00 -1.00 -4.00 -5.00 6.30) (8.00 9.00 2.00 1.00 6.00 -4.00 7.00 6.10 9.00 0.80) (9.00 7.80 9.00 6.10 -9.00 -3.00 0.50 8.00 9.00 -9.00) (-1.00 -3.00 6.00 7.00 3.00 3.00 5.70 55.50 32.50 -66.00) -->Centroid: (6.16 , 21.41)
Cluster No. 00:
(5.00 5.00 6.00 8.00 -9.00 4.40 22.00 8.50 7.70 4.00) (5.40 6.00 2.10 8.00 4.30 9.00 7.10 9.10 6.00 2.30) (-3.00 9.00 -2.00 -4.00 0.90 5.00 6.00 1.00 1.10 4.50) (5.00 1.00 0.20 9.00 0.40 -8.00 -1.00 -4.00 -5.00 6.30) (8.00 9.00 2.00 1.00 6.00 -4.00 7.00 6.10 9.00 0.80)
(9.00 7.80 9.00 6.10 -9.00 -3.00 0.50 8.00 9.00 -9.00) (-1.00 -3.00 6.00 7.00 3.00 3.00 5.70 55.50 32.50 -66.00) -->Centroid : (2.84 , 4.27)

Fig 2: Results from AUTOCLUS implementation

V. Conclusion

Partition based clustering algorithms face a problem that the number of partitions to be generated has to be entered by the user. Generally, algorithms of K-means family face this problem. As a result the clusters formed may not be upto mark. Because, it is difficult for a user to select the appropriate number of clusters without sound domain knowledge in prior. Again, hierarchical methods suffer from a fact that once a step (merge/split) is done, it can never be undone. This algorithm overcomes that problem. But it increases the computation cost because of the cluster validity process. In the development of the AUTOCLUS algorithm, it has been tried to minimize these drawbacks as much as possible. From the experiments it has been found that the algorithm is working properly with minimum user interaction. The number of clusters to be generated need not to be entered in prior. Again, in the cluster validation phase it can automatically accept or discard clusters based on the criteria function. The algorithm is tested with datasets of varying size and found satisfactory result.

VI. References

1) Yi Jiang, Efficient Classification Method for Large Dataset, School of Informatics, Guangdong Univ. of Foreign Studies, Guangzhou
2) Alexander Hinneburg, Daniel A. Keim, Clustering Techniques for Larges Data Sets from the Past to the Future,
3) A.K. Jain (Michigan State University), M.N. Murty (Indian Institute of Science) and P.J. Flynn (The Ohio State University), Data Clustering: A Review,
4) Lourdes Perez, Data Clustering, Student Papers, University of California San Diego, http://cseweb.ucsd.edu/~paturi /cse91/papers.html
5) Raza Ali, Usman Ghani, Aasim Saeed, Data ClusteringandItsApplications,http://members.tripod.com/asimsaeed/paper.htm,
6) Pavel Berkhin, Survey of Clustering Data Mining Techniques, Accrue Software Inc, San Jose, CA, (2002).
7) McQueen J.B. Some methods for classification and analysis of multivariate observations. In Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, volume 1, pages 281–297, Univ.of California, Berkeley, 1967. Univ.of California Press, Berkeley.
8) A.K. Jain (Michigan State University), M.N. Murty (Indian Institute of Science) and P.J. Flynn (The Ohio State University) Data Clustering: A Review.
9) I .Murtagh, A Survey of Recent Advances in Hierarchical Clustering Algorithms, Oxford Journals, The Computer Journal, Vol. 26, No. 4, pp. 354-359.
10) Dunn, J. C., A fuzzy relative of the ISODATA process and its use in detecting compact well separated cluster, J. Cybemet, 1974, 3: 32.
11) Bezdek, J. C., Pattern Recognition with Fuzzy Objective Function Algorithms, New York: Plenum Press, 1981

Implementing Search Engine Optimization Technique to Dynamic / Model View Controller Web Application

GJCST Computing Classification
D.2.11

R. Vadivel[1] Dr. K. Baskaran[2]

***Abstract*-the main objective of this paper is implementing the search engine optimization to dynamic web application / Model Viewer Controller web application. Implement the SEO concepts to both applications static and dynamic web application. There is no issue for create SEO contents to static (web contents does not change until that web site is re host) web application and keep up the SEO regulations and state of affairs. A few significant challenges to dynamic content poses. To overcome these challenges to have a fully functional dynamic site that is optimized as much as a static site can be optimized. Whatever user search and they can get information their information quickly. In that circumstances we are using few search engine optimization dynamic web application methods such as User Friendly URL's, URL Redirector and HTML Generic and few other SEO methods and concepts such as a crawler, an index (or catalog) and a search interface, search engine algorithms and page rank algorithms. Both internal and external elements of the site affect the way it's ranked in any given search engine, so all of these elements should be taken into consideration.**

Keywords-Search Engine Optimization (SEO), Model Viewer Controller (MVC), Dynamic web, Friendly URLs, ASP.Net

I. INTRODUCTION

If we have a website, we definitely need it to be a friend of search engines. There are several ways to attract visitors to our website, but in order to make searchers know about our website, search engine is the tool where we need to prove our contents. If we are just having a static HTML content, then there is no much problem in promoting it. But where in today's world of Content Managed Websites and eCommerce Portals we need to look further and implement a few more techniques in order to make the site more prominent to robots. In this article we will discuss how we can develop a SEO Friendly website where the content is driven from the Database with a Content Management System which is developed using ASP.NET. We will learn to build a simple CMS driven site with no nonsense URL, which Search Engines invite. Search Engine Optimization (SEO) is often considered the more technical part of Web marketing. This is true because SEO does help in the promotion of sites and at the same time it requires some technical knowledge – at least familiarity with basic HTML.

About-[1]Computer Science, Karpagam University Pollachi Road, Eachanari, Coimbatore, Tamilnadu India 641 024 (e-mail;vadivel.rangasamy@gmail.co)
About-[2]Asst. Professor (RD), Dept. of CSE and IT, Govt. College of Technology, Coimbatore – 641 006

SEO is sometimes also called SEO copyrighting because most of the techniques that are used to promote sites in search engines deal with text.

Generally, SEO can be defined as the activity of optimizing Web pages or whole sites in order to make them more search engine-friendly, thus getting higher positions in search results.

A Search Engine Optimization (SEO) is very popular term in web application industry. We can implement the SEO concepts to both applications static and dynamic web application. No matter for implement SEO to static web application. We have just followed up the SEO rules and conditions. We have to implement to dynamic / MVC web application it should be an insignificant complicate and use some tricky.

The specific objective is to implement search engine optimization for model 1 and model 2/Model Viewer Controller (MVC) dynamic web applications. There is no specified web technology in dynamic web applications. We can use any Microsoft or any other corporation software. In my work .NET has played major role.

To understand dynamic content, it's important to have an idea of its opposite, static content. The term static content refers to web content that is generated without using a data source such as a database. Essentially, the site viewer sees exactly what is coded in the web page's HTML.

With dynamic pages, a site can display the same address for every visitor, and have totally unique content for each one to view. For example, when I visit the social networking site Facebook (facebook.com), I see http://www.facebook.com/home.php as the address in my web browser, but I see a unique page that's different from what anyone else sees if they view that page at the same time. Thesite shows information about my friends in my account, and different information for each person in his account, or for someone who has no account.

Not all dynamically generated content is unique to every viewer, but all dynamic content comes from a data source, whether it's a database or another source, such as an XML file.

A. SEO in web application

A web application has playing most important role in the online business.

A million of static and dynamic web pages are available in the internet and million users can have used those web pages for their required information.

In this circumstances search engine optimization is play most important play between user and web applications.

In Million web pages are available the user should need their specific search criteria such as business man have search the own needs, students have search their own needs and etc.,

Our aim is whatever user search and they can get information their information quickly. In that situation we are using few search engine optimization methods and concepts such as a crawler, an index (or catalog) and a search interface, search engine algorithms and page rank algorithms.

Search engines take advantage of reverse broadcast networks to help save you time and money. Search allows you to "sell what your customers want, when they want it! ".

Search Engine Optimization is the science of customizing elements of your web site to achieve the best possible search engine ranking. That's really all there is to search engine optimization. But as simple as it sounds, don't let it fool you.

Both internal and external elements of the site affect the way it's ranked in any given search engine, so all of these elements should be taken into consideration. Good Search Engine Optimization can be very difficult to achieve, and great Search Engine Optimization seems pretty well impossible at times.

Optimization involves making pages readable to search engines and emphasizing key topics related to your content. Basic optimization may involve nothing more than ensuring that a site does not unnecessarily become part of the invisible Web (the portion of the Web not accessible through Web search engines).

II. Existing System

Previously SEO have implemented in static commercial / non-commercial web sites. In this way there is no dynamically site map and have not well-defined RSS feed for those implementations and there is no specific way to find the back links.

A. Dirty URLs

Complex, hard-to-read URLs are often dubbed dirty URLs because they tend to be littered with punctuation and identifiers that are at best irrelevant to the ordinary user. URLs such as http://www.example.com/cgi-bin/gen.pl?id=4&view=basic are commonplace in today's dynamic web. Unfortunately, dirty URLs have a variety of troubling aspects, including:

B. Dirty URLs are difficult to type

The length, use of punctuation, and complexity of these URLs makes typos commonplace.

C. Dirty URLs do not promote usability

Because dirty URLs are long and complex, they are difficult to repeat or remember and provide few clues for average users as to what a particular resource actually contains or the function it performs.

D. Dirty URLs are a security risk

The query string which follows the question mark (?) in a dirty URL is often modified by hackers in an attempt to perform a front door attack into a web application. The very file extensions used in complex URLs such as .asp, .jsp, .pl, and so on also give away valuable information about the implementation of a dynamic web site that a potential hacker may utilize.

E. Dirty URLs impede abstraction and maintainability

Because dirty URLs generally expose the technology used (via the file extension) and the parameters used (via the query string), they do not promote abstraction. Instead of hiding such implementation details, dirty URLs expose the underlying "wiring" of a site. As a result, changing from one technology to another is a difficult and painful process filled with the potential for broken links and numerous required redirects.

III. Related Works

There is a three technologies have been used that is 1. User Friendly URL's, 2. URL Redirector and 3. HTML Generic.

A Model View Controller has been used Microsoft .NET web application with ASP.NET and C#. In this application has used data model and business layer in separate module and its like a DLL (Dynamic Link Library) and we have started to created and converted dynamic URL's into Static URLs.

Fig 5 – Fig 8 is shows and implemented those technologies which are mentioned in early. The URLs converting code first we must grab the incoming URL and split the extension of the page. Which pages have ".html" extension we should redirect that page to related ".aspx" page on code behind they have executed business logic or data manipulation or whatever functionality need, and display to the end user exact content for that particular page with proper Meta description and keywords. In this time of period user can only view ".html" page but all other logics will execute the code behind.

A. Dynamic Content and SEO

SEO for dynamic content poses a few significant challenges. Luckily, you have ways to overcome these challenges to have a fully functional dynamic site that is optimized as much as a static site can be optimized. This section discusses the pitfalls of dynamic sites, and how to overcome them to create fully optimized dynamic sites.

B. Challenges for Optimizing Dynamic Content

Here are some common areas of dynamic sites that provide setbacks for humans as well as search engine spiders.

1) Dynamic URLs

A Dynamic URL is an address of a dynamic web page, as opposed to a Static URL, which is the address of a static web page. Dynamic URLs are typically fairly cryptic in their appearance. Here's an example from http://

www.financialadvisormatch.com/ article for a product called ***http://www.financialadvisormatch.com/article/product/B000FI73MA/ref=amb_link_7646122_1?pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-1&pf_rd_r=1FYB35NGH8MSMESECBX7&pf_rd_t=101&pf_rd_p=450995701&pf_rd_i=507846***

Notice that the URL doesn't contain any information about the item's product type, or anything about the item's name. For a well-trusted site like Amazon, this is not a problem at all. But for a new site, or for a site that's gaining credibility and popularity, a better solution can help search results by showing a searcher some relevant keywords in the page's URL. Here's an example of something a little more effective:

http://www.financialadvisormatch.com/article/products/electronics/kindle/

Kindle:

While search engines may not have problems indexing URLs with variables, it's important to note that highly descriptive URLs like the one just shown can get more clicks in searches than cryptic URLs.if searchers can clearly see keywords that have to do with the content they're looking for in your page's URL.

2) Logins and other forms

Login forms can restrict access to pages not only to users, but also search engines. In some cases, you want pages behind logins made searchable. In those cases, you can place code in those pages that determines whether the person visiting has access to view that content, and determine what to do from there.

```
protected void Page_Load(object sender, EventArgs e)
{
    _masterPage = (masterpages_Public)Master;
    _masterPage.IncludeGoogleMapsScript = true;

    //restrict the search engines
    if (!Page.Request.Browser.Crawler)
    {
        _masterPage.SetErrorMessage("Access denied.");
    }

    // check that this page is actually available in the implementation by checking the modules
    if (!_masterPage.Controller.IsSystemModuleAvailable(FirestarterController.ModuleNames.Companies))
    {
        Response.Redirect(_masterPage.Controller.Settings.Path + "pagenotfound.aspx");
    }

    // check if the company details should be visible to everyone
    if (null == _masterPage.Controller.UserSession && !_masterPage.Controller.Settings.CompanySearchVisibleToAll)
    {
        Response.Redirect(_masterPage.Controller.Settings.Path + "pagenotfound.aspx");
    }
    int companyID = 0;
    if (Request.QueryString["cid"] != null)
    {
        try
        {
            companyID = Convert.ToInt32(Request.QueryString["cid"]);
        }
        catch
        {
            // do nothing, will sort this out in the next statement
        }
    }
```

Fig – 1 Login and search engine validations

Other web forms, referring to content in <FORM> tags, can restrict access to pages as well. While Google has revealed that googlebot can go through simple HTML forms (see http://googlewebmastercentral.blogspot.com/2008/04/crawling-through-html-forms.html), not all search engines follow this same process, which means content hidden behind forms may or may not be indexed.

3) Cookies

Web cookies are small bits of data that are stored in a user's web browser. Cookies are used frequently on the Web for storing temporary data like shopping cart information or user

```
void SetCookie(FireStarterClassLibrary.Sessions.Session session)
{
    // create the cookie with the basic session data
    HttpCookie cookie = CommonFunctions.CreateSessionCookie(session, _masterPage.Controller.Settings.CookieName);

    // set the cookie
    Response.Cookies.Add(cookie);
}
```

Fig – 2 Add cookies with help of class library

preferences. Pages that require cookies can block spiders because spiders don't store cookies as web browsers do.

4)Session IDs

```
protected void Page_Load(object sender, EventArgs e)
{
    IFirestarterController controller = new FirestarterController(ConnectionString.Value);
    ISessionHandler sh = new SessionHandler(controller);

    string sessionID = Response.Cookies[controller.Settings.CookieName].Value;

    if(sessionID != string.Empty)
    {
        try
        {
            sh.SignOut(sessionID);
        }
        catch
        {
            // don't do anything, just don't puke
        }
    }

    Response.Cookies[controller.Settings.CookieName].Value = string.Empty;
    Response.Redirect("signin.aspx");
}
}
```

Fig – 3 Create a sessionid and store into database

Session IDs are similar to cookies in that if you need them to view pages, then spiders don't index those pages.

5) Hidden pages

Sometimes, pages on a website are hidden from search engines because they're buried too deep in a site's architecture. For example, a page more than three clicks deep from the home page of a website may not be crawled without an XML sitemap. Other pages that may be hidden include pages only visible via a site search.

1) JavaScript

```
<div class="Box">
    <div class="Head"><div class="TL"></div><div class="TR"></div></div>
    <div class="B"><div class="L">

        <div id="fstUserAvatar"></div>
        <script language="javascript" type="text/javascript">
            fst_GetUserAvatar();
        </script>

        <br />
        <div id="fstToolBox"></div>
        <script language="javascript" type="text/javascript">
            fst_GetToolBox();
        </script>

        <br />
        <RPNL:rightpanel ID="RightPanel" runat="server" />
        <asp:ContentPlaceHolder id="cphRightPanel" runat="server"></asp:ContentPlaceHolder>

    </div></div>
    <div class="Foot"><div class="BL"></div><div class="BR"></div></div>
</div>
```

Fig – 4 Include javascript into web form with master page

Search engines don't index content that requires full-featured JavaScript. Remember that spiders view content in much the same way as you would if you were using a browser with JavaScript disabled. Text that is created using JavaScript,

and therefore only accessible with JavaScript enabled, will not be indexed.

C. Ways to Optimize Dynamic Content

Dynamic content is often necessary in websites. In addition, content that is easily changed through an outside data source helps keep a site's content fresh and relevant. This increases its value to search engines. You don't need to worry that because your site is dynamic, your content won't be indexed. You just need to make sure you're following the appropriate guidelines when using dynamic content in order to keep your site optimized. Here are some things you can do to optimize your sites that contain dynamic content.

7)Creating static URLs

Dynamic URLs, especially dynamic URLs with vague names, can be a turnoff to searchers. In order to have friendly URLs, you want to rewrite your dynamic URLs as static URLs.

```
<%@ Application Language="C#" %>

<script runat="server">

    protected void Application_BeginRequest(Object sender, EventArgs e)
    {
        // grab the incoming http context
        HttpContext incoming = HttpContext.Current;
                              ]
        // grab the old path
        string oldpath = incoming.Request.Path.ToLower();

        // grab the name and extension of requested file
        string pageExtension = System.IO.Path.GetExtension(oldpath);

        // only try and rewrite the path if the incoming request is for an .html file (these are our "friendly" urls)
        if (pageExtension == ".html")
        {
            // assume paramArray[0] = 'firestarter'
            string baseDirectory = string.Empty;
            string newurl = string.Empty;
            string pageName = System.IO.Path.GetFileNameWithoutExtension(oldpath);
            string directoryPath = System.IO.Path.GetDirectoryName(oldpath).ToLower();
            string qString = Request.QueryString.ToString();
            string[] paramArray = directoryPath.Substring(1, directoryPath.Length - 1).Split('\\');

            // if www.365media.com/firestarter/blog... then set base param = 1
            // if www.365media.com/blog... then set base param = 0
            int offset = 1;
```

Fig – 5 Creating / converting dynamic into static web application (Coding Part I)

Blogs powered by wordpress or Blogger make it easy to convert dynamic links to static links. Blogger automatically creates static URLs, and with wordpress you need only a simple change in your settings. For wordpress, log in to your administrator account, and then, under Settings, click the Permalink button. From there, you simply select a static URL publishing method or create a custom one and save the changes. Nice!

```
// if I have a directory in the way then grab it
if (offset > 0)
{
    baseDirectory = paramArray[offset - 1].ToLower();
}

// ok, the base parameter will tell us what is being requested..
switch (paramArray[offset].ToLower())
{
    case "articles":
        if (pageName == "index")
        {
            newurl = "\\articles\\view\\index.aspx";
        }
        else if (pageName.IndexOf("_") > -1)
        {
            newurl = "\\articles\\view\\view.aspx?a=" + pageName.Substring(0, pageName.IndexOf("_"));
        }
        else
        {
            newurl = "pagenotfound.aspx";
        }

        break;
```

Fig – 6 Creating / converting dynamic into static web application (Coding Part II)

If your site isn't powered by a blogging application, you need to rewrite the URLs manually. The process is somewhat complex, and it requires modifying your .htm access file. Because modifying your .htm access file can cause permanent changes to your website, you want to either practice on a testing server or know exactly what you're doing before using these techniques on a production server. To test this process on a testing server, you can download and install a testing server (discussed in Chapter 4), and then download all or part of your website to your computer. That way, changes you make on your local computer don't affect your live site.

```
    else
    {
        string blogID = paramArray[offset + 1].ToString();
        if (pageName.IndexOf("_") > -1)
        {
            newurl = "\\blogs\\view\\viewpost.aspx?b=" + blogID + "&p=" + pageName.Substring(0, pageName.IndexOf("_"));
        }
        else
        {
            newurl = "\\pagenotfound.aspx";
        }
    }
    break;

case "forum":
    // need to get conversations

    // if it's pointing to default.html then just show the topics
    if (pageName == "index")
    {
        newurl = "\\forum\\index.aspx";
    }
    else if (paramArray.Length == (offset + 1) && pageName != "index")
    {
        // want to view a forum
        newurl = "\\forum\\viewforum.aspx?f=" + pageName;
    }
    else if (paramArray.Length == (offset + 2) && pageName != "index")
    {
        // want to view a forum but we're paging
        newurl = "\\forum\\viewforum.aspx?f=" + pageName + "&pg=" + paramArray[offset + 1].ToLower();
    }

    break;
```

Fig – 7 Creating / converting dynamic into static web application (Coding Part III)

```
case "blogs":
    // need to get blog
    // ok, so are we viewing a) the blog b) archive or c) post?
    // this is where the parameter count comes in handy..

    // viewing the blog itself
    if (pageName == "index" && paramArray.Length < 3)
    {
        newurl = "\\blogs\\view\\index.aspx";
    }
    else if (pageName == "index" && paramArray.Length > 2)
    {
        string blogID = paramArray[offset + 1].ToString();
        newurl = "\\blogs\\view\\view.aspx?b=" + blogID;
    }
    else if (paramArray.Length > offset + 2)
    {
        // i know that the blog id will be the second param
        string blogID = paramArray[offset + 1].ToString();
        // either viewing an archive or the blog post itself
        if (paramArray[offset + 2].ToLower() == "archive")
        {
            // viewing an archive month
            newurl = "\\blogs\\view\\archive.aspx?b=" + blogID + "&yr=" + paramArray[offset + 3].ToLower() + "&m=" + pageName;
        }
        else
        {

        }
    }
```

Fig – 8 Creating / converting dynamic into static web application (Coding Part IV)

8). Optimizing content hidden by forms

The fact that web forms can hide content can be a good thing, but sometimes forms hide content you may not want hidden. Login forms (forms that require a user name and password) can potentially block search engines if a login form is the only way to access that information. Of course, sometimes this feature is intentional, like for protecting bank account information on a banking site. For non-login forms, assuming that search engines index content that's accessible only by filling out text fields or other form elements is dangerous. Further, it's equally dangerous to assume that search engines don't index content that's accessible only via non-login forms. If you want your form's hidden content to be indexed, make sure to give access to it in ways other than through a form alone. If you don't want the content to be indexed, make sure to hide it from search engines via robots.txt, or some other method.

