Online ISSN: 0975-4172
Print ISSN: 0975-4350

Global Journal of Computer Science and Technology

DISCOVERING THOUGHTS AND INVENTING FUTURE

Technology
9
Reforming
Ideas

November 2011

Pinnacles

Inference Analysis Approach

Array Block Rotation Cipher

Ubiquitous Computing

convection boundary layer

The Volume 11
Issue 19
Version 1.0

© Global Journal of Computer Science and Technology, USA

ENG

Global Journal of Computer Science and Technology

Global Journal of Computer Science and Technology

Volume 11 Issue 19 (Ver. 1.0)

Open Association of Research Society

© Global Journal of Computer Science and Technology.2011.

All rights reserved.

This is a special issue published in version 1.0 of "Global Journal of Computer Science and Technology "By Global Journals Inc.

All articles are open access articles distributedunder "Global Journal of Computer Science and Technology"

Reading License, which permits restricted use. Entire contents are copyright by of "Global Journal of Computer Science and Technology" unless otherwise noted on specific articles.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission.

The opinions and statements made in this book are those of the authors concerned. Ultraculture has not verified and neither confirms nor denies any of the foregoing and no warranty or fitness is implied.

Engage with the contents herein at your own risk.

The use of this journal, and the terms and conditions for our providing information, is governed by our Disclaimer, Terms and Conditions and Privacy Policy given on our website http://globaljournals.us/terms-and-condition/menu-id-1463/.

By referring / using / reading / any type of association / referencing this journal, this signifies and you acknowledge that you have read them and that you accept and will be bound by the terms thereof.

All information, journals, this journal, activities undertaken, materials, services and our website, terms and conditions, privacy policy, and this journal is subject to change anytime without any prior notice.

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

(A Delaware USA Incorporation with "Good Standing"; Reg. Number: 0423089)

Sponsors:Global Association of Research

Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office,
Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141
United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU
United Kingdom.

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) & 250 USD (Color)

Editorial Board Members (HON.)

John A. Hamilton,"Drew" Jr.,
Ph.D., Professor, Management
Computer Science and Software Engineering
Director, Information Assurance Laboratory
Auburn University

Dr. Henry Hexmoor
IEEE senior member since 2004
Ph.D. Computer Science, University at Buffalo
Department of Computer Science
Southern Illinois University at Carbondale

Dr. Osman Balci, Professor
Department of Computer Science
Virginia Tech, Virginia University
Ph.D.and M.S.Syracuse University, Syracuse, New York
M.S. and B.S. Bogazici University, Istanbul, Turkey

Yogita Bajpai
M.Sc. (Computer Science), FICCT
U.S.A.Email:
yogita@computerresearch.org

Dr. T. David A. Forbes
Associate Professor and Range Nutritionist
Ph.D. Edinburgh University - Animal Nutrition
M.S. Aberdeen University - Animal Nutrition
B.A. University of Dublin- Zoology

Dr. Wenying Feng
Professor, Department of Computing & Information Systems
Department of Mathematics
Trent University, Peterborough,
ON Canada K9J 7B8

Dr. Thomas Wischgoll
Computer Science and Engineering,
Wright State University, Dayton, Ohio
B.S., M.S., Ph.D.
(University of Kaiserslautern)

Dr. Abdurrahman Arslanyilmaz
Computer Science & Information Systems Department
Youngstown State University
Ph.D., Texas A&M University
University of Missouri, Columbia
Gazi University, Turkey

Dr. Xiaohong He
Professor of International Business
University of Quinnipiac
BS, Jilin Institute of Technology; MA, MS, PhD,. (University of Texas-Dallas)

Burcin Becerik-Gerber
University of Southern California
Ph.D. in Civil Engineering
DDes from Harvard University
M.S. from University of California, Berkeley & Istanbul University

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor 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 SchoolPh.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 NeuroscienceNorthwestern University
Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-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, TaiwanUniversity 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

President Editor (HON.)

Dr. George Perry, (Neuroscientist)
Dean and Professor, College of Sciences
Denham Harman Research Award (American Aging Association)
ISI Highly Cited Researcher, Iberoamerican Molecular Biology Organization
AAAS Fellow, Correspondent Member of Spanish Royal Academy of Sciences
University of Texas at San Antonio
Postdoctoral Fellow (Department of Cell Biology)
Baylor College of Medicine
Houston, Texas, United States

Chief Author (HON.)