Typically, content that's viewable only after a user is logged into an account isn't necessary to index. If you have content that you want indexed hidden in a login-only area, consider taking that content out of the restricted area so it can be indexed.

IV. Results

Successfully implemented search optimization in model viewer controller web application with help of those technologies. Here show the few mock-up screen shots.

Fig – 9 has been displayed "ASPX" page of the blog / forum / articles.

Fig – 10 has searched the specific keywords in google search engine and showed results for that "ASPX" blog / forum / articles.

Fig – 11 and 12 has show that blog / forum / articles in HTML format.

Hence we have successfully implemented Search Engine Optimization technique for model view controller web application

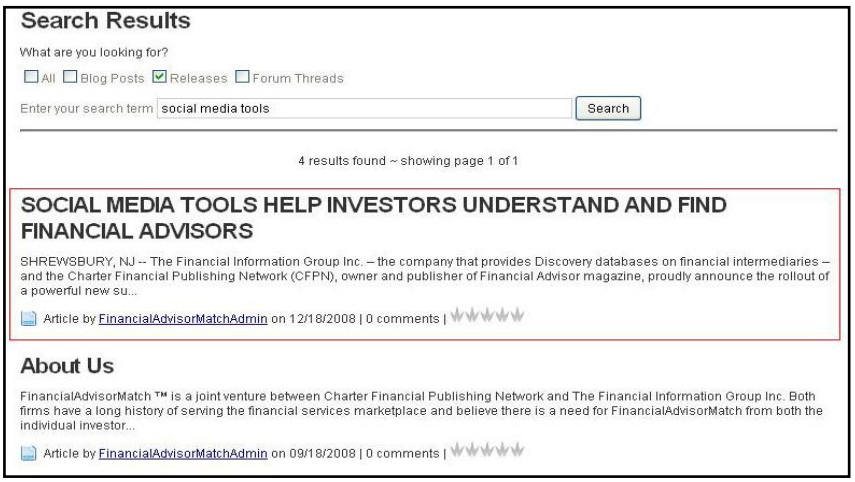


Fig – 9 ASPX page for article/forum/blog

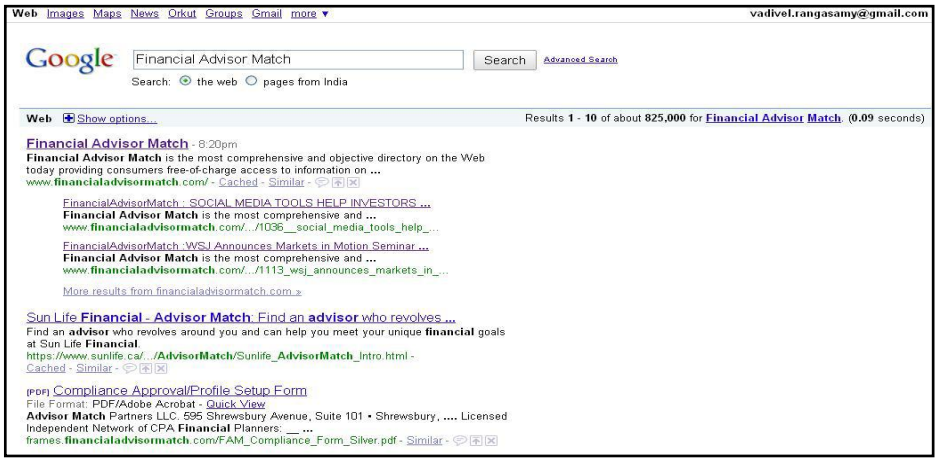


Fig – 10 Search keywords to google

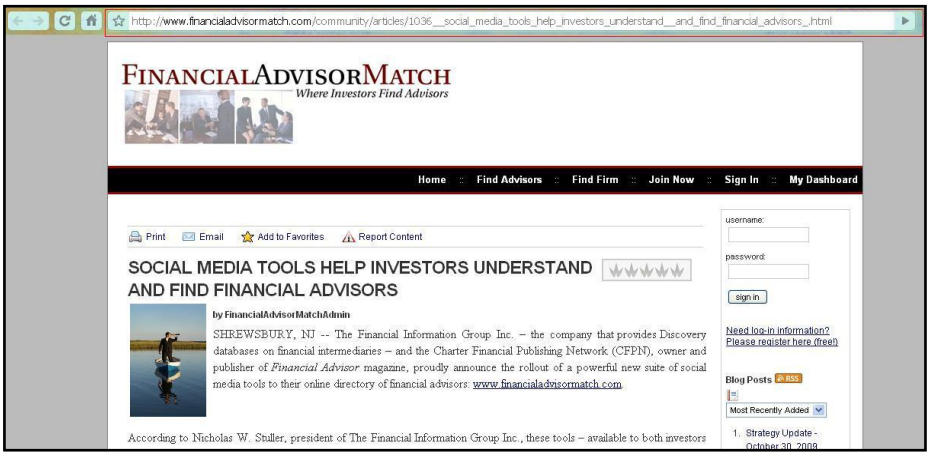


Fig – 11 Search results from google (Results – I)

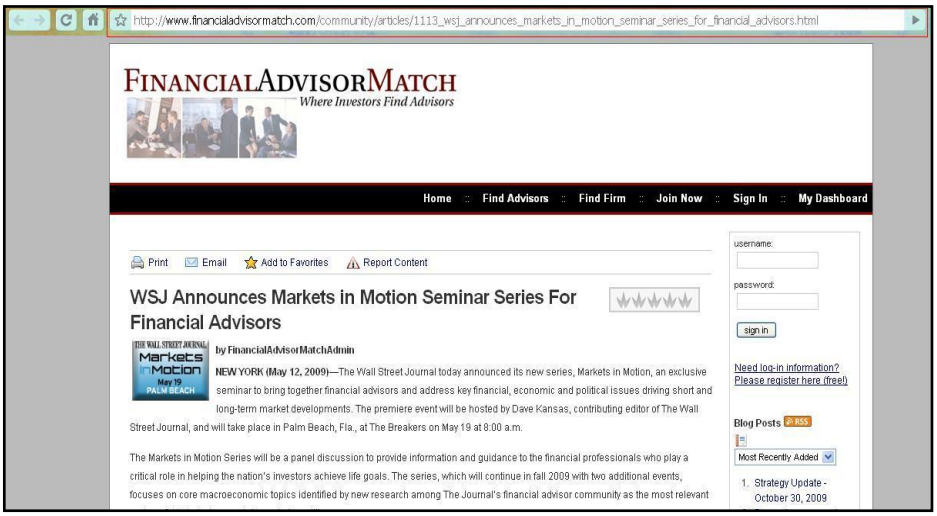


Fig – 12 Search results from google (Results – II)

V. Conclusions

A Search Engine Optimization has been implemented in dynamic web application. It has been used MVC web application and their techniques such as URL Redirector, HTML Generic, .NET security tools. The proposed is implementing the multiple query searches and personalized concept based clustering.

Most of the tips presented here are fairly straightforward, with the partial exception of URL cleaning and rewriting. All of them can be accomplished with a reasonable amount of effort. The result of this effort should be cleaned URLs that are short, understandable, permanent, and devoid of implementation details. This should significantly improve the usability, maintainability and security of a web site. The potential objections that developers and administrators might have against next generation URLs will probably have to do with any performance problems they might encounter using server filters to implement them or issues involving search engine compatibility. As to the former, many of the required technologies are quite mature in the Apache world, and their newer IIS equivalents are usually explicitly modelled on the Apache exemplars, so that bodes well.As to the search engine concerns, fortunately, Google so far has not shown any issue at all with cleaned URLs. At this point, the main thing standing in the way of the adoption of next generation URLs is the simple fact that so few developers know they are possible, while some who do are too comfortable with the status quo to explore them in earnest. This is a pity, because while these improved URLs may not be the mythical URN-style keyword always promised to be just around the corner, they can substantially improve the web experience for both users and developers alike in the long run.

VI. Reference

1) Kenneth Wai-Ting Leung, Wilfred Ng, and Dik Lun Lee, “Personalized Concept-Based Clustering of Search Engine Queries”, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 20, NO. 11, NOVEMBER 2008
2) AARON MATTHEW WALL,”Search Engine Optimization”, JUNE 2008
3) Ernest Ackermann & Karen Lartman, “The information Specialist Guide to Searching & researching on the Internet and World Wide Web”, Fitzroy Dearbon Publishers, 1999.
4) R.Elmasri and S.B. Navathe, “Fundamentals of Database Systems”, 2nd Edition, Menlo Park, CA: Addison- Wesley 1994.
5) Jeff Ferguson, Brian Patterson, Pierre Boutquin “ C# Bible”, John Wiley and Sons, June 2002
6) Wei Meng Lee, “C#.net Web Developer's Guide”, Syngress, January 1970
7) Jose Mojica, C# Web Development for ASP.NET, Peachpit Press, March 2003
8) http://www.macronimous.com/ 2009
9) http://www.seochat.com/ 2009
10) http://www.webtop.com.au/seo 2009
11) http://www.seocompany.ca/seo/seo-techniques.html
12) http://searchengineland.com/21-essential-seo-tips-techniques-11580
13) http://msdn.microsoft.com/en-us/library/ms972974.aspx

Eye detection in video images with complex Background

GJCST Computing Classification
I.4.8, I.4.6

M.Moorthi[1] Dr. M.Arthanari[2] M.Sivakumar[3]

***Abstract*-Detection of human eye is a significant but difficult task. This paper presents an efficient eye detection approach for video images with complex background. The propose method has two main phases to find eye pair such as locating face and eye region and finding eye. In the first phase the novel approach to fast locating the face and eye region is developed. In the second phase eye finding directed by knowledge is introduced in detail. Both phases developed using Mat lab 7.5. The proposed method is robust against moderated rotations, clustered background, partial face occlusion and glass wearing. We prove the efficiency of our proposed method in detection of eyes complex background i.e. both indoor and outdoor environment.**

Keywords-Face recognition, Facial features extraction, Eye detection

I. INTRODUCTION

Detection of eye is a crucial aspect in many useful applications ranging from face recognition and face detection to human computer interface design; model based video coding, driver behavior analysis, compression techniques development and automatic annotation for image data bases etc. By locating the position of the eyes, the gaze can be determined. A large number of works have been published in the last decade on this subject of which the effectiveness are not satisfied due to the complexity of the problem. Yet an efficient and accurate method is to be found. Generally the detection of eyes is done in two phases: locating face to extract eye regions and then eye detection. The face detection problem has been faced up with different approaches: neural network, principal components, independent components, and skin color based methods. Recently, methods based on boosting have become the focus of active research. The eye detection is done in the face regions which have been already located [1], [2], [3]. Little research has been done, however, on the direct search for eyes in whole images. Some approaches are based on active techniques: they exploit the spectral properties of pupil under near IR illumination. For example, in [4] two near infrared multiple light sources synchronized with the camera frame rate have been used to generate bright and dark pupil images. Pupils can be detected by using a simple threshold n the difference between the dark and the bright pupil images. In [5], iris geometrical information is used for o determining a region candidate that contains an eye in the whole image, and then the symmetry is used for selecting the pair of eyes. Although the detection rate is high, the assumption that the distance between the camera and the person does not change greatly limits its practical applicability.

In this paper, a knowledge-based algorithm for eye detection is presented. Knowledge guided eye contour searching effectively improves the system accuracy. The so called regional image processing techniques are also used both in the preprocessing step and in the detection algorithm itself. They can reduce the influence caused by the illumination variations in the small region. Since the processing algorithms in the second step only apply in the regions of small size, the efficiency of the system is improved.

This paper is organized as follows. Literature surveys are given in section 2. In section 3 we will devote ourselves to discussing the knowledge-based eye detection method in detail. Experimental results are reported in section 4. Conclusions will be drawn in section 5.

II. LITERATURE SURVEY

Pitas et. al. [8] uses thresholding in HSV color space for skin color extraction. However, this technique is sensitive to illumination changes and race. Ahuja et. al. [9], model human skin color as a Gaussian mixture and estimate model parameters using the Expectation Maximization algorithm. Yang et. al. [10] proposes an adaptive bivariate Gaussian skin color model to locate human faces. Baluja et. al. [13] suggests a neural network based face detector with orientation normalization. Approaches such as this require exhaustive training sets. Huang et. al. [11] perform the task of eye detection using optimal wavelet packets for eye representation and radial basis functions for subsequent classification of facial areas into eye and non-eye regions. Rosenfeld et. al. [12] use filters based on Gabor wavelets to detect eyes in gray level images. Pitas et. al., [8] adopt a similar approach using the vertical and horizontal relief for the detection of the eye pair requiring pose normalization. Feng et. d. [13] employ multi cues for eye detection on gray images using variance projection function. However, the variance projection function on a eye window is not very consistent. Compadelli et.al.[6] propose a binary template matching to find the feature image, searching for the two eyes .However this method can not deal with large out plane face rotation because the structure of the eye region changes.

About-[1] Assistant Professor, Department of computer Applications, Kongu Arts and Science College, Erode – 638 107, Tamil Nadu, India, phone:9842645643 (e-mail: moorthi_bm_ka@yahoo.com)
About-[2] Prof. & Head, Tejaa Sakthi Institute of technology for Women, Coimbatore – 641 659, (e-mail:arthanarimsvs@gmail.com)
About-3 Doctoral Research Scholar, Anna University,Coimbatore, (e-mail: sivala@gmail.com)

III. PROPOSED METHOD

Detection of the human eye is a very difficult task because the contrast of the eye is very poor. Under this situation, a good edge image is not to be obtained. However, it is found that some eye marks have relatively much higher contrast, such as the boundary points between eye white and eyeball. Besides this, eyes also have good symmetric characters. These marks can be used as knowledge to find the eye.

The propose method has two main phases to find eye pair such as locating face and eye region and finding eye. In the first phase the novel approach to fast locating the face and eye region is developed. In the second phase eye finding directed by knowledge is introduced in detail. The proposed method is robust against moderated rotations, clustered background, partial face occlusion and glass wearing. This is discussed one by one in the following section.

A. Face locating

Detecting the locations of human face in a scene is the first step in the face recognition system. In this step the region of the face candidate is roughly estimated using histogram thresholding technique. To simplify segmentation we assume that there is only one face in the image and is to be located. The binary image *B* (x, *y)* consists of all active pixels which include eye features. Histogram smoothing and automatic thresholding techniques are employed in this stage to eliminate the noises in the image and select the threshold.

B. Eye region extracting

The purpose of this stage is to roughly extract the eye region, which encloses two eyes from the face. The next eye detecting algorithm then will be applied only on this region. It therefore improves the efficiency of the system. The eye region extraction has the following steps:

1) Find the hair region from the binary image.

2) Identify the lower boundary of the hair region. The left and right ending points are denoted by; ledge and redge, respectively. The eye region is enclosed by ledge and redge called as *E*.

3) Find a pair of dark areas in E that may represent the locations of the eyes. This pair of dark areas should satisfy the following conditions:

i**.** Eyes are situated on the line that is parallel to the line joining ledge and redge.

ii. Eyes are symmetric with respect to the perpendicular bisector of the line .

iii. Eyes are situated below the eyebrows.

Then the eye region can be extracted from the image.

C. Eye detection

As in the image processed through the first step part of the eye information may have been lost, original eye region image is used at this second stage. It can be obtained by applying the eye region coordinates extracted from previous section 3.1 and 3.2 to the original face image. Eye detection has the following two steps.

D. Preprocessing

In an ordinary face image, the contrast of the eye region is usually relatively weak. Laplacian operator is used in this stage to enhance the contrast at edges. As this preprocessing is applied directly in the eye region based on the image situation in it, the edge information becomes more prominent.

E. Knowledge-oriented edge detection

The eye region image which is processed by Laplacian operator is sensitive to the edge. Automatic thresholding to this image can conserve most of the edge information. Edge detection has the following steps.

1) Locate big dark areas as the iris candidates using the following properties on a right eye pattern:

i. The two dark areas have the similar area;

ii. The line passing through the centre of the two dark areas is approximately

Parallel to the image x axis; and

iii. The two dark areas are ellipse shaped.

2) Find the top and bottom points of each iris. Let the pointes are called (topx, topy) and

(bottom,bottomy), respectively.

3) Find the upper eyelid is staring from (topx, topy) towards left part and right part of eyelid respectively using slop calculation. Apply the following knowledge to determine whether the last point is corner points.

The distance between two corners is larger than that between the points (topx, ropy) and (bottom, bottomy); and

Two corners are not lower than (bottomx ,bottomy).

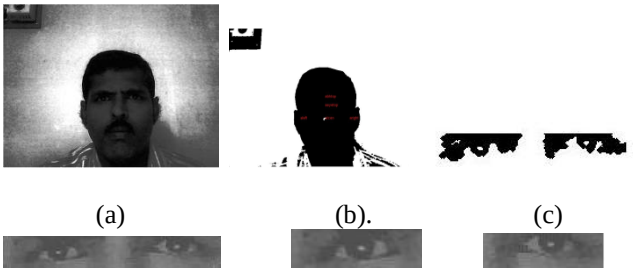
5) Find lower eyelid ie. Illumination variation usually has greater effect to the lower eyelids than to the upper eyelids. This makes the above algorithm not so effective to detect the low eyelids. However as the eye corners and points (bottomx, bottomy) have been known, a Parabola which passes through the three points for each eye can be found to approximate each lower eyelid.

IV. EXPERIMENTAL RESULTS

The proposed method was tested on the real video images. The video image of [480 x 640 pixels] of 75 different test persons and has been recorded during several sessions at different places. This set features a larger variety of illumination, background and face size. It stresses real world constraints. So it is believed to be more difficult than other datasets containing images with uniform illumination and background. The eye pair can be selected successfully in most cases, no matter whether face patterns are in different scale, expression, and illumination conditions. The eye location rate is 93.3%. Typical results of eye detection with the proposed approach are shown in Fig.2, 3. The input images vary greatly in background, scale, expression and illumination, the images also including partial face occlusions and glasses wearing. The correct judgment rate testing is shown in Fig 1and the results shown in Fig 2..

Algorithm	Test Scenario	Sample Number	Correct Judgment	%	Mean false alarm Rate
Binary Template Matching	Day	75	68	90.67	2%
	Night	50	40	80.00	
	Uniform Background	75	69	92.00	
	Complex Background	75	64	85.33	
Proposed Method	Day	75	70	93.33	1%
	Night	50	43	86.00	
	Uniform Background	75	70	93.33	
	Complex Background	75	67	89.33	

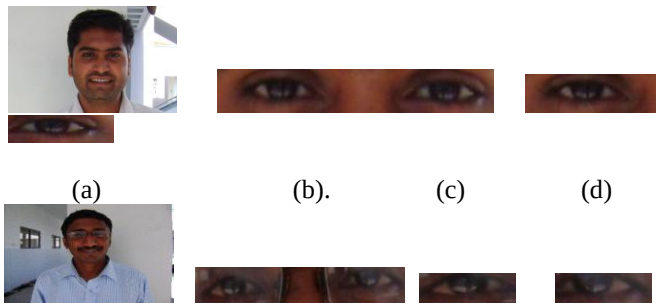
Fig.1: Correct Judgment Rate testing



(a) (b). (c)

(d) (e) (f)

Fig 2: Real Image capture from video using web camera (a). Original Image. (b) Binary Image. (c.) Detection of binary eye.(d) both eyes (e) Left eye. (f) Right eye.



(a) (b). (c) (d)

(a) (b). (c) (d)

Fig 3. Results using digital camera. (a). Original Image. (b) Both eyes (c) Left eye.
(d) Right eye

V. Conclusion

Fig 3. Results using digital camera. (a). Original Image. (b) Both eyes (c) Left eye.
(d) Right eye

In this paper, an efficient method for detecting eyes in video images with unconstrained background is presented. To obtain eye, the preprocessing is applied to input images. Homomorphic filtering is applied to enhance the contrast of dark regions; therefore, facial images with poor contrast are enhanced. Eye pairs are extracted by using knowledge oriented eye detection technique. The proposed method can deal with glasses wearing and partial face occlusions. However, the eye detection will fail if the reflection of glasses is too strong. If the reflection of glasses is too strong, the eyes can not be extracted. Closed eyes will not influence the results of eye location. The advantage of this method is that its computational cost is very low. The eye form is then searched based on the knowledge. Regional image processing techniques are also used in this paper to enhance the edge details. They improve the reliability of the system. The whole system has been successfully applied to eye form searching and the results are promising

VI. References

1) T. Kawaguchi and M. Rizon , "Iris detection using intensity and edge information," Pattern Recognition, vol. 36, pp. 549–562, 2003.
2) S. Baskan M. Bulut and V. Atalay, "Projection based method for segmentation of human face and its evaluation", Pattern Recognition Letters, Vol. 23, pp. 1623–1629, 2002.
3) S. Sirohey, A. Rosenfiled, and Z. Duric, "A method of detection and tracking iris and eyelids in video," Pattern Recognition, vol. 35, pp. 1389–1401, 2002.
4) A. Haro, M. Flickner, and I. Essa, "Detecting and tracking eyes by using their physiological properties, dynamics, and appearance," in Proc. IEEE Conf. computer Vision and Pattern Recognition, vol. 1, pp. 163– 168, 2000.
5) T. D'Orazio, M. Leo, G.Cicirelli, and A. Distante, "An algorithm for real time eye detection in face images," in Proc. 17th Int. Conf. on Pattern Recognition, vol. 3, pp. 278–281, 2004.
6) P. Campadelli and R. Lanzarotti, "Localization of facial features and fiducial points," in Proc. Int. Conf. Visualization, Imaging and Image Processing, pp. 491–495, 2002.
7) H. Rowley. S. Baluja. and T. Kanade. "Neural Network Based Face Detection," Proc., lEEE Conf. on Computer vision and Pattern Recognition. San Francisco, CA, 1996, 203-207.
8) K. Sobattka and I. Pitas, "A Novel Method for Automatic Face Segmentation. Facial Feature Extraction and Tracking," Signal Processing: Image Communication, 12(3) 1998, 263-281.Ming-Hsuan Yang and Narendra Ahuja, "Detecting Human
9) Faces in Color Images," Proceedings of IEEE Int'l conf on Image Processing, Chicago, IL, 1998, 127-1 30.
10) Jie Yang, Weier Lu and Alex Waibel, "Skin Color Modeling and Adaptation", Proceedings of ACCV'98 (tech report CMU-CS-97-146, CS dept, CMU 1997).

11) Jeffrey Huang and Harry Wechsler, "Eye Detection Using Optimal Wavelet Packets and Radial Basis Functions", International Journal of Pattern Recognition and Artificia1 Intelligence, Vol. 13, No 7, 1999.
12) S. A. Sirohey and Azriel Rosenfeld, "Eye detection in a face image using linear and nonlinear filters", Pattern I. Recognition. Vol. 34, 2001, 1367-1391.
13) Guo Can Feng and Pong C. Yuen, "Multi-cues eye detection on gray intensity Image", Pattern Recognition. Vol. 34, 2001, 1033-1046

Multi-Layer User Authentication Approach For Electronic Business Using Biometrics

Machha. Narendar[1] M.Mohan Rao[2] M.Y.Babu[3]

GJCST Computing Classification
K.6.5, D.4.6

***Abstract*-With the increased awareness of the dangers of cyberterrorism and identity fraud, the security of information systems has been propelled to the forefront as organizations strive to implement greater access control. Access control for information systems is founded upon reliable user authentication, and the predominant form of authentication remains the username-password combination. There are several vulnerabilities associated with an over-reliance upon this method of authentication, stemming from weaknesses in both the user construction of passwords and single-layer authentication techniques. The growing number of Internet business transactions highlights the need for a more secure method of user authentication that is cost-effective as well as practical. A multi-layer user authentication scheme is proposed as a solution, incorporating the use of dynamic biometric data selection and a timestamp to guard against reuse of intercepted authentication bit streams.**

I. Introduction

Computer-based information systems are becoming increasingly vital to the su ccess of many businesses. As organizations move to adapt to the digital era, the quantity of confidential and sensitive data stored in electronic form on computers continues to increase at a blinding pace. The growing trend in customer relationship management and the need to offer personalization through customized information further adds to the wealth of data contained in these information systems. Since the compromise of the sensitive data stored in information systems can be disastrous for an organization, the security of these systems is of utmost concern. Given that "practically every penetration of a computer system, at some stage, relies on the ability to compromise a password" it seems rather surprising that passwords continue to form the basis of user authentication methods. In the password-based scheme, users of the information system are required to enter a username password combination. The username establishes the identity of an individual as a valid user, and the password serves to confirm that identity and provide access to authorized resources. Passwords are inherently weak security constructs due to the ability of hackers to guess them through brute-force methods enabled by the processing power of today's computers. Despite their knowledge of the vulnerability posed by password-based user authentication systems, information systems managers continue to rely heavily upon single authentication using password-based access control because of its low implementation cost and end-user convenience. In the case of Internet web sites that require user authentication to provide personalized information or sensitive data, there does not appear to be a cost-effective alternative to the use of the username-password pair for access control. While major corporations have the financial ability to augment the security of their intranets and extranets through the use of smart cards and token devices, it is impractical and far too costly for business-to-consumer web sites to deploy this same technology. Such an effort would require the manufacture and shipment of a special token or smart card for every registrant on every web site. It is in this context of Internet transactions and electronic commerce (ecommerce) where the issue of information system security will be explored. The purpose of this study is to analyze in detail the inherent flaws in password-based user authentication and propose a solution to address how managers can effectively increase information system security and maintain access control through an improvement in the user authentication schemes at the root of current information security policy

About-[1]Assistant Professor,HITS College of Engineering
(e-mail-machha.narender@gmail.com)
About-[2]Assistant Professor, Tirumala Engineering College
(e-mail-mohanrao19@yahoo.com)
About-[3]Assistant Professor, Aurora Engg College
(e-mail-mannavababu@gmail.com

II. Vulnerabilities of Password-Based User Authentication

Information security is concerned with enabling authorized users to access appropriate resources and denying such access to unauthorized users. The ability to authenticate valid users is therefore at the foundation of any access control system. Passwords have long been the access control method of choice for most organizations, in part because of their low implementation cost and convenience to users. However, password-based authentication schemes have several vulnerabilities

1. Weaknesses in Password Construction
2. Ease of Password Compromise
3.Alternatives to Password-Based Authentication

When juxtaposed with the tendency of individuals to reuse the same username password combinations across several web sites, these factors reveal the lack of security offered by information systems that grant access based solely on the input of a valid username-password combination.

A. Weaknesses in Password Construction

often contributes to its weakness as a security mechanism. When passwords are generated by computer, they are generally more secure at the expense of being harder to remember. Userselected passwords, on the other hand, have

the added benefit of being easier to recall, but are usually less secure in their construction. Case studies of real users over the past two decades reveal that characteristics of user-selected passwords have not changed significantly in response to publicity of information security breaches. According to a study by Morris and Thompson (1979), more than 85 percent of user passwords were dictionary words; words spelled backwards, names of people or places, or a sequence of numbers. Further investigated the characteristics of user passwords, and examined issues such as password length, character composition, reset frequency, and the use of personal information as passwords. They conducted a survey of a sample of computer users by using an anonymous questionnaire that inquired about the users' password features. According to the study, they determined that the majority of passwords contained either five or six characters. Furthermore, their survey revealed the following

71.9% of respondent's passwords were between one and six Characters

80.1% of passwords were composed of strictly alphabetic characters

79.6% of respondents never changed their passwords

65.2% of respondents had used personal information in their password

35.3% of users wrote down their passwords nearby to remember them

Computer users tend to choose passwords that are short, constant, and based on their surroundings or personal information. Studies of user-selected passwords highlight that the common features of the passwords have remained fairly consistent over time. The underlying reason for this consistency is a matter of convenience for the end-users, who choose a password that will be simple and easy for them to remember. Hackers are undoubtedly aware of this trend and can subsequently focus their efforts to guess user passwords.

B. Ease of Password Compromise

The second vulnerability of the password-based user authentication scheme is the ease with which hackers can obtain these passwords. The common characteristics of the overwhelming majority of passwords are the primary reason that passwords are easily compromised. Knowing that most passwords are short, alphabetic or alphanumeric strings of characters, hackers can run brute-force attacks that use dictionary words, proper names, and numbers to gain illegal access to information systems. Passwords can also be obtained by intercepting their transmission over communications channels, a technique known as "password sniffing". Given the findings of Zviran & Haga (1999) that over a third of users write down their passwords nearby, a password in this case "is no longer something to be guessed but becomes something to be located". If an observer is able to see the user's password written down somewhere, or happens to see the user type the password, then the security of the password is subsequently compromised. Furthermore, despite creating passwords that are easy to remember, computer users are often faced with the burdensome task of remembering many passwords. As a result, users place repeated calls to help desks to obtain their password or to have it reset. An intruder with knowledge of a valid username can just as easily contact the help desk and obtain a working password, enabling him to then log in using the valid username-password combination.

C. Alternatives to Password-Based Authentication

The weaknesses associated with password-based access control can be overcome by taking advantage of alternative methods of user authentication. According to Lui and Silverman (2001), the following three categories can be used for authentication purposes.

1. Knowledge, "something you know"
2. Possession, "something you have"
3. Biometric, "something you are"

The first category includes information known by an individual, such as a password or personal identification number (PIN). The second category consists of an identifiable physical object that an individual possesses, such as a smart card, token, or identification badge. The third category, known as biometrics, includes biological attributes specific to an individual. The third category of user authentication, called nbiometrics, involves an identifier that cannot be misplaced or forgotten (Liu and Silverman, 2001). Biometric devices use physical, biological features to identify and verify individuals. A biometric can take many forms, and in fact, any physical or behavioral characteristic of a person that can serve to uniquely identify that person can be considered a biometric. Examples include a fingerprint, hand geometric pattern, iris, retina, voice, signature, facial pattern, or even DNA (Liu and Silverman, 2001). Commonly accepted as evidence in law enforcement, a biometric is considered by many people Regardless of the specific type of biometric used, the first step in implementing a biometric-based authentication system is generally to store a template of the biometric data of a user. Upon a subsequent attempt to access the information system, the user must present the required biometric identifier to a scanning or recording device, which then compares the input to the database of templates for a potential match. The need to store a biometric template for each user is, unfortunately, one of the major drawbacks of biometric-based authentication systems. Scalability becomes a major hurdle because the amount of time it takes a system to verify an individual increases significantly as more templates are added and checked against everym input. Bandwidth likewise becomes a significant issue since the digitized data from biometric inputs can be quite large.To be the most secure method of uniquely identifying individuals. Biometric-based authentication is considered to be extremely reliable, but like any authentication system, it is not foolproof. It is necessary for information systems managers to decide upon an acceptable balance between the false acceptance rate (FAR) and the false rejection rate (FRR) of a biometric system. The false acceptance rate is a

measure of what percentage of unauthorized users are granted access to the system due to similarities between the user and a stored template that are close enough to be considered a match. The false rejection rate, on the other hand, is a measure of the percentage of authorized users who are refused access, generally due to extraneous factors such as lighting or cleanliness variations of the subject.

Higher success rates of user identification may come at the expense of other disadvantages, however. While some biometric systems can read a user's input through a non-invasive method (such as signature recognition), other methods such as retinal scanning may seem somewhat uncomfortable for users. Furthermore, in the unlikely but possible event that biometric data is compromised, new biological features cannot be distributed to an individual as easily as passwords can be reset. With their personal biometric data stored on servers, users are faced with the fear that their data will be compromised or their privacy violated. And finally, them financial cost of such a system cannot be ignored. Biometric systems are perhaps the most costly method of authentication to implement. Nonetheless, the additional security they provide must be factored into an analysis of their practicality and usefulness. User authentication controls, whether based on passwords, tokens, cards, or biometrics, provide a layer of security to information systems. However, each of these access control methods relies upon a single layer of authentication and can be compromised in a single step. The security of information systems can be increased through a technique called double authentication, which relies upon a combination of methods to perform user authentication and verification. This technique is much more secure than access control based on single-layer authentication because even if one form of authentication is compromised, there is an additional check in place to prevent unauthorized access to information system resources. Double authentication can take many forms. Several of these dual-layer systems have been inn existence for quite some time, while other combinations are just emerging. Perhaps the most well known double authentication technique is the use of a magnetic card along with a PIN known by the user. Banks have been using this dual layer of authentication at automated teller machines (ATMs) or with debit cards. This system incorporates something that the user possesses (the magnetic card) with something that the user knows (the PIN), thereby providing two layers of authentication before providing access to finances. Even in the event that an individual's debit card is stolen, the thief must also know the user's PIN for the card to be of any use. The combination of a PIN and a possession is also utilized by most token-based access control systems. Instead of a magnetic card, users possess a token that displays a dynamic numeric access code. This code must be entered along with the user's PIN in order to gain access to the system. Token-based systems involving a token and PIN combination are slightly more secure than a magnetic card and PIN combination because the former also makes use of a timestamp to prevent password re-use. A timestamp is a date and time associated with the moment a password is entered by the user, and it must fall within the time specified by the server that a particular password is still valid. If a hacker, for example, knows the account number on a user's magnetic card and knows the user's PIN, he is able to compromise the system. On the other hand, even if a hacker is able to determine what number a user entered from the token and what number the user entered as a PIN, the hacker is unable to use that information to subsequently compromise the system since the number on the token will have changed. Biometrics can even be used in conjunction with other forms of authentication to provide a greater degree of reliability. The emergence of "hybrid technology" that encodes a user's biometric template on a smart card/sensor device. This device enables users to scan their fingerprint directly on a portable card, which compares the scanned information with the biometric data stored on the card. While biometrics offer increased security over other methods of authentication, this device can still be stolen and with it, an individual's biometric data. As mentioned earlier, the consequences of compromising a full biometric template are severe since an individual only possesses one set of fingerprints for life. In addition, the technology already exists to lift a fingerprint from a surface and manufacture a false finger capable of fooling some biometric sensors. As a result, new biometric sensors are emerging that can detect the presence of a live finger by reading a pulse.

The biometric smart card is nonetheless a step in the right direction. Due to the storage of biometric data on the device itself, it is much faster than conventional biometric systems that store a user's biometric template on a server. When biometric data is stored on a central server, it takes a significant amount of time for the system to search every template in its database to find a match. As a result, some companies including MasterCard have implemented a system in which the user first indicates his or her name (which does not add much security), and that individual's biometric template is then retrieved from the database. The individual then submits to a biometric scan that is compared with the template pulled from the database. Using this method, the system does not have to compare a scan with every template in the database.

Of all the forms of user authentication, biometrics is considered to be the most difficult to compromise. The combination of biometrics with alternative forms of authentication therefore seems to provide the most secure method of access control.

III. Proposed Solution to User Authentication for E-Business Applications

The proposed solution to increase the security of Internet transactions in a cost-effective manner makes use of all three aforementioned categories of user authentication. This multi-layer authentication method combines the use of a PIN (something the user knows), a magnetic card (something the user has), and a biometric sample (something the user is). However, simply combining all three technologies will not solve the problem of secure user

authentication unless it is cheap, versatile, and accepted by users. The proposed security solution satisfies all three criteria. In order for this approach to be implemented, a small hardware investment is required on the user's end. Specifically, this proposal would require the use of a specialized keyboard that contained a USB card reader as well as a small fingerprint scanner. Such an approach would be very cost-effective because each web site wishing to conduct electronic business would not have to spend time and money to distribute tokens or smart cards to each user, and instead could take advantage of a technology that can be purchased once and used for all web sites. The proposed solution will require each individual to have a username stored on a magnetic strip card. The username must be a unique string of both alphanumeric and symbolic characters and a recommended length of ten such characters, such as "m49K2g#%6L". This string must not contain as a substring the individual's name or social security number. Since the majority of Internet transactions take place with the use of a major credit card, it would seem logical to work with the credit card companies to add an individual's username to the data currently stored on the magnetic strip on a credit card. An individual would specify at the time of applying for a credit card if he desired that specific credit card to contain his username, and that card-issuing company would then create a username for the cardholder and encode it on the card. The credit card- username technique would not add any significant cost to the distribution of usernames, would be portable (in the user's wallet), and would enable the user to maintain the same username across multiple sites, eliminating the need to remember multiple usernames.

Secondly, the user would select a PIN upon registering at each web site. This PIN will be known only by the user and not recorded anywhere. In addition, the user can choose to have a separate PIN for each e-business web site but can also securely use the same PIN for each site. This apparent security vulnerability warrants further explanation. The PIN would not be stored anywhere and would serve to tell the fingerprint scanner which bits of the user's scanned biometric reading to use for authentication purposes. Combining each of these features, the proposed solution for secure user authentication during Internet transactions would work according to the following procedure. Upon registering at a web site, the user would first enter his username and then swipe the credit card encoded with the same username for initial verification. The user would then be prompted to scan his finger on the biometric sensor attached to the keyboard. The biometric scanner would detect whether a live finger or a fake has been presented as input by reading a pulse from the source. The digitized biometric data would only be stored locally for 60 seconds. During that time, the user would enter his PIN (the user PIN), and the web site would send a numeric value (henceforth labeled the site PIN) as well as a timestamp. The PIN and the number sent by the web site would specify which combined bits of the biometric reading to use as the individual's password for that particular website, and this combination of biometric data bits (henceforth labeled the biopair value) would be sent back to the website with the user's timestamp. The biometric data sent to the website would only be a small portion of the user's full biometric reading, thereby maintaining the privacy of the actual biometric reading and avoiding the high bandwidth transmission of an entire reading. The timestamp would ensure that the biometric reading occurred within a specified time range after the request by the website was issued. This procedure is illustrated in Figure 1.2.

Each e-business web site would only be responsible for storing a username, site PIN, and biopair value for each user, a feature that enables this multi-layer authentication technique to be completely scalable. Upon each subsequent visit to a site, the user would have to be authenticated and then permitted to perform any number of business-to-business or business-to-consumer transactions that are permitted for the specified user on that site. To perform each authentication, the site would query its database for the username and return the associated site PIN to the biometric scanner. The user would once again scan his finger and enter his PIN, and the scanner would combine the bits of the biometric reading specified by the user PIN with the bits specified by the site PIN. This combined value would be sent back to the web site, which would then compare this biopair with the biopair value in its database.

This multi-layer authentication technique solves a number of the problems with current methods of authentication. Privacy of biometric data is maintained and bandwidth resources are not overwhelmed since only a portion of the full biometric reading is sent over the Internet or stored in a web site's database. User PINs, which are known by the user and not stored anywhere, ensure that a user can specify which bits from his biometric reading to use as part of his password. This technique enables a user to change his biometric site password at any time by merely changing his PIN. Even if a biometric transmission is intercepted, the timestamp ensures that the intercepted information cannot be reused, and the relationship of the biometric reading to the PIN ensures that the password can be changed if compromised. The problem with current biometric systems is that since the full biometric data is used for the comparison, a compromise of the data would be severe because a user has a limited number of fingerprints. Since each web site associates its own site PIN with each user's biopair value, a password that is hacked from one web site cannot be used to gain access to other sites, even though the username is the same. This approach thereby enables users to use the same username and PIN for every web site without sacrificing security.

The downside to this technique lies in the added cost to the user in additional hardware functionality. However, this one-time cost is far outweighed by the increased level of security offered by this multi-layer authentication method. In addition, the keyboard scanner is extremely versatile in that it can be used for every e-business site that chooses to implement this security method. This increased level of security across all sites can therefore be obtained at a cost

much less than if the user had to purchase a token or proprietary biometric scanner from each e-business.

IV. Conclusion and Future Research

Passwords remain the most prevalent method of user authentication for information systems, and especially Internet transactions for e-business. Password-based authentication is lacking in security due to several factors contributing to the weakness of password construction and the ease with which passwords can subsequently be compromised. The Computer Security Institute (2002) reported in its "Computer Crime and Security Survey" that 38 percent of responding corporations has security breaches resulting from unauthorized access to areas of their web sites.

Alternative forms of user authentication, including tokens, smart cards, and biometrics, attempt to address some of the vulnerabilities of password-based systems, but suffer from their own vulnerabilities when employed in a single layer authentication scheme. Double authentication techniques have been developed which combine the methods of two authentication techniques to increase the level of security of information systems. E-business transactions have yet to take advantage of increased security in user authentication methods due to the high costs associated with a large scale deployment of double authentication technology by each individual site. The cost of increased security remains a principle inhibitor to its implementation, and the percentage of information technology budgets allotted to security has not kept pace with the increase in threats. In 2002, businesses reportedly spent only 11.8% of their information technology budget on security. The multi-layer authentication method proposed in this study can increase the security of web-based transactions by providing a more reliable way to authenticate valid users and simultaneously reduce security implementation costs through the adoption of a single technology source usable by all e-business web sites. While this study has laid the groundwork for a proposal to increase the security of Internet transactions, there are several areas that can be nexplored as further extensions of this research. Future study can look into the methods of authentication used by the 0.5 percent of Internet transactions identified as using more than strictly passwords (Radcliff, 2002). In addition, further research can analyze the multi-layer authentication method proposed in this study to determine its possible areas of vulnerability. And finally, the physical keyboard-scanner technology central to this proposal can be explored to reduce the cost of such a device and propel its

V. References

1) Anthes, G. H. (1994). SecurID keeps passwords changing. Computerworld. Retrieved October 10,2002
2) Anthes, G. H. (1994). TGV's onetime passwords evade intruders. Computerworld. Retrieved October 10, 2002 Anthes , G. H. (1998).
3) Promising technology has yet to gain wideacceptance. Computerworld. Retrieved October 10,2002
4) Bishop, M., Klein, D.V. (1995). Improving system security via proactive password checking. mComputers and Security, Vol. 14, No. 3, 233-249.
5) Black, J. (2002). A Growing Body of Biometric Tech. BusinessWeek Online. Retrieved October 10,2002
6) Computer Security Institute. (2002). Computer Crime and Security Survey. Retrieved November 5,2002
7) Two integrated schemes of user authentication and access control in a distributed computer network. IEE Proceedings: Computers and Digital Techniques, Vol. 145, No. 6., 419-423.
8) Lui, S., Silverman, M. (2001). A Practical Guide to Biometric Security Technology. IT Professional. Retrieved October 10, 2002
9) Millman, H. (2002). Making Passwords Passe . omputerworld. Retrieved October 10, 2002 l
10) Morris, R., Thompson, K. (1979). Password security: a case history. Communication of the ACM, Vol. 22, No. 11, 594-597.
11) Porter, S.N. (1982). A password extension for human factors. Computers and Security, Vol. 6, No. 5, 403-416.