Dr. R.K. Dixit
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

Sangita Dixit
M.Sc., FICCT
Dean & Chancellor (Asia Pacific)
deanind@computerresearch.org

Luis Galárraga
J!Research Project Leader
Saarbrücken, Germany

Er. Suyog Dixit
(M. Tech), BE (HONS. in CSE), FICCT
SAP Certified Consultant
CEO at IOSRD, GAOR & OSS
Technical Dean, Global Journals Inc. (US)
Website: www.suyogdixit.com
Email:suyog@suyogdixit.com

Pritesh Rajvaidya
(MS) Computer Science Department
California State University
BE (Computer Science), FICCT
Technical Dean, USA
Email: pritesh@computerresearch.org

Contents of the Volume

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mining Closed Itemsets for Coherent Rules: An Inference Analysis Approach

By Kalli Srinivasa Nageswara Prasad, Prof. S. Ramakrishna
Sri Venkateswara University

Abstract - Past observations have shown that a frequent item set mining algorithm are alleged to mine the closed ones because the finish offers a compact and a whole progress set and higher potency. Anyhow, the most recent closed item set mining algorithms works with candidate maintenance combined with check paradigm that is dear in runtime likewise as area usage when support threshold is a smaller amount or the item sets gets long. Here, we show, PEPP with inference analysis that could be a capable approach used for mining closed sequences for coherent rules while not candidate. It implements a unique sequence closure checking format with inference analysis that based mostly on Sequence Graph protruding by an approach labeled "Parallel Edge projection and pruning" in brief will refer as PEPP. We describe a novel inference analysis approach to prune patterns that tends to derive coherent rules. A whole observation having sparse and dense real-life information sets proved that PEPP with inference analysis performs larger compared to older algorithms because it takes low memory and is quicker than any algorithms those cited in literature frequently.

Keywords : *Data mining, Association Rule Mining, Closed itemset, Frequent Itemset,KDD,PEPP.*

GJCST Classification : *H.2.8*

Strictly as per the compliance and regulations of:

© 2011l . Kalli Srinivasa Nageswara Prasad, Prof. S. Ramakrishna. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Mining Closed Itemsets for Coherent Rules: An Inference Analysis Approach

Kalli Srinivasa Nageswara Prasad [α], Prof. S. Ramakrishna [Ω]

Abstract - Past observations have shown that a frequent item set mining algorithm are alleged to mine the closed ones because the finish offers a compact and a whole progress set and higher potency. Anyhow, the most recent closed item set mining algorithms works with candidate maintenance combined with check paradigm that is dear in runtime likewise as area usage when support threshold is a smaller amount or the item sets gets long. Here, we show, **PEPP** with inference analysis that could be a capable approach used for mining closed sequences for coherent rules while not candidate. It implements a unique sequence closure checking format with inference analysis that based mostly on Sequence Graph protruding by an approach labeled "Parallel Edge projection and pruning" in brief will refer as **PEPP**. We describe a novel inference analysis approach to prune patterns that tends to derive coherent rules. A whole observation having sparse and dense real-life information sets proved that **PEPP** with inference analysis performs larger compared to older algorithms because it takes low memory and is quicker than any algorithms those cited in literature frequently.

Keywords : Data mining, Association Rule Mining, Closed itemset, Frequent Itemset, KDD,PEPP.

I. Introduction

Association rule mining, introduced in [28], is considered as one of the most important tasks in Knowledge Discovery in Databases [29]. Among sets of items in transaction databases, it aims at discovering implicative tendencies that can be valuable information for the decision-maker. An association rule is defined as the implication $X \rightarrow Y$, described by two interestingness measures support and confidence, where X and Y are the sets of items and $X \bigcap Y = \phi$. Apriori [28] is the first algorithm proposed in the association rule mining field and many other algorithms were derived from it. It is very well known that mining algorithms can discover a prohibitive amount of association rules; Starting from a database, it proposes to extract all association rules satisfying minimum thresholds of support and confidence. For instance, thousands of rules are extracted from a database of several dozens of attributes and several hundreds of transactions. Furthermore, as suggested by Silbershatz and Tuzilin [30], valuable information is often represented by those rare low support and unexpected association rules which are surprising to the user. So, the more we increase the support threshold, the more efficient the algorithms are and the more the discovered rules are obvious, and hence, the less they are interesting for the user. As a result, it is necessary to bring the support threshold low enough in order to extract valuable information. Unfortunately, the lower the support is, the larger the volume of rules becomes, making it intractable for a decision-maker to analyze the mining result. Experiments show that rules become almost impossible to use when the number of rules overpasses 100. Thus, it is crucial to help the decision-maker with an efficient technique for reducing the number of rules.