Cloud Computing – A Paradigm Shift

Manjula K A[1] Karthikeyan P[2]

GJCST Computing Classification
C.1.4

***Abstract*-Grid technology is finding its way out of the academic incubator and entering into commercial environments. Ensembles of distributed, heterogeneous resources, or Computational Grids, have emerged as popular platforms for deploying large-scale and resource-intensive applications. Large collaborative efforts are currently underway to provide the necessary software infrastructure. This paper explains Grid Computing and introduces its basic concepts. Clouds, another variant of Grids, and their significance is also discussed. GridGain which is an open source product from GridGgain Systems Inc, is an ideal platform for Native Cloud Applications. This provides developers a powerful and elegant technology to develop and run applications on private or public clouds. GridGain enthusiastically supports the MapReduce model of computation. This paper also discusses about this open source business model which is growing fastest with its noted characteristics of ease and transparency.**

Keywords-Cloud Computing, Distributed Computing, Grid Computing, GridGain, Open Source, Middleware.

I. Introduction

This paper discusses Grid Computing, which is a form of Distributed Computing whereby resources of many computers in a network is used at the same time, to solve a single problem. Grid Computing is the use of hundreds, thousands, or millions of geographically and organisationally disperse and diverse resources to solve problems that require more computing power than is available from a single machine or from a local area distributed system [1]. This technology has been applied to computationally intensive scientific, mathematical, and academic problems through volunteer computing, and it is used in commercial enterprises for such diverse applications as drug discovery, economic forecasting, seismic analysis, and back-office data processing in support of e-commerce and Web services.

Compared to Grid Computing, Cloud Computing is relatively a newer concept, which has become popular recently with the availability of environment like Amazon EC2. Clouds leverages virtualization technology and that makes it distinguishable from Grids. Cloud Computing is the use of a third party service (Web Services) to perform computing needs. Here Cloud depicts Internet. With Cloud Computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, which is beneficial to small and medium-sized businesses. Basically consumers use what they need on the Internet and pay only for what they use. Cloud Computing poses a number of challenges: deployment, data sharing, load balancing, failover, discovery (nodes, availability), provisioning (add, remove), management, monitoring, development process, debugging, inter and external clouds (syncing data, syncing code, failover jobs). Cloud platforms like GridGain, GigaSpaces, Terracotta, Coherence, Hadoop etc. makes it affordable to grow and manage grids. Gridgain is an open source computational grid framework that enables Java developers to improve general performance of processing intensive applications by splitting and parallelizing the workload. GridGain can also be thought of as a set of middleware primitives for building applications.

In this paper grid computing is discussed in the next section, followed by cloud computing and a comparision of these two technologies. The paper concludes with a discussion on the capabilities and characteristics of GridGain.

II. Grid Computing

The main concept of Grid Computing is to extend the original ideas of the Internet to sharing widespread computing power, storage capacities and other resources [2]. The term, Grid Computing, has become one of the latest buzzwords in the IT industry. Grid Computing can be thought of as distributed and large scale Cluster Computing and as a form of network distributed parallel processing. This innovative approach of computing leverages on existing IT infrastructure to optimize computing resources and manage data as well as computing workloads. Grids are collections of heterogeneous computation and storage resources scattered along distinct network domains. Grids provide tools that allow users to find, allocate and use available resources [3]. Grid middleware provides users with seamless computing ability and uniform access to resources in the heterogeneous grid environment [4]. Structure of a grid is depicted in Fig. 1.

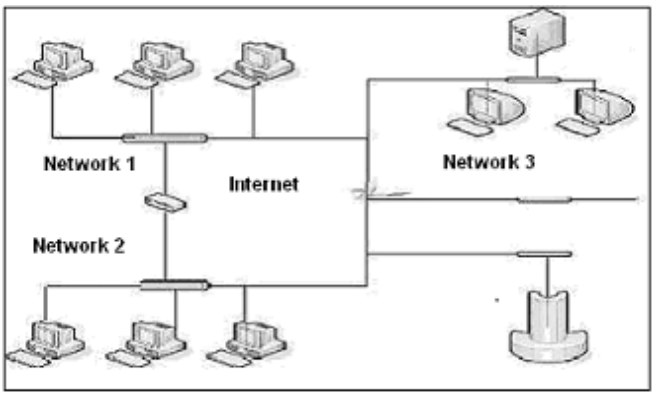


Fig. 1 Example for a Grid structure

Grid computing appears to be a promising trend for three reasons [5]:

- Its ability to make more cost effective use of a given amount of computer resources.

About-[1]Department of Information Technology
Kannur University, India (e-mail; manjulaka@gmail.com)
About-[2]MES College of Engineering Kuttippuram, Kerala, India

- As a way to solve problems that cannot be approached without an enormous amount of computing power.
  It suggests that the resources of many computers can be cooperatively and perhaps synergistically harnessed and

managed as collaboration toward a common objective.
Grid Computing is becoming a critical component of science, business, and industry. Grids could allow the analysis of huge investment portfolios in minutes instead of hours, significantly accelerate drug development, and reduce design times and defects. Larger bodies of scientific and engineering applications stands to benefit from grid computing, including molecular biology, financial and mechanical modeling, aircraft design, fluid mechani
biophysics, biochemistry, drug design, tomography, data mining, nuclear simulations, environmental studies, climate modeling, neuroscience/brain activity analysis, astrophysics[6].

III. CLOUD COMPUTING

Cloud Computing evolves from grid computing and provides on-demand resource provisioning. Grid computing may or may not be in the cloud depending on what type of users are using it [7]. Cloud Computing is the convergence and evolution of several concepts from virtualization,
distributed application design, grid, and enterprise IT a
management to enable a more flexible approach for
deploying and scaling applications[Fig. 2]. To deliver future state architecture that captures the promise of Cloud Computing, architects need to understand the primary benefits of Cloud computing[8]:

- Decoupling and separation of the business service from the infrastructure needed to run it (virtualization).
- Flexibility to choose multiple vendors that provide reliable and scalable business services, development environments, and infrastructure that can be leveraged out of the box and billed on a metered basis—with no long term contracts.
- Elastic nature of the infrastructure to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.
- Cost allocation flexibility for customers wanting to move capital expenditure into operating expenditure.
- Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

Cloud computing eliminates the costs and complexity of buying, configuring, and managing the hardware and software needed to build and deploy applications, these applications are delivered as a service over the Internet (the cloud). Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. Cloud computing incorporates infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) as well as Web 2.0

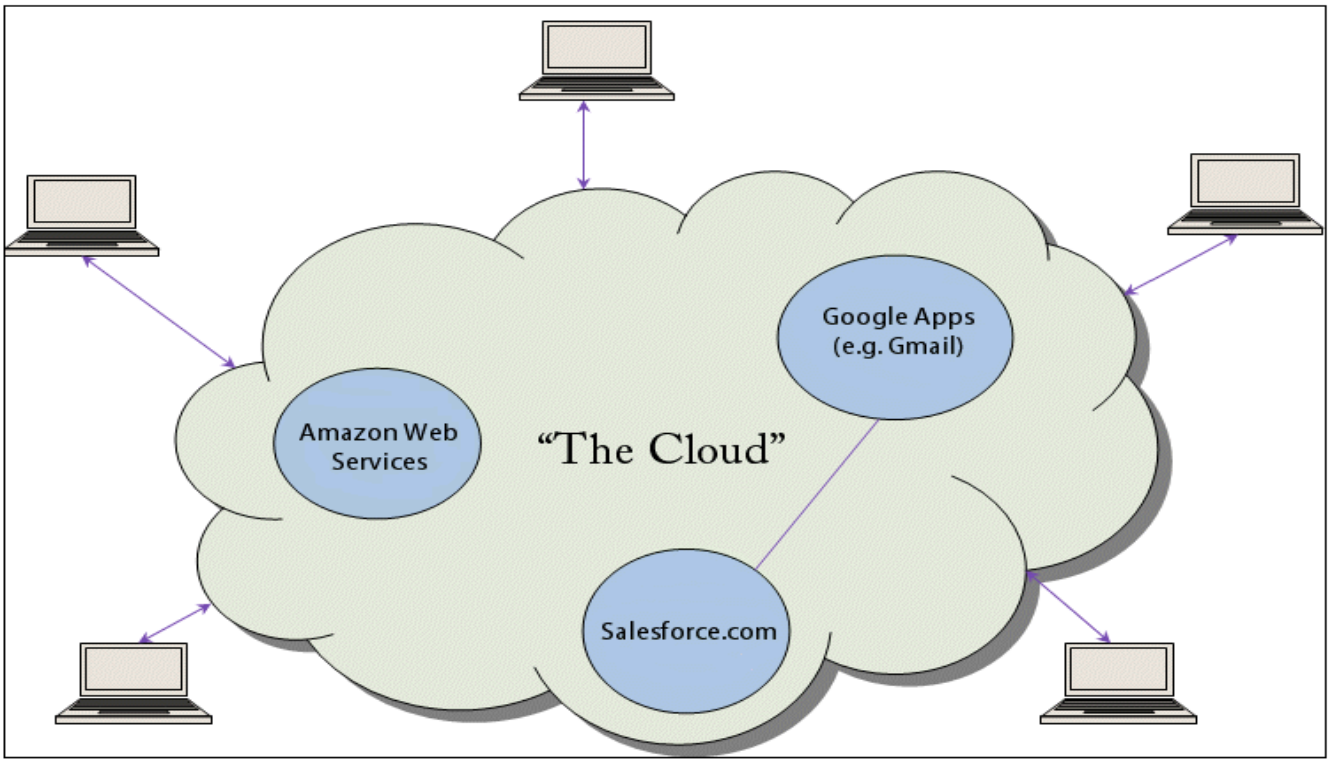


Fig. 2. The architecture of cloud [Source: http://www.cloudup.net]

From a hardware point of view, three aspects are new in Cloud Computing[9].

- The illusion of infinite computing resources available on demand, thereby eliminating the need for Cloud Computing users to plan far ahead for provisioning.
- The elimination of an up-front commitment by Cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs.
- The ability to pay for use of computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful.

Cloud computing is massively scalable, provides a superior user experience, and is characterized by new, internet-driven economics. [10]

IV. GRID COMPUTING vs CLOUD COMPUTING

Cloud Computing and Grid Computing do have a lot in common; both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. Both computing types involve multitenancy and multitask, meaning that many customers can perform different tasks, accessing a single or multiple application instances[7]. Cloud and grid computing provide service-level agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. At the same time Cloud Computing and Grid Computing do have differences[11]. One major difference being that while grids are typically used for job execution (i.e. limited duration execution of a program, often as part of a larger set of jobs, consuming or producing all together a significant amount of data), clouds are more often used to support long-serving services. While Grids provide higher-level services that are not covered by Clouds; services enabling complex distributed scientific collaborations (i.e. virtual organizations) in order to share computing data and ultimately scientific discoveries. In Clouds Amazon S3 provides a Web services interface for the storage and retrieval of data. An object as small as 1 byte and as large as 5 GB or even several terabytes can be stored. S3 uses the concept of buckets as containers for each storage location of objects. The data is stored securely using the same data storage infrastructure that Amazon uses for its e-commerce Web sites. Users are gaining confidence in the cloud services and are now outsourcing production services and part of their IT infrastructure to cloud providers such as Amazon. A comparison of grid (EGEE Grid) and cloud (Amazon cloud) is depicted in Fig.3. which points out to the power of cloud computing [11]

	EGEE Grid	Amazon Cloud
Target Group	Scientific Community	Business
Service **SLA**	Short-lived batch-style processing (job execution) Local (between EGEE project and the resource providers)	Long-lived services based on hardware virtualization Global (between Amazon and users)
User Interface	High-level interfaces	HTTP(S), REST, SOAP, Java API, BitTorrent
Resource-side middleware	Open Source (Apache 2.0)	Proprietary
Ease of use	Heavy	Light
Ease of Deployment	Heavy	Unknown
Resource Management	Probably similar	
Funding Model	Publicly funded	Commercial

Fig. 3. Comparison between EGEE Grid and Amazon Cloud

Michael Sheehan(12) analysed the trends in search volume and news reference volumes of computing terms Grid Computing and Cloud Computing. He finds that the term Grid Computing, which has been around for a while is seen trending downwards. But, the newcomer Cloud Computing, which made its full entrance into this trend analysis around 2007 is rapidly gaining momentum. 2008 seems to be a pivotal time where it surpassed Grid Computing (and continues to grow).

V. GRIDGAIN

In order to control and manage the various resources that Grids can offer, various Grid middleware like Optimal Grid [13]; Ice [14]; GridGain [15], Gigaspaces[16], Terracotta[17] etc. have been developed. One among these, GridGain is an open source product released under the terms of GNU General Public License (GPL) from GridGain Systems Inc. The developers of GridGain are of the opinion[15] that it is an ideal platform for Native Cloud Applications and is noted for the ease of use and transparency it renders with regard to the deployment issues. GridGain with its modern design is based on Java programming language, and is adequate for networking systems and applications. GridGain provides developers with powerful and elegant technology to develop and run applications on private or public clouds. GridGain is foccused on providing the best Java software middleware to develop and run Grid applications on the Cloud infrastructure in a simple and productive way. GridGain's open Cloud platform is a new breed of Cloud Computing software. It enables developers to write any custom Grid-enabled applications or Grid enable the existing one and seamlessly deploy it on the Cloud taking a full advantage of such concepts like MapReduce, data grids, affinity load balancing, zero deployment, and peer-to-peer class loading among many other.

GridGain's SPI architecture is ideally suited for hybrid cloud deployment with any mix of internal and external Clouds in the same time allowing to develop entire application locally and then seamlessly deploy them on virtualized Cloud without any changes to business logic, the code or how it was developed [15]. The key features of GridGain are

- Hybrid Cloud Deployment.
- Cloud Aware Communication & Deployment.
- Advanced Affinity Map/Reduce.
- Annotation-based Grid-enabling with AOP.
- SPI-based integration and customization.
- Advanced load balancing and scheduling.
- Pluggable Fault-Tolerance.
- One compute grid - many data grids.
- Zero deployment model.
- JMX-based Management & Monitoring.

The characteristics that are considered to be promoting the growth of GridGain are[18].

- Cost - It Is Free.
- Source Code - It Is Open Source.
- Support - Enterprise Level Support.
- Java - It Is Made In Java And For Java.
- AOP - Innovative AOP-based Grid Enabling.
- Simplicity - Ease Of Use.
- Features - Best of Breed Grid Computing Features.
- Practicality - Everything You Need, Nothing You Do not.
- Integration - Out-Of-The-Box Integration With Spring, JBoss, Aspect etc
- Agile - Made With Developers In Mind.

According to the developers of GridGain[19], the next major release is expected to include ability to execute Grid task from any Ajax-based application via REST/JSON combination providing native integration between server-side GridGain and Web 2.0 client side applications. GridGain is pioneering in field of mobile Grid Computing and work is ongoing on developing GridGain on Google Android platform. Next version of GridGain is expected to feature improved management and monitoring for subscription subscribers based on VisualVM featuring enterprise grade capabilities such as role-based access control, global alerts, scheduling control, trend base-lining, reporting, and distributed monitoring.

VI. CONCLUSIONS

Computational Grids act as popular platforms for deploying large-scale and resource-intensive applications. Another related technology, the newly emerging IT delivery model—Cloud Computing—can significantly reduce IT costs & complexities while improving workload optimization and service delivery. Cloud Computing is found to be massively scalable, provides a superior user experience, and is characterized by new, internet-driven economics. Grid Computing and Cloud Computing resemble on some respects, but there are differences. GridGain is a newly introduced promising grid framework, which is an open source product. This middleware enables developers to write any custom grid-enabled applications and performs well with its key features like SPI based Integration-Customization, Advanced Affinity Map/reduce, AOP. The developers of GridGain are expecting to incorporate much more improved management and monitoring features into this product in coming releases.

VII. REFERENCE

1) Lewis, M. Grid Computing. Retrieved from http://grid.cs.binghamton.edu.

2) Yang, C.T., Han, T.F., & Kan, H.C. (2009). G-BLAST: a Grid-based solution for mpiBLAST on computational Grids. Concurrency and Computation: Practice and Experience, vol. 21, no. 2, pp. 225-255.

3) [3Amador, G., Alexandre, R., & Gomes, A (2009). Re-engineering Jake2 to work on a grid. Retrieved from http://www.av.it.pt/conftele2009/Papers/96.pdf

4) Buyya, R., & Venugopal, S.(2005). A Gentle Introduciton to Grid Computing and Technologies. CSI Communications, July, 2005.
5) Berman, F., et al. (2003). Grid Computing: John Wiley and Sons.
6) Kaufman, J.H., et al. (2003). Grid Computing Made Simple. The Industrial Physicist, vol. 9, no. 4, pp. 31-33.
7) Myerson, J.M. (2009) . Cloud computing versus grid computing. Retrieved from http://www.ibm.com
8) [Bennett, S., Bhuller, M., & Covington, R. (2009). Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing. Retrieved from www.oracle.com
9) Armbrust, M., & Fox, A., et al. (2009). Above the Clouds: A Berkeley View of Cloud Computing. whitepaper, UC Berkeley Reliable Adaptive Distributed Systems Laboratory. Retrieved from http://radlab.cs.berkeley.edu/
10) Cloud Computing. Retrieved from http://www.ibm.com/ibm/cloud/
11) Klems, M. (2008). Comparative study: Grids and Clouds, Evolution or Revolution. Retrieved from www.eu.egee.org 11/6/2008
12) Sheehan, M., (2008). Trending Various Computing Terms – Clouds are getting Congested. Retrieved from www.gogrid.com
13) OptimalGrid. Retrieved from http://www.alphaworks.ibm.com/tech/optimalgrid
14) Ice. Retrieved from www.zeroc.com
15) Gridgain. Retrieved from www.gridgain.com
16) GigaSpaces. www.gigaspaces.com
17) Terracotta. Retrieved from www.terracotta.org
18) 10 Reasons to use GridGain. Retrieved from http://www.gridgainsystems.com
19) GridGain: One Compute Grid, Many Data Grids. Retrieved from http://highscalability.com

.

On Security Log Management Systems

Sabah Al-Fedaghi[1] Bader Mattar[2]

GJCST Computing Classification
H.2.7, D.4.6

***Abstract*-A log management system (LMS) is a system for creating, receiving, processing, releasing, and transferring of security log data. Its main objectives include detecting and preventing unauthorised access and abuse, and meeting regulatory requirements. One of its main components is the classification of events to make decisions related to archiving and to invoking responses to certain events. Most current approaches to LMS design are system dependent and involve specific hardware (e.g., firewalls, servers) and commercial software systems. This paper presents a theoretical framework for LMS in terms of a flow-based conceptual model with emphasis on security-related events. The framework includes four separate flow systems: active system, log system, alarm system, and response system. All systems are composed of five inclusive stages: receiving, processing, creating, releasing, and transferring. The experimental part of the paper concentrates on log analysis in the processing stage in the log system. We select actual log entries and classify them according to these five stages.**

Keyword-log management system, security-related events, conceptual model, logs classification.

I. INTRODUCTION

A log is a record of a computer event arising during processing in systems and networks. It is "append-only, time stamped records representing some event that has occurred in some computer or network device" [23]. Logging refers to the action of recording events in a log database. Event logging is a major component in most critical systems. Applications, security systems, and operating system components can make use of a centralised log service to report events that have taken place, such as a failure to start a module, complete an action, or block or deny some connections.

A centralised log service provides valuable security-related functions such as troubleshooting and monitoring. Logging tools can improve security for systems, applications, and storage with benefits that include the following [19] [13]

- Detect/prevent unauthorised access and insider abuse
- Meet regulatory requirements
- Analyse and correlate forensic data
- Track suspicious behaviour
- IT troubleshooting and network operations

The use of computer security logs from servers, network devices, diagnostic tools, and security-specific devices has increased tremendously (89 percent of organisations in 2010, compared with 43 percent in 2005 [19]). This has created the need for log management. (Security) log management is the process "for generating, transmitting, storing, analyzing, and disposing of computer security log data" [18]. According to [18], a fundamental problem with log management is balancing log management resources with the quantity of log data. "Log generation and storage can be complicated by several factors, including a high number of log sources; inconsistent log content, formats, and timestamps among sources; and increasingly large volumes of log data" [18]. There are several widely used formats of log messages, e.g., Apache Common Log Format [14] for Web servers, and Unix Syslog format [10]; however, there are no common standards for log message encoding.

To assist in facilitating more efficient and effective log management, Kent [18] recommends the establishment of a log management infrastructure that is used to generate, transmit, store, analyze, and dispose of log data, and support the policy and roles. When designing infrastructures, major factors to be considered include the volume to be processed, network bandwidth, storage, the security requirements, and resources needed for staff to analyze the logs. [18]

There are many log management systems on the market, and also many internally managed log management systems. It is reported that "because of difficulties in setup and integration, most organizations have only achieved partial automation of their log management and reporting processes" [19]. According to Patrick Mueller [21],

The legal requirements around log management may make you feel like you're battling the Hydra—solve one problem, two more pop up in its place. Analyzing and aggregating the incessant streams of information created by computer and network logs has always been a difficult, thankless task, but now it's taking on epic proportions because of regulatory compliance.

For example, the 2006 PCI Data Security Standard (DSS) requires that certain events be logged with specific details of each audit entry and with network time synchronisation among logging components. The Health Insurance Portability and Accountability Act (HIPAA) mandates "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Modern log management systems are typically complex systems. Although LMS is dependent on actual requirements and needs, theoretical study of these systems provides a foundation for requirement analysis, design, and implementation. Design of such a system needs all system development methodologies that have been used in other computer systems. Insufficient efforts have been invested in studying LMS in the abstract.

About-[1,2] Kuwait University (e-mail;[1] sabah@alfedaghi.com)
About[2] (e-mail;Eng.bader@yahoo.com)

This paper is concerned with developing high-level architectural issues for these systems. After reviewing current abstract architectures, we propose a conceptual model that depicts various functionalities involved in logging procedure. The paper also concentrates on computer security related logs that can be generated by many sources, including security software, intrusion detection systems, operating systems, and applications. An implementation-independent scheme of classification of log entries is also proposed. The classification method is applied to actual entries of events. Our approach is based on a flow model, as reviewed in the next section.

II. Flow Model

Recently, a flow model (FM) has been proposed and used in several applications, including communication and engineering requirement analysis. For the sake of making this paper self-contained, we review such a model introduced in several works [4], with additional materials related to event classification.

In FM, the flow of "things" indicates movement inside and between spheres. The sphere is the environment of the flow and includes five stages that may be subspheres with their own five-stage schema. The stages may be named differently; for example, in an information sphere, a stage may be called "communication," while in raw material flow the same stage is called "transportation". The information creation stage may be called "manufacturing" in materials flow.

A. General view

A flow model is a uniform method for representing things that "flow", i.e., things that are exchanged, processed, created, transferred, and communicated. "Things that flow", called *flowthings*, include information, materials (e.g., in manufacturing), and money. To simplify this review of FM, we introduce the model in terms of *information* flow. Information occurs in five *states*: transferred, received, processed, created, and released, as illustrated in Fig. 1. Here, we view "*state* of information" in the sense of properties; for example, water occurs in nature in the states of liquid, solid, and gas.

Fig. 1 also represents a transition graph, called *flowsystem*, with five states and arrows representing flows among these states. Information can also be stored, copied, destroyed, used, etc., but these are secondary states of information in any of the five generic states. In Fig. 1, flows are denoted by solid arrows that may *trigger* other types of flow, denoted by dashed arrows, as will be discussed.

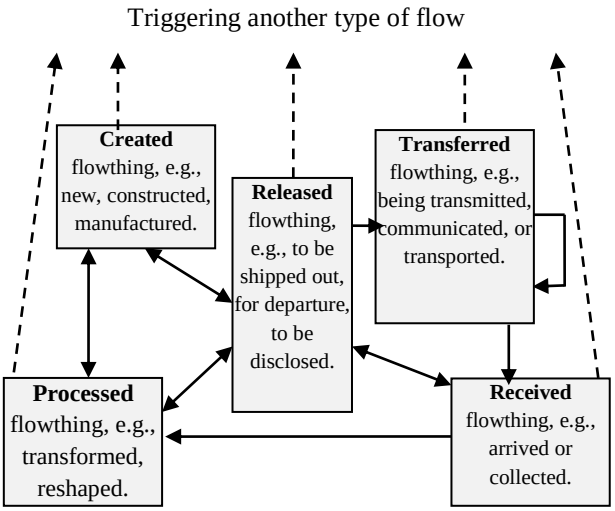


Fig. 1. State transition diagram for the flow model with possible triggering mechanism.

The environment in which information exists is called its sphere (e.g., computer, human mind, organisation information system, department information system). The flowsystem is reusable because a copy of it is assigned to each entity (e.g., software system, vendor, and user). An entity may have multiple flowsystems, each with its own flowsystem. As will be developed later, an improvement cycle can be described in terms of flowsystems of different flowthings: information, plans, actions, and systems. As forms of information, plans, actions, and systems are flowthings that can be received, processed, created, released, and transferred.

A flowsystem may not necessarily include all states; for example, conceptualisation of a physical airport can model the flow of passengers: received (arriving), processed (e.g., passports examined), released (waiting to board), and transferred (to planes); however, airports do not *create* passengers (ignoring the possibility of an emergency where a baby is born in the airport). In this case, the flowsystem of the airport includes only passenger states of received, processed, released, and transferred.

As mentioned, we view a system as the environment in which information exists, called its sphere (e.g., computer, human mind, organisation information system, department information system). A system is also viewed as a complex of flowsystems. From this perspective, many notions discussed in this paper take different spots. For example, "Where events happen" is understood as the position of events in flowsystems and in stages of flowsystems. "Who is affected" is translated as what flowsystem is affected. "What subsystems are involved" asks what subflowsystems are involved. This also applies to flows, substages, and so forth related to events.

B. *Exclusiveness of information states*

The states shown in Fig. 1 are exclusive in the sense that if information is in one state, it is not in any of the other four states. Consider a piece of information σ in the possession of a hospital. Then, σ is in the possession of the hospital and can be in only one of the following states:

1. σ has just been collected (received) from some source, e.g., patient, friend, or agency, and stored in the hospital record waiting to be used. It is *received* (row) information that has not been processed by the hospital.
2. σ has been processed in some way, converted to another form (e.g., digital), translated, compressed, etc. In addition, it may be stored in the hospital information system as *processed* data waiting for some use.
3. σ has actually been created in the hospital as the result of doctors' diagnoses, lab tests, processing of current information (e.g., data mining), and so forth. Thus, σ is in the possession of the hospital as *created* data to be used.
4. σ is being released from the hospital information sphere. It is designated as *released* information ready for transfer (e.g., sent via DHL). In an analogy of a factory environment, σ would represent materials designated as ready to ship outside the factory. They may actually be stored for some period waiting to be transported; nevertheless, their designation as "for export" keeps them in such a state.
5. σ is in a *transferred* state, i.e., it is being transferred between two information spheres. It has left the released state and will enter the received state, where it will become received information in the new information sphere.

It is not possible for processed information to directly become received information in the same flowsystem. Processed information can become received information in another flowsystem by first becoming released information, then transferred information, then arriving at (being received by) another flowsystem.

Consider the seller and buyer information spheres shown in Fig. 2. Each contains two flowsystems: one for the flow of orders, and the other for the flow of invoices. In the seller's infosphere, processing of an *order* triggers (circle 3) the creation of an *invoice* in the seller's information sphere, thus initiating the flow of invoices.

The reflexive arrow of the transfer state shown in Fig. 1 (above) denotes flow from the transfer state of one flowsystem to the transfer state of another.

In Fig. 2, the *Buyer* creates an *Order* that flows by being released and is then transferred to the *Seller*. The "transfer components" of the Buyer and the Seller can be viewed as their transmission subsystems, while the arrow between them represents the actual transmission channel.

The notion of triggering will be used in our cycle of improvement, where information flow (e.g., data about a current system) triggers plan flow, which in turn triggers action flow that creates a new system (system flow)

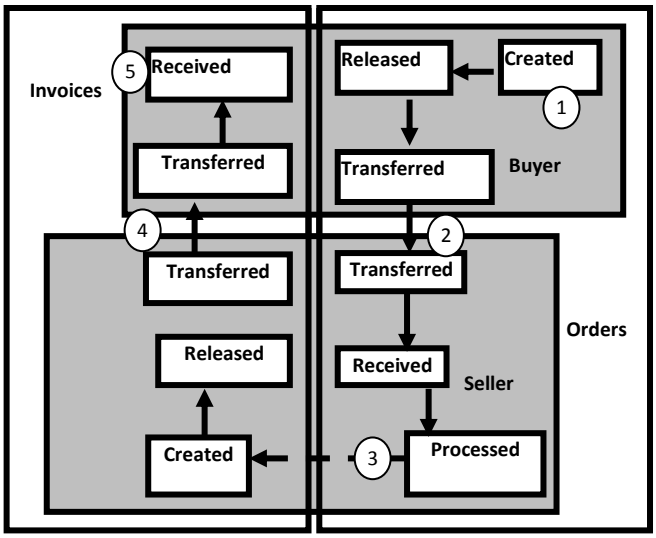


Fig. 2. Order flow triggers invoice flow.

C. *Formal View*

Fig. 2 illustrates the triggering mechanism of flows of orders and invoices. An important principle of FM is the separation of flows. An order triggers an invoice, and each has its flowsystem in its own information sphere. Triggering in the context of FM means *activation* of a state or substate, which may generate a flow. Suppose the *receive* state is activated by triggering; when flow is *received*, triggering may then result in:

(1) Activating the flow to *release*
(2) Activating the flow to *process*
(3) Mistriggering

Mistriggering indicates that the triggering has not succeeded. Triggering may specify a chain of flow. For example, a triggering in *receive* may specify flow to *release* or flow to *release and transfer*. In the last case the triggering is a chain of triggering.

FM reflects a map of possible flows, just as a city map represents possible routes. Traffic lights internally trigger flows.

Secondary stages include Copy, Store, Delete, and Destroy that can be in any of the five FM stages. For example, there is *stored* received information, *stored* created information, *stored* processed information, *stored* released information, and *stored* transferred information.

This FM formalisation can be supplemented with rules and constraints that permit flow from one state to another. Additional "logic gates" (e.g., OR, AND) can also be overbuilt on the basic flowsystem.

III. Conceptualising Log Management Systems

The design of log management systems is a complex process that needs all system development methodologies that have been utilised in other computer systems, including conceptual modelling. A conceptual model is viewed as a high-level abstract description of concepts that correspond to entities, processes, and relationships in real-world systems. The resulting representation can be used as a first

step in building a less abstracted description of the phenomenon under study. It is also useful for identifying common constructs and can serve as general understanding in designing and communication.

In the context of LMS, [22] presents a "conceptual" model of a "typical" log management solution utilising servers, firewall, and so forth. According to [22], The Syslog standard [is used] to aggregate logs from key systems across the network. A correlation engine is then used to look at relationships between events. This event correlation step allows a view into collections of events that may point to malicious or other unwanted network behaviour.

Clearly, such a description is a highly specific system in comparison with, say, database systems that are described in such terms as objects, attributes, entities, and relationships.

Fischer [9] describes transfer of a log message in a more abstract fashion, as shown in Fig. 3.

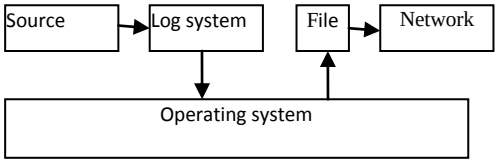


Fig. 3. Example transfer of a log message (Modified from [9]).

"First step to implement a logging infrastructure is listing critical systems ... and determining what logging is turned on" [7]. At the analysis stage, raw log data are analysed and interpreted to consolidate logs. Sophisticated tools are needed to spot security problems. A number of software products are available to help collect and analyse audit and log data.

According to Fischer [9]

Although the specific technical architecture of a log management system has to be adapted to specific requirements, the basic structure of a log management system is layered in three tiers:

- Input layer
- Processing layer
- Output layer

Fischer [9] then gives an example of a log management system, as shown in Fig. 4

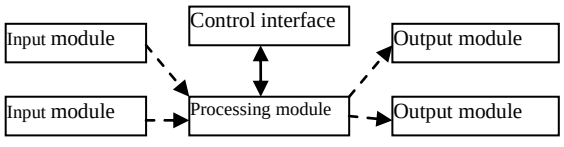


Fig. 4. Sample log management system (from [9]).

The input layer receives, formats, and sends log messages to the processing layer. The processing layer includes the processing module and the rule store (Control). Log messages are processed and filtered against rules to select different output modules. Typical processing includes interpretation, categorisation, normalisation, reduction, and execution. The rules are used to extract the needed information to decide which of the configured actions should be executed next. For example, "the result triggers an action, such as displaying an alert or running an external program" [9]. The output layer uses database back-ends for storing and retrieving received log messages.

An important architectural issue in OMS is the *separation of concerns*:

Each functional subsystem or module of a system should be cleanly separated from other system components and encapsulate exclusively functionality that is absolutely required for the specific task…

On a higher level of abstraction, this requirement might be fulfilled by structuring a log management system into the mentioned basic building blocks, namely input, processing and output layer. [9] [6]

While this type of description is independent of a specific system, it falls short of drawing a complete conceptual picture in comparison with our FM-based model. Also, it does not distinguish clearly among functionalities and subsystems.

IV. FM-Based Log System

We conceptualise LMS infrastructure as a system of flowsystems created from an active system, logging system, alert system, and response system, as illustrated in Fig. 5(a).

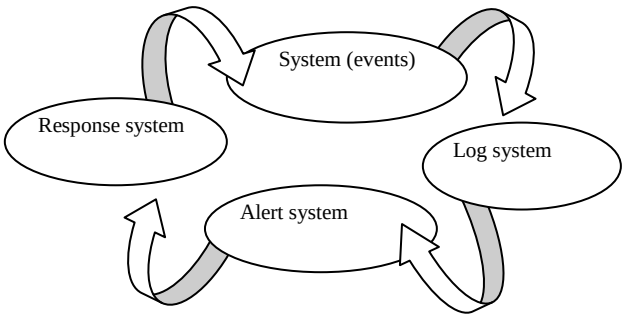


Fig. 5. General view of FM-based LMS infrastructure.

The notion of "event" is a central concept in logging. Logged events are selected to cover different types of events at different security-relevant points in the system. In FM, events are flowthings that can be received (e.g., the event of log-in), processed (e.g., request to retrieve data), created (e.g., activating a program), released (e.g., the action of buffering out bound file), and transferred (e.g.,

transmission). Any of these events is a change of state in an active system which is viewed as a flowsystem. They trigger creating and processing log entries. Events are actions (in common sense), while logs, in this case, are records of the actions.

Logs, in their turn, are flowthings. Some log entries trigger alarms. Alarms, in its different forms, are flowthings that can be created, processed, received, released, and transfer. Alarms, also, trigger responses. Typically, a response is a type of an action (purposeful event), hence, it is a flowthing. Fig. 6 shows the possible sequence of flowthings.

Nevertheless, in the context of security-related events, system's events can be viewed as an outside action (e.g., attack) and system's reaction as shown in Fig. 7.

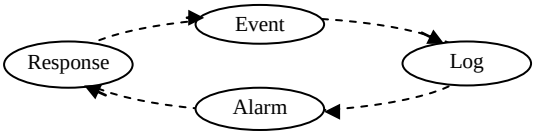


Fig. 6. General sequences of flowthings.

Figure 8 shows a detailed representation of these flowsystems. Notice that the log system keeps recording all activities including alarms and responses (circles 1 and 2). In the figure, instead of drawing too many dotted arrows, triggering mechanisms are drawn starting from the edge of the flowsystem box to denote that origins of activities can be in any point in the flowsystem.

These figures provide a theoretical framework for LMS in terms of a flow-based conceptual model. We assume that the log system includes all typical functions such as analysis, archiving, and reporting. Thus, the log system by itself is a complex of flowsystems of flowthings that are related to logging. The same flow-based methodology can be utilised as different levels of descriptions. In the next section we concentrate on the classification of events as part of the log analysis.

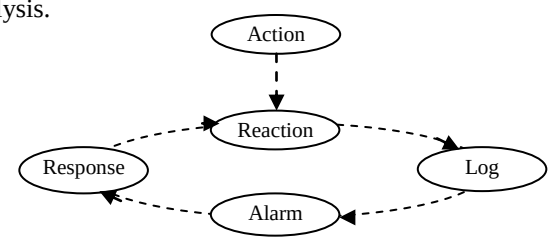


Fig. 7. General sequences of flowthings in the context of security-related events.

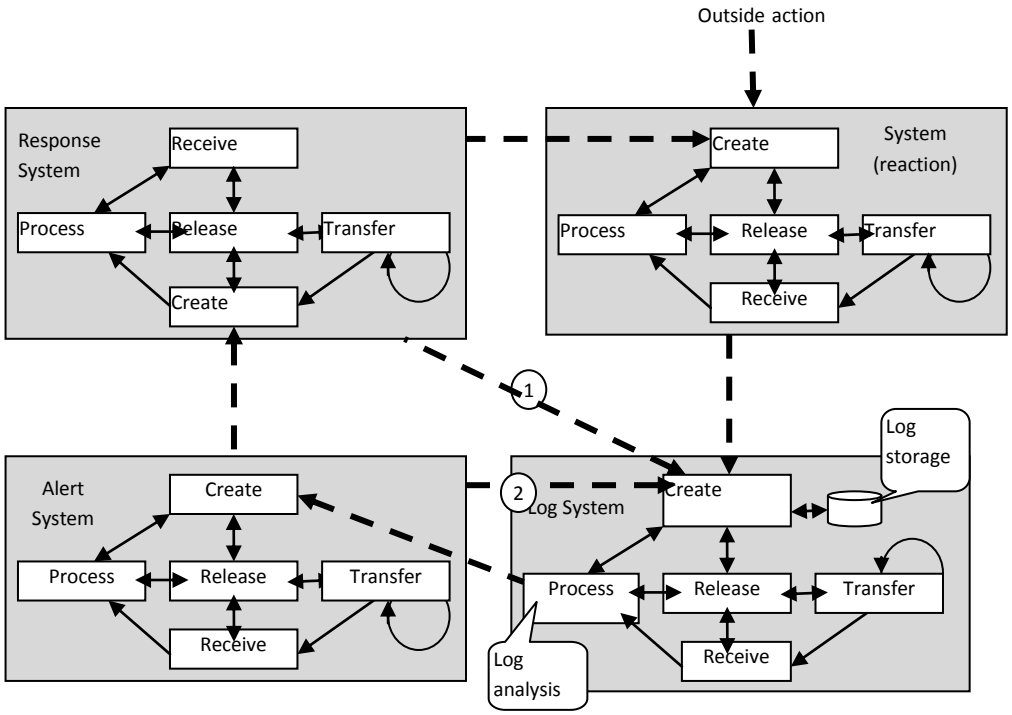


Fig. 8. Conceptualisation of log system and related systems.

V. Flow-Based Logging Model

FM provides a conceptual foundation for the classification of security-related events as received, processed, created, released, or transferred information events. Classification here is based on information flow in different stages of the (active) flowsystems. In addition, the flow model allows establishing rules for such issues as classifying the severity/sensitivity of processed events. In privacy enhancing systems, creation of personal information is generally a more sensitive event than processing it. In addition, releasing such information to outsiders is a more privacy-significant event than receiving it. In such cases it is possible to configure a type of filtering mechanism that would apply to these types of events; e.g., the rule: the event of releasing personal identifiable information to an outsider triggers sending an e-mail to alert the proprietor of that personal identifiable information, as required by some privacy regulations.

Separate protection mechanisms can be used for each class of log information. "The use of different mechanisms for different classification gives the opportunity to use mechanisms that give more usability for information that doesn't need that strong mechanism. This allows the possibilities of using the same mechanism with lower assurance or strength" [17].

There are many security-oriented event classifications. We review a few methods as examples [4].
AIX [5] uses the following classifications (some subcategories are deleted for the sake of brevity):

A. *Security Policy Events*

-Subject Events: process creation, process deletion, setting subject security attributes
-Object Events: object creation, object deletion, object open, object close
- Import/Export Events: importing or exporting an object
-Accountability Events: adding a user, changing user attributes in the password *database*, *user login*, and *user logoff*
-General System Administration Events: use of privilege, file system configuration, device definition and configuration, normal system shutdown
-Security Violations (potential): access permission refusals, privilege failures, diagnostically detected faults and system errors.
In such a long list of events, grouping is performed according to subject/object, then import/export, then violations. In this case, a list seems to be built from examining different rules (subject/object), functions (e.g., accountability), organisational units (system administration), and status (violations).
In the area of network intrusion events, Kazienko and Dorosz [11] list monitoring of the following events groups:

- Network traffic (packets) attempting to access the host
- Login activity on the networking layer
- Actions of a super-user (root)
- File system integrity, e.g., any changes to the files
- System registers state
- The state of key operating system files and streams

We can observe no systemised grouping of event types: activities, actions, or changes to files, states, and streams, extracted from the network operating environment.

Windows event logs contain the following types of events [12]: error event, warning event, information event (successful operation of an application, driver, or service), success audit event, failure audit event. Again, these classes of events seem to lack systemisation and are specified according to the hosting system.

HP recommends basic monitored events: admin event, login event, moddac self-auditing event, execv, execve, and pset event [12]. "Admin", "login", "exec"… seem to be targeted events according to the specifics of the system.

Web Services Architecture [15] contains an "audit guard" that monitors agents, resources, and services, and actions relative to one or more services. We again note the heterogeneous categorisation of monitoring types.

It can be concluded that a general theory for event classification for monitoring purposes is lacking. The required classification must be generic in the sense that it is not tied to any specific system activity. In the next section, we introduce the foundation of such an approach to event logging.

From the security point of view, monitoring for security breaches can be accomplished by way of network level TCP/IP, server, and application, and through process-specific monitoring [7]. A record of monitoring typically shows the identity of any entity that has accessed a system and types of operations executed. It may include attempted accesses and services, a sequence of events that have resulted in modifying data. The purpose is mostly to provide evidence for reconstruction of the sequence of events that led to a certain effect or change.

To accomplish its function, a log system runs in a privileged mode to oversee and monitor all operations. Key information in such a system includes information format, type of activity, identity, storage, location, time, cause, tools and mechanisms used, and so forth [13].

VI. Experimentation: Security-Related Logs

There is no system that uses the proposed FM-based classification of security-related events. Consequently, we have opted to inspect one current log of events to identify

entries that can be classified accordingly. We select a eXchange) firewall logging monitor tool [16]. PIX is a popular IP firewall and network address translation (NAT) appliance that runs a custom-written proprietary operating system originally called Finesse (Fast Internet Server Executive), now known simply as PIX OS. It is classified as a network layer firewall with stateful inspection, which means it keeps track of the state of network connections (such as TCP streams, UDP communication) travelling across it. Technically the PIX would more precisely be called a Layer 4—Transport Layer—Firewall, although its access is not restricted to Network Layer routing, but to socket-based connections. By default it allows outbound traffic , which is the traffic generated from the inside host to the outside one, and it allows only inbound traffic generated in response to a valid request from an insider or allowed by a predefined access control list (ACL) or conduit. The PIX can be configured to perform many functions, including network address translation (NAT) and port address translation (PAT), as well as being a virtual private network (VPN) endpoint appliance. [16]

The PIX, like many other security devices, has a logging tool. This tool helps security engineers and network administrators to track, debug, and monitor any normal or abnormal security events.

The log classifies events according to their predefined severity: Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, and Debugging.

sample log file extracted from Cisco PIX (Private Internet Table 1 shows a view of the output screen, including tracked events in the PIX firewall. It shows some error logs, for example, one stating no translation found for a specific IP address, and other informational logs of building and denying TCP connections according to the rules of allowing and denying traffic of the PIX firewall, and higher severity logs are also shown, like termination of some TCP or UDP connections because of time out or for other reasons.

Different event meanings are shown in Table 2.

The entire sample log file is examined for entries that can be classified according to the five stages of FM. We can classify each row in the event log by matching the actual meaning of the log with the theoretical concept of the FM classification model (created, processed, received, disclosed, communicated), as shown in Table 3. The table contains only selected rows from Table 2.

The first row in Table 3:

*Login permitted from 53.215.253.172/49810 to Inside:53.215.253.254/https for user *****

is a request to access, and the request is accepted according to authentication. It is received event. Note that the receiving component in the system has its own processing aspect. Received means that the original imported data has been kept in its original form. It could be compared with (operated on), as in this case, a stored file in the receiving state, but the data itself has not been changed in form.

Table 1. Sample logged entries.

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Description
6	Dec 30 2009	04:04:59	305011	192.168.253.120	62.215.253.148	Built dynamic UDP translation from inside2:192.168.253.1
6	Dec 30 2009	04:04:59	302016	187.46.24.211	192.168.253.185	Teardown UDP connection 186409920 for Outside:187.4
6	Dec 30 2009	04:04:59	302016	187.47.99.25	192.168.253.185	Teardown UDP connection 186409919 for Outside:187.4
6	Dec 30 2009	04:04:59	305012	192.168.253.128	62.215.253.148	Teardown dynamic TCP translation from inside2:192.168.
4	Dec 30 2009	04:04:59	106023	96.11.235.34	62.215.253.188	Deny tcp src Outside:96.11.235.34/4679 dst Inside:62.2
6	Dec 30 2009	04:04:59	302015	174.113.186.60	62.215.253.223	Built outbound UDP connection 186413873 for Outside:17
4	Dec 30 2009	04:04:59	106023	69.122.15.231	62.215.253.223	Deny tcp src Outside:69.122.15.231/51299 dst Inside:62
4	Dec 30 2009	04:04:59	106023	78.93.161.232	62.215.253.148	Deny udp src Outside:78.93.161.232/23459 dst Inside:6
4	Dec 30 2009	04:04:59	106023	78.93.161.232	62.215.253.148	Deny udp src Outside:78.93.161.232/23459 dst Inside:6
3	Dec 30 2009	04:04:59	305005	192.168.253.196		No translation group found for udp src Inside:192.168.93
6	Dec 30 2009	04:04:59	302014	213.199.170.73	192.168.93.75	Teardown TCP connection 186413160 for Outside:213.19
6	Dec 30 2009	04:04:59	302014	213.199.170.73	192.168.93.75	Teardown TCP connection 186413159 for Outside:213.19
4	Dec 30 2009	04:04:59	106023	82.60.16.13	62.215.253.13	Deny udp src Outside:82.60.16.13/12720 dst Inside:62.2
6	Dec 30 2009	04:04:59	302021	83.96.24.232	62.215.253.236	Teardown ICMP connection for faddr 83.96.24.232/0 gac
4	Dec 30 2009	04:04:59	106023	114.77.71.43	62.215.253.231	Deny tcp src Outside:114.77.71.43/51985 dst Inside:62.
6	Dec 30 2009	04:04:59	302015	62.78.152.69	192.168.253.120	Built outbound UDP connection 186413871 for Outside:62
4	Dec 30 2009	04:04:59	106023	62.215.0.241	62.215.253.122	Deny udp src Outside:62.215.0.241/49199 dst Inside:62.
4	Dec 30 2009	04:04:59	106023	62.215.0.241	62.215.253.122	Deny udp src Outside:62.215.0.241/49199 dst Inside:62.
6	Dec 30 2009	04:04:59	302016	90.229.251.125	62.215.253.198	Teardown UDP connection 186410115 for Outside:90.229
6	Dec 30 2009	04:04:59	302016	151.53.76.5	62.215.253.198	Teardown UDP connection 186410114 for Outside:151.5
6	Dec 30 2009	04:04:59	302016	207.255.224.225	62.215.253.198	Teardown UDP connection 186410110 for Outside:207.25

Table 2. Different event meanings.

Seq	Event	Meaning
1	Login permitted from 53.215.253.172/49810 to Inside:53.215.253.254/https for user ****	User has been logged in to the system
2	Deny udp src Outside:53.215.0.241/49197 dst Inside:53.215.253.122/2056	System denies the "udp" connection requested from outside source to inside agent
3	Device completed SSL handshake with client Inside:53.215.253.172/49810	Secure Sockets Layer used for transmitting private documents via the Internet
4	Built inbound TCP connection for inside2:192.168.253.129/2608 to Inside:53.215.253.100/110	Connection built on user request and traffic prepared to be sent to the outside
5	portmap translation creation failed for udp src inside2:192.168.253.180/1025 dst Inside	Connection cannot be created between the client and the WWW server
6	53.215.253.179 Accessed URL 213.199.141.140	The user accessed a URL
7	Deny TCP (no connection) from 207.46.148.33/80 to 53.215.253.62/58806 flags SYN ACK	The connection closed (Terminated)
8	Permit TCP connection from 207.46.148.33/80 to 53.215.253.62/58806 flags Backup	The connection has been created
9	SSL client Inside:53.215.253.172/52321 request to resume previous session.	Request from user to restore the session
10	Built outbound TCP connection for Outside:213.199.141.140/80 to Inside:53.215.253.179/1417	Connection built on user request and traffic sent to the inside
11	Deny TCP (no connection) from 65.55.15.123/80 to 53.215.253.62/43197 flags SYN ACK	The connection closed (Terminated)
12	portmap translation created for udp src inside2:192.168.253.180/1025 dst Inside:192.168.93.3/161	Connection created between the client and the WWW server
13	Teardown ICMP connection for faddr 196.221.174.51/0 laddr 192.168.253.115	Connection closed because of SYN timeout
14	Permit outbound UDP connection for Outside:77.28.78.85/10780 to inside2	Connection built on user request and traffic sent to the inside
15	Built inbound ICMP connection for faddr 196.221.174.51/0 laddr 192.168.253.115	Connection built on user request and traffic sent to the outside
16	Teardown dynamic TCP translation from inside2:192.168.253.109/1352 to Outside	Connection closed because of SYN timeout

Table 3. Event classifications according to FM model

	Event	Create	Process	Receive	Release	Transfer
1	Login permitted from 53.215.253.172/49810 to Inside:53.215.253.254/https for user ****			*		
2	Deny udp src Outside:53.215.0.241/49197 dst Inside:53.215.253.122/2056		*	*		
3	Device completed SSL handshake with client Inside:53.215.253.172/49810		*		*	
5	portmap translation creation failed for udp src inside2:192.168.253.180/1025 dst Inside		*	*	*	*
6	53.215.253.179 Accessed URL 213.199.141.140	*	*	*		
8	Permit TCP connection from 207.46.148.33/80 to 53.215.253.62/58806 flags Backup	*	*		*	*
16	Teardown dynamic TCP translation from inside2:192.168.253.109/1352 to Outside				*	*

The second row in Table 3 shows a deny action taken by the security device, where the request was received and processed.

System deny the "udp" connection requested from outside source to inside agent

The request was processed because it involved inside agent. This implies that the original request was analysed to break it down into components.

Note that in such a system, alert is not incorporated as an independent notion into the system. In our methodology, the process may be visualised as follows:

1. Receiving stage: Request Q has been received by user A. (Apparently, user A is a legitimate user, otherwise, it would be denied access, as in the previous case)

2. Processing stage: request has been processed as
"udp" connection requested from outside source to inside agent
The processing module denied permission.
3. Log system: Creating registries of these events in the log system. If (this event has been designated as alarm), then trigger alarm system.
4. Alarm system: Create alarm description, and then trigger response system.
Response system: Instruction to the receiving module to watch out for this user.
Row 3:
Device completed SSL handshake with client Inside:53.215.253.172/49810
shows a different classification event:
Process: The device did a handshake with the host to ensure availability.
Release: After ensuring of host availability, traffic is prepared to be sent to that host.
Row number 4 indicates:
Built inbound TCP connection for inside2: 192.168.253.129/2608 to Inside: 53.215.253.100/110
The entry means four different actions:
1- Received: authenticated user.
2- Processed: authorised operation.
3- Created: built inbound TCP connection.
4- Released: traffic was prepared to be sent "disclosed" to the outside.
Note how the sequence of events was registered by these FM log entries, as shown in Fig. 8. If there is an alert, it involves the entire sequence of events, not only the last one.

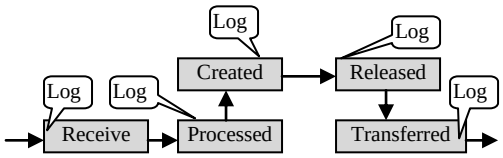


Fig. 8. Map of compound events involved in row 4 of Table 3.

Row 5 states:
portmap translation creation failed for udp src inside2:192.168.253.180/1025 dst Inside

This means the connection cannot be created between the client and the WWW server. In terms of the FM model, the sequence of events is:
1- Receiving: request from the host.
2- Processing: to check for permission
3- Releasing: buffering the data to be sent
4- Transferring: denying the connection requested.
Here the desired connection is not clear. Failure to establish connection may indicate decisions made at several stages. Figure 9 shows the stream of flow of possible communication between source and destination, where the system acts as mediator. The crossed circles denote positions where a decision is made to abort the connection. For example, it is possible that the distinction is a blacklisted site; thus, any request to connect to that site is rejected at the transfer or receive stages.

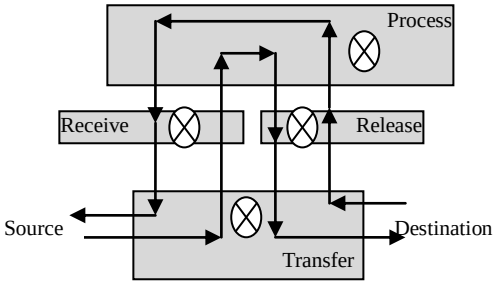


Fig. 9. Streams of flow in line 5, Table 3.

This is contrast to line 6, which states:
53.215.253.179 Accessed URL 213.199.141.140
Here the user requests access to a certain WWW server; after processing, the connection is created.
In row number 8:
Permit TCP connection from 207.46.148.33/80 to 53.215.253.62/58806 flags Backup
"Backup" results from transferring files from their original location to another location like media storage. This would establish a communication channel between source and destination to release and transfer the backup information. Notice that storage in FM is divided logically into five stages. Suppose that the transferred files are log system files. These are created information and should be stored in the new location as such.
Line 16:
Teardown dynamic TCP translation from inside2:192.168.253.109/1352 to Outside
This is an example of an event without receiving that does not involve the receiving stage. It could be because of the connection timeout; hence the system closes the session.
Other events can be classified in the same way. The key issue is knowing the actual meaning of each event in the log so it can be easily classified by mapping it to the theoretical concept of the FM classification model.
For security-related events the FM approach provides a logical map for clear description of the sequence of events that cause a security-related awareness.

VII. Conclusion

This paper presents a theoretical framework for LMS in terms of a flow-based conceptual model with emphasis on security-related events. The framework includes four separate flow systems: active system, log system, alarm system, and response system. All systems are composed in terms of flow systems. The experimental part of the paper concentrates on log analysis in the log system.
The high level modelling methodology provides a promising approach for LMS design. Further research aims at constructing a centralised LMS for simple hardware/ software system where the flowsystem and its classification are applied right from the beginning.

VIII. References

1) Al-Fedaghi, S. (2010). Threat risk modeling. 2010 International Conference on Communication

Software and Networks (ICCSN 2010), Singapore, 26-28 February.
2) Al-Fedaghi, S. (2009). On developing service-oriented Web applications. The 2009 AAAI (Advancement of Artificial Intelligence)/IJCAI (International Joint Conferences on Artificial Intelligence) Workshop on Information Integration on the Web (IIWeb:09), July 11, Pasadena, CA, USA. Paper: http://research.ihost.com/iiweb09/notes/9-P4-ALFEDAGHI.pdf
3) Al-Fedaghi, S. (2009). Flow-based description of conceptual and design levels. IEEE International Conference on Computer Engineering and Technology 2009, January 22-24. Singapore.
4) Al-Fedaghi, S., & Mahdi, F. (2010). Events classification in log audit. International Journal of Network Security & Its Applications (IJNSA), 2(2). http://airccse.org/journal/nsa/0410ijnsa5.pdf
5) AIX, System management concepts: Operating system and devices (1st ed.) Chapter 3, Auditing overview. (September 1999). http://www.chm.tu-dresden.de/edv/manuals/aix/aixbman/admnconc/audit.htm
6) Dijkstra, E. W. (2003). On the role of scientific thought. http://www.cs.utexas.edu/users/EWD/transcriptions/EWD04xx/EWD447.html
7) Becta. (2009). Good practice in information handling: Audit logging and incident handling. Becta, V2, March 2009 http://schools.becta.org.uk/upload-dir/downloads/audit_logging.doc
8) GFI. (2008). Auditing events. http://docstore.mik.ua/manuals/hp-ux/en/5992-3387/ch10s04.html
9) Fischer, R. (2007, April). Motivations and challenges in designing a distributed log management framework. Diploma Thesis, Institut f¨ur Softwaretechnik und interaktive Systeme. http://cocoon.ifs.tuwien.ac.at/lehre/diplomarbeiten/2007_Fischer.pdf
10) Gerhards, R. (2005, Oct.). The syslog protocol. http://tools.ietf.org/html/draft-ietf-syslog-protocol
11) Kazienko, P., & Dorosz, P. (2004). Intrusion detection systems (IDS) Part 2 - Classification; methods; techniques. WindowsSecurity.com.
12) http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html
13) GFI EventsManager. (2009, October). GFI Software Ltd. Manual. http://www.gfi.com/esm/esm8manual.pdf
14) SANS Consensus Project. (2007). Information system audit logging requirements. SANS Institute. http://www.sans.org/resources/policies/info_sys_audit.pdf
15) The Apache Software Foundation. (2006). Common log format. .http://httpd.apache.org/docs/2.2/logs.html#accesslog
16) W3C Working Draft 8, Web Services Architecture, August 2003.
17) Cisco PIX, Dec 2009. http://en.wikipedia.org/wiki/Cisco_PIX
18) Försvarets Materielverk, FMV (Swedish Defence Material Administration), Design Rule: Security aspects of information, 2008-04-30. https://www.fmv.se/upload/Bilder%20och%20dokument/Vad%20gor%20FMV/Uppdrag/LedsystT/FMLS%202010/FMLS%20Design%20Rules/LT1O%20P06-0108%20DR%20Security%20aspects%20of%20information%203.0.pdf
19) Kent, K., & Souppaya, M. (2006, Sept.) Guide to computer security log management. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-92. http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
20) Shenk, J. (2008, Oct.). Log management in the cloud: A comparison of in-house versus cloud-based management of log data. SANS Whitepaper. http://www.sans.org/reading_room/analysts_program/LogMgmtCloud_Oct08.pdf
21) Shenk, J. (2010, Apr.). SANS sixth annual log management survey report. SANS Whitepaper. https://www.sans.org/reading_room/analysts_program/logmgtsurvey-2010.pdf
22) Mueller, P. (2008, May 31). Facing the monster: The labors of log management. InformationWeek. http://www.informationweek.com/news/global-cio/compliance/showArticle.jhtml?articleID=208400730
23) Olzak, T. (2010, Apr. 24). Five common gaps in logical network security. Bright Hub, Edited & published by Michele McDonough. http://www.brighthub.com/computing/enterprise-security/articles/66298.aspx?p=2
24) Adam, S. (2002). A new architecture for managing enterprise log data. In: Proceedings of the 16th Systems Administration Conference (LISA-02). Philadelphia, PA: USENIX Association, 121–132.

A Transformation Scheme for Deriving Symmetric Watermarking Technique into Asymmetric Version

Rinaldi Munir[1] Bambang Riyanto[2] Sarwono Sutikno[3]

Wiseto P. Agung[4]

GJCST Computing Classification
I.4.5, G.0

***Abstract*-This paper proposes a transformation scheme for rendering the asymmetric watermarking technique into its asymmetric version. The asymmetric technique uses secret watermark as private key and public watermark as public key. The public watermark has a normal distribution and the private watermark is a linear combination of the public watermark and a secret sequence. The detection process is implemented by correlation test between the public watermark and the received image. The scheme is used to transform Barni Algorithm, a symmetric watermarking technique, into a asymmetric version. Experiments showed that the asymmetric technique was proved as robust as its symmetric version against some typical image processing schemes.**

Keywords- asymmetric watermarking, Barni Algorithm, transformation, correlation.

I. Introduction

Digital watermarking has been used widely as a tool for protecting copyright of digital multimedia data (e.g images) [1, 2]. Many digital watermarking techniques for still images have been proposed [1-3]. The particular problem with the state-of-the-art watermarking techniques is that the majority of these schemes are symmetric: watermark embedding and detection use the same key. The symmetric watermarking scheme has a security problem: once attacker knows the secret key, the watermark not only can be detected, but it can be easily estimated and removed from the multimedia data completely and thereby defeat the goal of copyright protection.

A solution to solve the problem is the asymmetric watermarking scheme, in which different key(s) are used for watermark embedding and detection. An asymmetric watermarking system uses the private key to embed a watermark and the public key to verify the watermark. Anybody who knows the public key could detect the watermark, but the private key cannot be deduced from the public key. Also, knowing the public key does not enable an attacker to remove the watermark [3].

Review of several existing asymmetric watermarking techniques can be found in [3]. The asymmetric techniques proposed until now can be classified into two categories [8]. The first category is watermark-characteristics-based-method where the watermark is the signals which have special characteristics such as periodicity. The other is transform-based-method to make a public key from a given private key by a proper transform. Legendre-sequence-key et al. [5] belong to the first category, whereas Hartung and Girod's [6] and Gui [7] techniques belong to the second category.

Many symmetric watermarking techniques have been proposed and some of them have good results in robustness and imperceptibility. Thus we have an idea to derive a symmetric watermarking technique into its asymmetric version, because designing a new asymmetric watermarking technique may need intensive effort and time. In this paper, we contribute to propose a transformation scheme which can be used to derive the symmetric technique into its asymmetric version. We choose a classical symmetric watermarking technique which has good robustness and imperceptibility, i.e. Barni Algorithm [9]. We use the scheme to derive an asymmetric version of Barni Algorithm

II. Proposed Scheme

In several symmetric techniques, the secret key is the watermarks itself where they have the normal distribution. In asymmetric version of the symmetric technique, the private key and the public key is referred as the private watermark (Ws) and the public watermark (Wp) respectively. The public watermark should have a correlation with the private watermark, because the detection is implemented by using correlation test between the public watermark and the received image.

In our scheme we map the symmetry method into the asymmetry version. Based on the compatibility between symmetric and asymmetric watermarking method, then in the mapping no change in the watermark embedding algorithm. Watermark embedding on the asymmetric version is same as the original method (symmetric), but watermark detection algorithm is a slight change. The change is in the reference watermark used in correlation test. In the symmetric method correlation test performed between the received image and original watermark, then in the asymmetry version correlation test is performed by the received image and the public watermark

A new process added to the mapping is a transformation of a private watermark to produce a public watermark. The public watermark W_p is generated by the transformation f to the private watermark W_s,

$$W_p = f(W_s) \qquad (1)$$

Fig.1 shows the transformation diagrams. The transformation f is a one-way function, so that

About-[1,2,3] Rinaldi Munir, Bambang Riyanto, Sarwono Sutikno (School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia).(e-mail;rinaldi-m@stei.itb.ac.id[1],briyanto@lskk.ee.itb.ac.id[2] ssarwono@gmail.com[3]

About-[4] PT.Telekomunikasi,Indonesia(e-mail; wiseto@telkom.co.id)

computationally almost impossible to derive private watermark from the corresponding public watermark. One-

process of transformation the symmetric watermarking method into its asymmetric version.

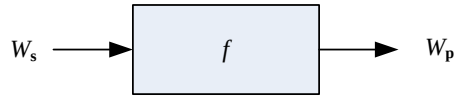


Fig. 1. Transformation of the private watermark to the public watermark

We design both of watermarks to have normal distribution, as the choice of this distribution gives resilient performance against collusion attack [1]. We use a concept in statistics to design a function *f*.

In statistics, if we add two or more random variables as a linear combination where each of them has normal distribution, then the result has normal distribution too. Let X be a sequence with mean μ_1 and variance σ_1^2 and Y be sequence that independent from X with mean μ_2 and variance σ_2^2. A combination linear of X and Y is defined as $Z = aX + bY$ where a and b is parameters. Sequence Z has the mean $\mu_3 = a\mu_1 + b\mu_2$ and variance $\sigma_3^2 = a^2\sigma_1^2 + b^2\sigma_2^2$ [10].

In generating the watermarks we have to ensure that the combination linear is secure. It means that the private watermark cannot be deduced from the public watermark. Furthermore, knowing the public watermark does not enable a user to remove the embedded watermark from the watermarked image. This characteristic is realized by adding the public watermark with a secret sequence. Security of this asymmetric version depend on the secret sequence. Let W_p be the public watermark and R be the secret sequence, the private watermark can be obtained by adding W_p and R as

$$W_s = f(W_p, R) = \beta_0 W_p + \beta_1 R \qquad (2)$$

where β_i is a parameter in [0, 1] to control the trade off between the two sequences and $\beta_0 + \beta_1 = 1$. In order to make the sequence R is more secure, we encrypt R by a random permutation before adding with W_p. Thus, eq. (2) can be written as

$$W_s = f(W_p, R) = \beta_0 W_p + \beta_1 \tilde{R} \qquad (3)$$

where $\tilde{R}$ is encrypted version of R. Fig. 2 shows the process of generating the public and the private watermark.

The private watermark W_s is embedded into the image according to the equation used by its symmetric technique. In the detector side, using the public watermark, W_p, the test correlation is computed to accomplish the watermark detection.

way nature of this property is important to provide security on asymmetric watermarking method. The Function f is core

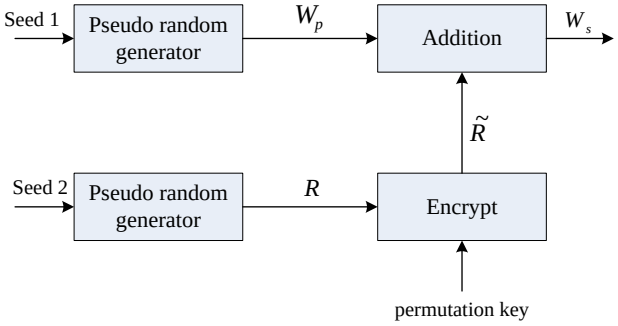


Fig. 2. Generating of the public and the private watermark

III. Security Analysis

Because of the public watermark, detector, and watermarked image are publicly available (not secret), the attacker uses the public information to deduce the private watermark W_s. Such attacks are called public attack. Once W_s can be calculated, then W_s is removed from the watermarked image by performing a subtraction operation on watermark embedding formula (depending on methods).

Security of this transformation scheme is based on two factors as follows:

A. One-way function

One-way functions are commonly used in cryptography to enhance system security. In the one-way function, computing to evaluate function value of the variables is relatively easy, but to discover variables value of the function value is relatively computationally difficult and even impossible. In Eq. (3) parameter R can be viewed as trapdoor, it is impossible to find Ws without knowing the trapdoor, because the attackers must do the inversion of the one-way function. The attacker knows Wp but he (or she) does not know R. Because of $\tilde{R}$ is an encrypted version of R, the attacker must know the R before getting $\tilde{R}$.

B. Permutation

Let the attacker knows R, next he (or she) needs to know a random permutation used to encrypt R. Because cardinality of R is n, the attacker must try $n!$ permutation to find the right one. Remember that n is large enough, it is about 25% of original image size, so that finding the right permutation needs $O(n!)$ computation. For n = 10000 as example, there are 10000! computation. We conclude that it is impossible for attackers to deduce the private watermark from these public information.

IV. Case Study: Transformation of Barni Algorithm

In this section we present derivation of a symmetric watermarking method into the asymmetric version based on transformation scheme which has been described in Section

II. The symmetric watermarking method is a classic method, i.e Barni Algorithm.

In Barni Algorithm, the watermark consists of a pseudo random sequence of M real number, $W = \{w(1), w(2), ..., w(n)\}$, that has a normal distribution with *mean* = 0 and *variance* = 1. The watermark W is inserted into selected DCT coefficients, $V = \{v(1), v(2), ..., v(n)\}$. The watermark detection is done by computing correlation between the selected DCT coefficients from a possibly corrupted image I^*, i.e. $V^* = \{v^*(1), v^*(2), ..., v^*(n)\}$.

In the asymmetric version of Barni Algorithm, we use two watermarks, the first is a private watermark, $W_s = \{w_s(1), w_s(2), ..., w_s(M)\}$, that embedded into the host image and the second is a public watermark $W_p = \{w_p(1), w_p(2), ..., w_p(n)\}$, for detection phase. Both of the watermarks are generated by the procedure explained in Section 2. The private watermark is embedded into the image according to formula:

$$v_w(i) = v(i) + \alpha \left| v(i) \right| w_s(i) \qquad (3)$$

In the detector side, using the public watermark, W_p, the following correlation is computed:

$$c = \frac{1}{n}\sum_{i=i}^{n} v^*(i) \cdot w_p(i) \qquad (4)$$

After we set the threshold T, the watermark detection is finished by comparing c and a threshold. The threshold is depend on the received image and calculated with following formula:

$$T = \frac{\alpha}{3n}\sum_{i=1}^{n}\left|v^*(i)\right| \qquad (5)$$

V. Simulation and Results

We apply our method to image watermarking by using MATLAB as programming tool. The test image is a 512 × 512 color image 'train'. Size of the private watermark is n = 16000. The watermark and the secret sequence R have a normal distribution with *mean* = 0 and *variance* = 1. The public watermark is generated by function f which has been explained in Section II with β_0 is equal to 0.8 and β_1 = 0.2. The embedding strength α is equal to 0.25. Histogram of the public watermark and the private watermark is shown in Fig. 3. From Fig. 2(b) we observe that shape of distribution graphics of the private watermark is like a bell as common standard normal distributions.

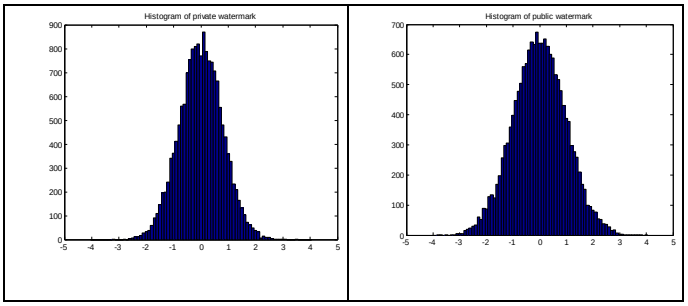
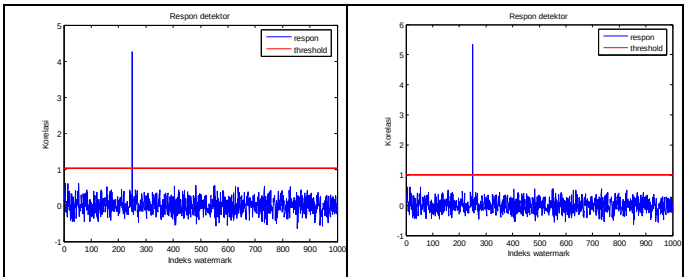


Fig.3. Histogram of the private and public watermark

Before embedding the private watermark, the original image is transformed from *RGB* to *YcbCr*. The watermark is embedded to luminance component (*Y*) only, and the final result is retransformed from *YcbCr* to *RGB*.

Figure 4(a) shows the original image and Figure 4(b) shows the watermarked image (PSNR = 36.9833). Visually the watermarked image quality was almost identical with the original image. Figure 4(c) shows response of a public detector to 1000 random watermarks, one of them (index 250) is a public watermark that have a correlation with the private watermark. Such images provide two interpretations [9]. The first interpretation, the response to the public watermark is compared with the T to decide the existence of the (private) watermark within the image. The second interpretation, if people do not know which watermark is embedded in the image, then response from all the public watermark is compared and the highest response is selected. Response from the public watermark is should be the highest compared with the others and this suggests the existence of a corresponding private watermark in the image.

(a) Original image (b) Watermarked image



(c) Response of public detection (c) Response of private detection

Fig. 4. Output of watermark embedding and detection on 'train' image .

Figure 4(c) shows that the correlation test with the correct public watermark correlation value is significantly higher than the other. The threshold T is calculated analytically from equation (5) is 1.0188. In case there is no attack on the watermarked image, the detector gives the value c = 4.2512. Because c > T, it can be concluded that the image contains the (private) watermark. For comparison, in private

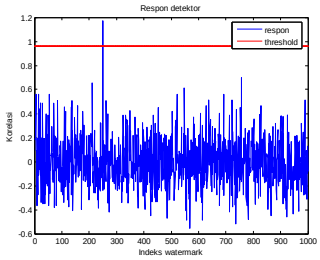
detection (using the private watermark on correlation test) gives c = 5.3251 (Fig. 4(d)).

The next experiment was done to see robustness of the watermark against some non-malicious attacks, which is the general operations performed on image processing (cropping, compression, low-pass filtering, etc.). We use Jasc Paint Shop version 6.01 as image processing software. The experiments and results are explained as follows.

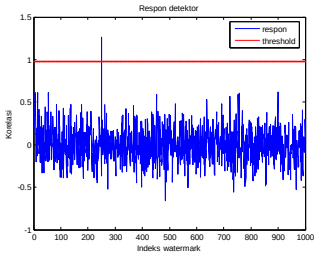
V.1. Experiment 1: JPEG Compression

We tested the robustness against JPEG compression with extreme compression qualitie. For compression quality 6%, the watermark can be detected succesfully (c = 1.1727, T = 0.9602). For comparison, in private detection (using the private watermark) gives c = 1.4632). See Fig. 5

(a) JPEG image with low compression quality



(b) Response of public detection

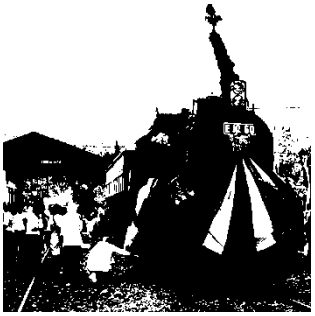


(c) Response of private detection

Fig 5. JPEG compression with compression quality 6%. The watermark can be detected

V.2 Experiment 2: Dithering

We convert the watermarked image to a binary image by dithering operation. It means plenty of gray-level information lost. It is shown in Fig. 6 that the watermark still can be detected. The response to the right watermark is largest among the response to all the watermarks (c = 3.4352, T = 2.4982).



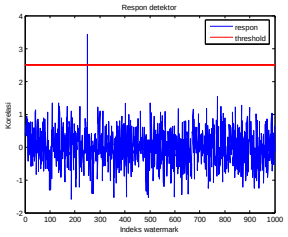


Fig. 6. (a) Dithering. (b) Response of public detector

V.3. Experiment 2: Image Cropping

Image cropping will remove some watermark information. In our simulation, we cut unimportant part from the watermarked image (about 50%), the missing part of the image is replaced with black pixels (see Figure 7a). In fact, we can always correctly detect the watermark because the correlation value (c = 2.1752, T = 0.8579) is still greater significantly than the others. For comparison, in private detection gives c = 2.7349.

(a) Cropped image

(b) Image after histogram equalization

Fig. 7. Image cropping and histogram equalization

V.4. Experiment 4: Histogram Equalization

The watermarked image is adjusted so that distribution of gray-level is uniform by using histogram equalization operation (a typical low-pass filtering operation, see Fig. 7(b)). Experiment shows that the watermark can be detected where c = 6.4877, T = 1.2269. For comparison, in in private detection gives c = 8.1186.

V.5. Experiment 5: Resizing

The watermarked image is resized until 50% of the original size. Experiment shows that the watermark still can be detected. For resizing up to 200% of the original image, the watermark still can be detected well (we found that c = 1.8030, T = 0.4520). For comparison, in in private detection gives c = 2.2571

VI. Discussion

Based on a series of experiments that have been done for asymmetric version of Barni algorithm, it has achieved some results which are analyzed as follows.

A series of experimental results show that the asymmetric

version remains robust to typical image processing operations like JPEG compression, histogram equalization, dithering, cropping, and resizeng. Detector response of asymmetric method is not much different to original symmetric version, and correlation values yielded by detector not differ significantly

VII. Conclusion

In this paper a scheme for deriving a symmetric watermarking technique into its asymmetric technique has been proposed. For test case, Barni algorithm, a classical image watermarking, is successfully transformed into an asymmetric watermarking technique. This technique uses two watermarks: the first watermark is a public watermark used for public detection, and the second watermark is a private watermark that has a correlation to the public watermark. The private watermark is a linear combination of the public watermark and an encrypted version of a secret sequence. Security of this asymmetric technique is based on one-way function with trapdoor and the difficulty of finding the secret sequence where it needs O(n!) computation. Simulations against various attacks confirmed that this asymmetric technique is as robust as its symmetric version

VIII. References

1) Ingemar J. Cox, et al, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. On Image Processing, Vol. 6, No. 12, Dec 1997, pp.1673-1687.
2) Mauro Barni, Franco Bartolini, Watermarking Systems Engineering, Marcel Dekker Publishing, 2004.
3) Joachim J. Eggers, Jonathan K. Su, and Bernd Girod, Asymmetric Watermarking Schemes, GMD Jahrestagung, Proceedings, Springer-Verlag, 2000.
4) R.G. Schyndel, A.Z.,Tirkel, I.B. Svalbe, (1999): "Key Independent Watermark Detection", in Proceeding of the IEEE Intl. Conference on Multimedia Computing and Systems, volume 1, Florence, Italy.
5) J.J. Eggers, J.J., J.K. Su, B. Girod (2000): "Public Key Watermarking by Eigenvectors of Linear Transform", EUSIPCO 2000.
6) F. Hartung, F. and B. Girod (1997): "Fast Public-Key Watermarking of Compressed Video", Proceedings of the 1997 International. Conference on Image Processing (ICIP).
7) Guo-fu Gui, Ling-ge Jiang, and Chen He, "A New Asymmetric Watermarking Scheme for Copyright Protection" IECE Trans, Fundamentals Vol. E89-A, No 2 February 2006.
8) Geun-Sil Song, Mi-Ae-Kim, and Won-Hyung Lee, "Asymmetric Watermarking Scheme Using Permutation Braids", Springer-Verlag, 2004.
9) Mauro Barni, F. Bartolini, V. Cappellini, A.Piva, "A DCT-Domain System for Robust Image Watermarking", Signal Processing 66, pp 357-372, 1998.
10) Walpole, Ronald E., Myers, Raymond H., (1995), Probability and Statistics for Engineers and Scientists, Mc. Graw-Hill, 1995

A Novel Scheme to Support WiMax/WiFi Vertical Handoff using SIP

Dr. V.Sumathy[1]

E.Prince Edward.[2]

GJCST Computing Classification C.2.1

***Abstract*-In recent days vertical handoff has become one of the most challenging issues in wireless and mobile networks ,when users roam between different access networks. Managing vertical handoff have been proposed and realized on different layers. In this paper a novel scheme named Modified SIP (MOD-SIP) is proposed for WiMax/WiFi vertical handoff in application layer. Our proposed scheme aims to provide (i) better charging procedures during handoff to support network service providers. (ii) minimizes the workload on CH to perform handoff (iii) a better way to eliminate the stale address situation. We have developed a prototype model in java and tested it in different real-time user scenarios. We have measured throughput and packet loss and the performance characteristics of MOD-SIP are studied. The results reveal that both handoffs i.e. from WiMax to WiFi network and from WiFi to WiMax network work well and fulfill our aims, but have some limitations in packet loss and handoff latency. Hence further works are carried out to reduce packet loss and achieve low latencies.**

Keywords-MOD-SIP, Wifi,Wimax, Vertical Handoff, SDP(Session Description protocol), Handoff Phases.

I. Introduction

Future generation wireless networks is striving to integrate different wireless access networks such as IEEE 802.11, IEEE 802.16, 3G, GPRS, UMTS to achieve a ubiquitous computing environment. Hence heterogeneous wireless networks have to cooperate in providing users with better quality of service (QoS) and seamless mobility. One of the important wireless technologies today is WiFi. Standard personal devices like Laptop, mobile devices uses WiFi technology to connect to the Internet. But its range is very limited. The new emerging wireless technology is IEEE 802,16 WiMax(Worldwide Interoperability for Microwave access). WiMAX is a relatively new but very promising standard for wireless communication because it provides the speed of WiFi and the coverage of UMTS (Universal Mobile Telecommunications System). Wireless LAN's limited coverage range makes it difficult to support a ubiquitous computing environment. 3G can offer universal network access its access rate is very limited. WiMax can provide high speed internet access in wide area. Hence it is natural to combine WiMax and WiFi and create a better wireless solution to provide high speed Internet for mobile users In general in heterogeneous networks seamless handoff is achieved with the help of handoff management protocols. Handoff management have been proposed in different OSI layers. Mobile IP[1] a standardized protocol by IETF for IP Mobility functions in the network layer. SCTP[3] (Stream Control Transmission protocol), functions in the transport layer. When these protocols are used modifications have to be done in the mobile devices at network and transport layers, respectively. Session Initiation Protocol (SIP) [2], which functions in the application layer, is transparent to the underlying networks. Hence, modifications are not required at underlying layers. We have done a survey of seamless vertical handoff schemes for WiFi/WiMax heterogeneous wireless networks[12]. Based on that, we have chosen Session Initiation Protocol in the application-layer and studied the handoff characteristics of the mobile node.

Several works have been carried out in vertical handoff, but most of them is related to WWAN and WLAN [6]. Authors in [7] have considered real-time applications but they have not given importance to network service provider environment .In [11] authors have proposed a scheme in which a CH bicasts in the handoff region. This adds additional load to the CH and becomes critical in real user environment. Vertical handoff between WiFi and WiMax is presented in [12]but they have used mSCTP which does not support network service provider environment . In our paper we have presented MOD-SIP by modifying the Mid-call mobility in SIP in order to fulfill the proposed criteria in WiMax/WiFi heterogeneous networks. Overview of IEEE802.11 and IEEE802.16 is presented in section II. SIP based terminal mobility with MOD-SIP is explained in section III. The fourth section deals with the vertical handoff between WiMax and WiFi networks. Simulation and evaluation using MjSip is presented in section V followed by conclusion

II. Protocol Overview

A. Overview of WiFi

The IEEE 802.11 standard [15] provides low cost and effective wireless LAN service. The deployment of high speed network (11Mbps in 802.11b and 54Mbps in 802.11a/g) can be easily established by the free and unlicensed spectrum (2.4GHz in 802.11b/g and 5GHz in 802.11a). The IEEE 802.11b standard is one the most commonly used standards for the WLAN. There are 11 available channels in this standard and 3 of them are non-

About-[1]Asst.Professor,Dept. of ECE ,GCT, Coimbatore. India (e-mail;sumi_gct2001@yahoo.co.in)

About[2] Dept. of Electronics, VLBJ Polytechnic College, Research Scholar, Anna University, Coimbatore. India (e-mail;edprince_in@yahoo.com)

overlapping channels. On the PHY layer, it employs the Direct Sequence Spread Spectrum (DHSS) technique with Complementary Code Keying (CCK) modulation scheme. This standard operates in two modes: One is the Ad Hoc Mode and the other is the Infrastructure Mode. The Ad-hoc mode of operation allows the computing devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points. In an Infrastructure type of a WLAN, an Access Point is used to connect computing devices to wired nodes. In this paper we have considered the later type of a WLAN setup.

B. Overview of WiMAX

WiMAX, is a new emerging Wireless technology based on the IEEE 802.16 standard[14]. Its main objective is to provide broadband wireless access over long distances. WiMax base stations can offer greater wireless coverage of about 5 miles, with LOS (line of Sight) transmission within bandwidth of upto 70mbps.The most popular WiMax standards are IEEE 802.16d and IEEE 802.16e.The IEEE 802.16d was proposed in 2004 called fixed WiMAX created by WiMAX Forum [2], but it does not support for mobility. The second standard is IEEE 802.16e proposed in 2005. It is introduced to support for mobility and is called mobile WiMAX. WiMAX specifies the MAC layer and the PHY (physical) layer. These specifications describe the air interface between a Base Station (BS) and a Mobile Station (SS). WiMAX operates in two modes. One is point-to-multipoint (PMP) mode and and the other is mesh mode. In PMP mode every Mobile Station (MS) makes its own connection to the Base Station(BS), whereas in mesh-mode every MS gets connected to BS through the other MS. WiMAX is based on the RF technology called Scalable Orthogonal Frequency Division Multiple Access (SOFDMA). This can be described as a division of the frequency band into several sub-carriers. And also the inclusion of (MIMO) Multiple Input Multiple Output, means that both transmitter and receiver use multiple antennas along with flexible sub-channelization schemes enable the Mobile WiMAX technology to provide high data rates and larger coverage and better performance.

III. SIP MOBILITY SUPPORT

SIP (Session Initiation Protocol) as defined by the IETF in RFC 3261[2] is an application layer control signaling protocol used to establish, modify and terminate sessions in an IP based network. Such sessions could be among two or more users and could include Internet Telephone calls, multimedia distribution and multimedia conferences. SIP runs on top of several different transport protocols. SIP can support terminal, session, personal and service mobility [4]. Terminal mobility is one in which a MN moves between different access networks and continues any ongoing session without any break during its movement. Two types of terminal mobility is supported by sip. One is the Pre-Call mobility, and the other is the Mid-Call mobility. In Pre-call mobility a connection is established during the beginning of a new call when the MN has moved already and to a foreign network, whereas in mid-call mobility during the middle of an ongoing session.

A. Existing Mid-call mobility

In most of the existing Mid-Call mobility support, SIP re-INVITE method is used as a solution. Here the MN's movement to a new network is directly informed to the CH using the SIP request. According to [2] a SIP User agent is capable of initiating a request and modify an existing session.
This is done by sending a new INVITE message using the same Call-ID.

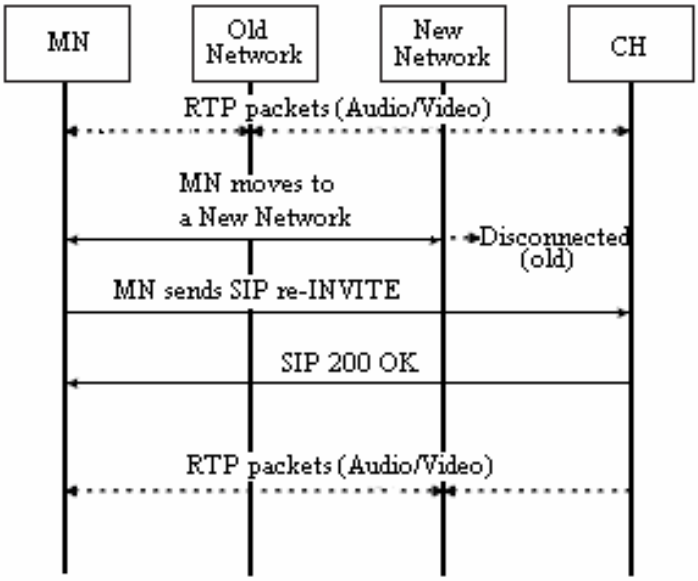


Fig. 1. Mid-Call Mobility

A SIP mid-call mobility scenario is shown in the fig .1.Here when the MN moves to a new network in the mid of a session it obtains a new IP address and attaches it with the re-INVITE message and sends to CH informing about its change in location. On receiving re-INVITE the CH responds with SIP 200 OK and the session continues.

B. Problems in Existing Mid-call mobility

(i)In the re-INVITE method[2], there is a direct end to end communication between the MN and the CH. In such case , the CH is responsible for performing the handoff by establishing a new media session using the IP address of the MN in the new network. Hence the CH must be capable enough to handle the handoff situation completely which becomes difficult in a real user scenario. (ii)When the CH due to some reason has lost the address of the mobile host, it must have a fall-back mechanism to overcome the situation. For example when we have two mobile hosts having a conversation and when driving through a tunnel both loses its connection for a while and when the connection is regained , both would have got a new IP address totally different from that of the old one[4]. Such situations can be avoided by sending retransmissions of invitations also to the SIP server located in the MN's home network. The CH can relocate a MN by contacting the SIP server in the MN's

home network. (iii)In network service provider environment information about location change has to be send to the SIP server before thenew SIP session starts between the MN and CH which is not possible in the existing mid-call mobility support. This is important to enable proper charging because prices in two different networks can be different. But charging procedures using AAA server is not considered and it is beyond the scope o f t he paper.

C. Modified mid-call mobility(MOD-SIP)

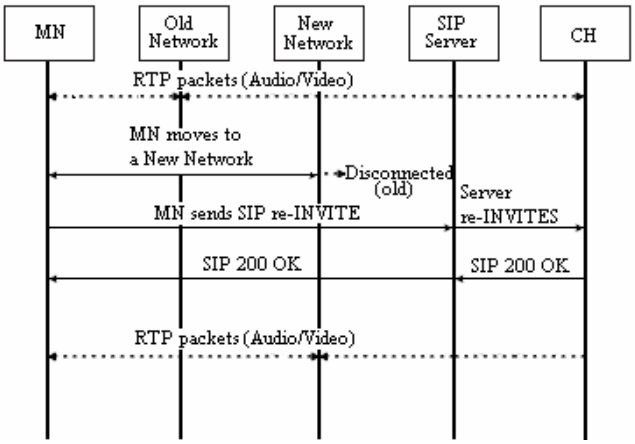


Fig. 2. Modified Mid-call Mobility

In this paper we propose a novel method which provides solutions for all the problems in the existing mid-call mobility support. But in our MOD-SIP the handoff is totally performed by the sever and the CH is totally unaware of the handoff taking place. This totally reduces the load on the CH to perform handoff. And also the change in access technology is handled by the server. This scheme also supports the stale address situation because every move of MN is registered in the server and known to the server In the author has proposed a solution where the movement about the MN is informed to the SIP server only after the SIP re-INVITE message is sent to CH [9]. However, in network service provider environment the information about new location of MN should be known to SIP server before the new session starts between MN and CH. This should be done for proper charging because prices in two different networks may vary. The proposed modified mid-call mobility , is shown in Fig.2 Here when the MN moves to a new network in the mid of a session, it informs the SIP server about its change in location by sending a re-INVITE message. In turn the server informs the CH about MN's new location by sending the re-INVITE message. After receiving 200 OK from the CH the session continues. The advantage of MOD-SIP is that every movement of MN to a new location is registered in the SIP server prior to its move, enabling the network service providers to acquire MN's information irrespective of its location.

IV. Handoff between WiFi and WiMax Networks

A. Handoff Phases

Handoff in mobile networks can be classified into two types one is horizontal handoff and the other vertical handoff. When the Mobile node switches between base stations or access points within the same wireless access networks is called as horizontal handoff. When it switches between heterogeneous networks is called as vertical handoff. Viz., the handoff within Wi-Fi is horizontal handoff and the handoff from Wi-Fi to WiMAX is vertical handoff. The future mobile terminals must be dual mode terminals, capable of connecting to both 802.11 and 802.16 heterogeneous networks so that users can roam freely experiencing better Qos. Handoff between WiMax and WiFi networks is shown in Fig. 3.Handoff can be carried out in three phases. They are (i) network detection, (ii) handoff decision and (iii)handoff execution. In network detection phase the mobile terminal detects a new network. All the network interfaces has to be activated in order to detect a new network quickly. Hence while roaming in a heterogeneous environment the mobile terminal has to monitor and trigger the handoff whenever it moves outside the network coverage.

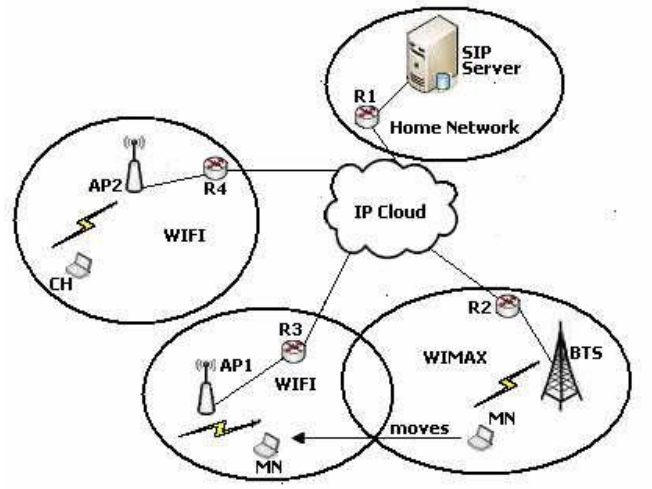


Fig. 3. Proposed Network Model

Handoff for decision is made in the second phase. Here the decision is made based on some threshold levels of performance metrics. In handoff process this phase is more critical because if decision is not made properly there will be high degradation in the Qos. According to the predefined Threshold level handoff takes place from one network to another network.

The third phase is responsible for switching the traffic to a new network. It means that the connection with an old network is terminated and all the traffic traverse the new network.

V. Simulation And Evaluation

We have developed a prototype model by modifying MjSip open source Java SIP stack[16] according to our proposed solution. We have written our own coding in java for WiMax and Wifi networks. Here the SBC(session border controller)of the MjSip is modified to support handoff and used as the SIP server. Fig. 3 shows our simulation network model. We have defined MN which is a dual mode terminal,

which can be connected to both WIFI and to WIMAX network. Static IP addresses were assigned for mobile nodes, SIP server and Access Points. A new SIP message called INVITE_HANDOFF is defined which is similar to the SIP INVITE message. This message is sent to the SIP server from the MN whenever handoff occurs. The movement pattern of MN in the mid of a session from WiMax to WiFi network and vice versa is studied. The handoff process is initiated by the decision for handoff which is a simple decision function written inside MjSip stack to initiate handoff.

The simulation period was set to 180 sec. For exchange of RIP messages and for network routing to set automatically it takes 100 sec initially. Between MN and CH the media streaming application with SIP signalization was used. The streaming application time between MN and CH was set to 60 sec. During that time MN will move from WiMax to the WIFI network coverage and then return back from the WIFI network. The average media packet size is taken as 500 bytes and the approximate transmit rate as 100 packets / second. The threshold level of S/N is set as 10dB. The average end to end latencies across WIMAX network is 120ms and WiFi network
is 10 ms for one way.

A. Simulation results

In the simulation the handoff time and packet loss during handoff is measured and its performance is analyzed. calculation. Handoff execution consumes maximum time among the overall handoff time. A new SIP session establishment, is defined as a time interval from decision for handoff to the time when new session is established via new network. After exchanging the SIP messages for new session RTP packets between MN and CH is sent via the new network. To calculate the overall handoff delay this time interval needs to be added to new SIP session establishment time. The delay taken for Handoff is calculated according to (1)

$$D_{handoff\_time} = D_{new\_session} + D_{first\_RTP\_packet} \quad (1)$$

The $D_{new\_session}$ is the delay added for the exchange of all SIP messages and $D_{first\_RTP\_packet}$ is the delay added for first RTP packets to traverse to the new the network. When new SIP session is established the RTP packets between MN and CH traverse to the new network, but there are still some packets that traverse the old network. Those packets are lost and will be discarded. The proportion of the lost packets represents the packet loss during handoff and is defined as in (2).

$$packet\_loss = 1 - (received\_packets / sent\_packets) \quad (2)$$

The number of packets is measured on the MN (received packets) and CH (sent packets) in time period from SIP INVITE_HANDOFF message to the time when first RTP packets arrive.

B. Handoff From WiMax to WiFi

In Fig. 4 throughput on all interfaces of MN is presented for handoff from WiMax to WiFi. As it is observed from the graph that THS/N is exceeded at 124.9 sec of the simulation and the handoff is executed. Immediately the SIP INVITE_HANDOFF message is sent via WiFi TX to the SIP server to handle the handoff situation whereas the RTP packets still traverse the WIMAX TX. After receiving SIP 200 OK from the SIP server the RTP packets start traversing the WIFI TX. Now the throughput on WIMAX receiver and transmitter starts to decrease, while the throughputs on WIFI interfaces starts to increase.

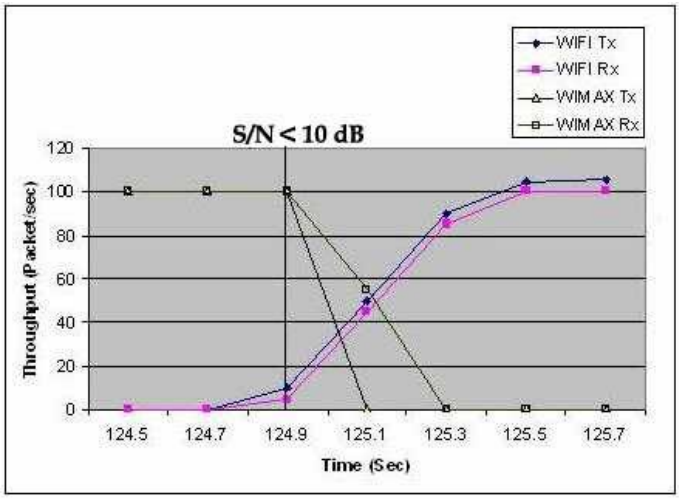


Fig. 4. Throughput on all interfaces of MN (WiMax to WiFi)

Table 1 shows the handoff characteristics measurements for WiMax to WiFi. From the results it is observed that handoff time to WIFI network is not critical. This is because of the very fast connection in WIFI network, which enabled quick SIP session setup in 49 ms and first RTP packets transmission of in 14 ms. But the packet loss during handoff is 28 % which can be critical. Such a proportion of discarded packets happened due to bigger delay in WIMAX network and large number of packets in WIMAX network.

Parameter	Value
$D_{new\_session}$	49ms
$D_{first\_RTP\_packet}$	14ms
$D_{handoff\_time}$	63ms
Packet Loss	28%

Table 1. Handoff measurements (WiMax to WiFi)

C. Handoff From WiFi to WiMax

In Fig.5 throughput on all interfaces of MN is presented for handoff from WiFi to WiMax. As observed from the graph the S/N ratio of WiFi network felt below $TH_{S/N}$ at 145.3 sec of the simulation. This started handoff process. It is also observed that the SIPINIVTE_HANDOFF message was sent via WIMAX Tx and Rx of MN, while for the RTP stream still old network has been used (i.e. packet traversing via WIFI Tx and Rx interface of MN). Because of bigger delays in WIMAX network the SIP message exchange was longer than in the previous case. After the SIP 200 OK, MN started to sent RTP packets via new network. When this happened throughputs on WIFI Rx and Tx interfaces started to decrease, while throughputs on WIMAX Rx and Tx interfaces started to increase.

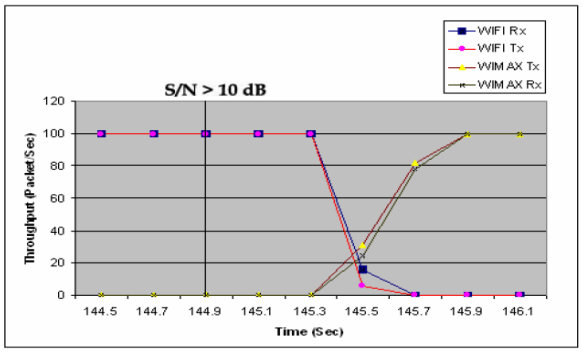


Fig. 5. Throughput on all interfaces of MN (WiFi to WiMax)

Table 2 shows the handoff characteristics measurements for WiFi to WiMax. From the results we can see that total handoff delay is high compared to previous case. This is because of the bigger delay in WIMAX network. The packet loss which is not critical in this case because delay of the WIFI network is very low .Therefore only very small number of packets that traverse WIFI network, and hence the packet loss is only 7%.

Parameter	Value
$D_{new\_session,}$	304ms
$D_{first\_RTP\_packet}$	78ms
$D_{handoff\_time}$	382ms
Packet Loss	7%

Table 2. Handoff measurements (WiFi to WiMax)

VI. Conclusion

In this paper we have presented a novel scheme MOD-SIP to support network service provider environment by modifying the existing SIP protocol. Our solution also reduces the load on the CH to perform handoff because handling handoff by the CH in real time environment is highly critical. And also when the connection between the MN and the CH is lost for a moment i.e. the stale address situation, is avoided by registering each and every movement of the MN with the SIP server. The handoff latency and packet loss of a Mobile Node in a WiMax/WiFi heterogeneous networks is studied under different cases. Based on the simulation it is observed that this method enhances our proposed aims but the handoff latency and packet loss in SIP is high to provide seamless handoff. We are further working on it to reduce the packet loss and handoff latency and achieve seamless handoff. This novel scheme MOD-SIP can be extended as such to other heterogeneous wireless networks.

VII. Acknowledgment

Here I would like to thank my supervisor Dr.V.Sumathy. As my research supervisor she helped me, guided me, gave valuable suggestions in setting up the research work in an efficient manner. With her comments and suggestions, I was able to proceed and execute my research work successfully.

VIII. References

1) C. Perkins, IP mobility support for IPv4 RFC-3344, IETF, Aug . 2002.
2) J. Rosenberg et al., SIP : session initiation protocol. RFC-3261 IETF,Jun. 2002.
3) Stewart R., et al., " Stream Control Transmission protocol " IETF RFC 2960 October2000
4) Henning Schulzrinne , Elin Wedlund , " Application - LayerMobility using SIP ", ACM Mobile Computing and communications Review, Volume 4, Number 3, July 2000.
5) E. Wedlund and H. Schulzrinne , Mobility support using SIP, " 2nd ACM / IEEE International Conference on Wireless and Mobile Multimedia, Aug. 1999, pp. 76-82.
6) SIP – based vertical handoff between WWANs and WLANs" Wei Wu Banerjee , N. Basu, K. Das, S.K. ALCATEL , USA, IEEE Wireless Communications June 2005 Volume: 12, Issue : 3 On page(s): 66- 72
7) SIP – Based Handoff in 4G Mobile Networks" Yen Wen Lin Ta - HeHuang Dept. of Comput. & Inofrmation Sci., National Taichung Univ .; IEEE Wireless Communications and Networking Conference,. WCNC 2007. March 2007 On page(s): 2806-2811.
8) Signaling Analysis of SIP - based Terminal mobility Protocol Between WLAN and WMAN "J.- P. Chen, W.S. Chen, J .Y. Chen, H.- T . Chu, and L.Hsieh Communication Systems and network - 2007
9) R. Rajavelsamy, S. Anand, Osok Song, Sungho Choi, "A novel scheme for mobility management in heterogeneous wireles networks, " Wireless Personal Communications, Vol. 43, No 3, 2007, pp. 997-1018.
10) S. Salsano, A. Polidoro,C. Mingardi, S. Niccolini, L. Veltri , SIP – based Mobility Management in Next Generation Networks, IEEE Wireless Communications,April 2008 Seok Joo Koh and Wook Hyun, " mSIP: Extension of SIP for Soft
11) Handover with Bicasting," IEEE Communications Letters, Vol. 12, No. 7,pp. 532-534, July 2008.
12) Tarek Bchini et al, " Performance of MSCTP Protocol in Vertical Handover Case Between IEEE 802.16e and IEEE 802.lle Networks" Global Information Infrastructure Symposium, 2009. GIIS '09.pg 1-4
13) Prince Edward.E , Sumathy. V , "A survey of seameless vertical handoff schemes for WiFi/WiMax heterogeneous networks" going to appear in IEEE International Conference on Signal Processing & Communications,July 18-21 ,2010,SPCOM 2010.
14) WiMAX Forum, http://www.wimaxforum.org.
15) Wi-FiIEEE802.11, http://en.wikipedia.org/wiki/802_11
16) MjSip open source Java SIP stack, http://www.mjsip.org.
17) http://www.wimax.com/commentary/news/wimax_industry_news/2010/march-2010

Global Journals Guidelines Handbook 2010

www.GlobalJournals.org

FELLOW OF INTERNATIONAL CONGRESS OF COMPUTER SCIENCE AND TECHNOLOGY (FICCT)

- FICCT' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FICCT" can be added to name in the following manner e.g. **Dr. Andrew Knoll, Ph.D., FICCT, Er. Pettor Jone, M.E., FICCT**
- FICCT can submit two papers every year for publication without any charges. The paper will be sent to two peer reviewers. The paper will be published after the acceptance of peer reviewers and Editorial Board.
- Free unlimited Web-space will be allotted to 'FICCT 'along with subDomain to contribute and partake in our activities.
- A professional email address will be allotted free with unlimited email space.
- FICCT will be authorized to receive e-Journals - GJCST for the Lifetime.
- FICCT will be exempted from the registration fees of Seminar/Symposium/Conference/Workshop conducted internationally of GJCST (FREE of Charge).
- FICCT will be an Honorable Guest of any gathering hold.

ASSOCIATE OF INTERNATIONAL CONGRESS OF COMPUTER SCIENCE AND TECHNOLOGY (AICCT)

- AICCT title will be awarded to the person/institution after approval of Editor-in-Chef and Editorial Board. The title 'AICCTcan be added to name in the following manner:
  eg. **Dr. Thomas Herry, Ph.D., AICCT**
- AICCT can submit one paper every year for publication without any charges. The paper will be sent to two peer reviewers. The paper will be published after the acceptance of peer reviewers and Editorial Board.
- Free 2GB Web-space will be allotted to 'FICCT' along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted with free 1GB email space.
- AICCT will be authorized to receive e-Journal GJCST for lifetime.
- A professional email address will be allotted with free 1GB email space.
- AICHSS will be authorized to receive e-Journal GJHSS for lifetime.

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.

Online Submission: There are three ways to submit your paper:

(A) (I) Register yourself using top right corner of Home page then Login from same place twice. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal from "Research Journals" Menu.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer (Although Mozilla Firefox is preferred), then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org as an attachment.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Times New Roman.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be two lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.

Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global Journals are being

abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals and Editorial Board, will become the copyright of the Global Journals.

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our

Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments. Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads: Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also. Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.
The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.
It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals, ought to include:
Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.
Abstract, used in Original Papers and Reviews:
Optimizing Abstract for Search Engines
Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words
A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.
One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: *Please make these as concise as possible.*

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals.

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals (Publication Prior to Print)

The Global Journals are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

Informal Tips for writing a Computer Science Research Paper to increase readability and citation

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

Techniques for writing a good quality Computer Science Research Paper:

1. Choosing the topic- In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by

asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should

NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research

- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.
- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.

You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.
Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals:

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals.

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

N

O

P

R

S

T

U

V

W

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350