To overcome this drawback, several methods were proposed in the literature. On the one hand, different algorithms were introduced to reduce the number of itemsets by generating closed [31], maximal [32] or optimal itemsets [33], and several algorithms to reduce the number of rules, using non redundant rules [34], [35], or pruning techniques [36]. On the other hand, post processing methods can improve the selection of discovered rules. Different complementary post processing methods may be used, like pruning, summarizing, grouping, or visualization [37]. Pruning consists in removing uninteresting or redundant rules. In summarizing, concise sets of rules are generated. Groups of rules are produced in the grouping process, and the visualization improves the readability of a large number of rules by using adapted graphical representations.

However, most of the existing post processing methods are generally based on statistical information in the database. Since rule interestingness strongly depends on user knowledge and goals, these methods do not guarantee that interesting rules will be extracted. In this paper, we propose a novel framework to identify closed itemsets. Associations are discovered based on inference analysis. The principle of the approach considers that an association rule should only be reported when there is enough interest gain claimed during inference analysis in the data. To do this, we consider both presence and absence of items during the mining. An association such as

$beer \rightarrow nappies$ will only be reported if we can also find that there are fewer occurrences of $\neg beer \rightarrow nappies$ and $beer \rightarrow \neg nappies$ but more of $\neg beer \rightarrow \neg$

Author [α] : Research Scholar in Computer Science Sri Venkateswara University, Tirupati Andhra Pradesh, India, Mobile: 9490171769 Email : kallisnprasad@gmail.com
Author [Ω] : Department of Computer Science Sri Venkateswara University, Tirupati Andhra Pradesh, India, Mobile : 944149572 Email : profsramakrishnasvu@gmail.com

© 2011 Global Journals Inc. (US)

nappies. This approach will ensure that when a rule such as
beer → nappies is reported, it indeed has the strongest interest in the data as comparison was made on both presence and absence of items during the mining process.

II. Related Work

The sequential item set mining problem was initiated by Agrawal and Srikant, and the same was developed as a filtered algorithm, GSP [2], basing on the Apriori property [19]. Since then, lots of sequential item set mining algorithms are being developed for efficiency. Some are, SPADE [4], Prefixspan [5], and SPAM [6]. SPADE is on principle of vertical id-list format and it uses a lattice-theoretic method to decompose the search space into many tiny spaces, on the other hand Prefixspan implements a horizontal format dataset representation and mines the sequential item sets with the pattern-growth paradigm: grow a prefix item set to attain longer sequential item sets on building and scanning its database. The SPADE and the Prefixspan highly perform GSP. SPAM is a recent algorithm used for mining lengthy sequential item sets and implements a vertical bitmap representation. Its observations reveal, SPAM is better efficient in mining long item sets compared to SPADE and Prefixspan but, it still takes more space than SPADE and Prefixspan. Since the frequent closed item set mining [15], many capable frequent closed item set mining algorithms are introduced, like A-Close [15], CLOSET [20], CHARM [16], and CLOSET+ [18]. Many such algorithms are to maintain the ready mined frequent closed item sets to attain item set closure checking. To decrease the memory usage and search space for item set closure checking, two algorithms, TFP [21] and CLOSET+2, implement a compact 2-level hash indexed result-tree structure to keep the readily mined frequent closed item set candidates. Some pruning methods and item set closure verifying methods, initiated that can be extended for optimizing the mining of closed sequential item sets also. CloSpan is a new algorithm used for mining frequent closed sequences [17]. It goes by the *candidate maintenance-and-test* method: initially create a set of closed sequence candidates stored in a hash indexed result-tree structure and do post-pruning on it. It requires some pruning techniques such as *Common Prefix* and *Backward Sub-Item set pruning* to prune the search space as CloSpan requires maintaining the set of closed sequence candidates, it consumes much memory leading to heavy search space for item set closure checking when there are more frequent closed sequences. Because of which, it does not scale well the number of frequent closed sequences. BIDE [26] is another closed pattern mining algorithm and ranked high in performance when compared to other algorithms discussed. BIDE projects the sequences after projection it prunes the patterns that are subsets of current patterns if and only if subset and superset contains same support required. But this model is opting to projection and pruning in sequential manner. This sequential approach sometimes turns to expensive when sequence length is considerably high. In our earlier literature [27] we discussed some other interesting works published in recent literature.

III. Dataset Adoption and Formulation

Item Sets 'I': A set of diverse elements by which the sequences generate.

$$I = \bigcup_{k=1}^{n} i_k$$ Note: 'I' is set of diverse elements.

Sequence set 'S': A set of sequences, where each sequence contains elements each element 'e' belongs to 'I' and true for a function p(e). Sequence set can formulate as

$$s = \bigcup_{i=1}^{m} < e_i \mid (p(e_i), e_i \in I) >$$

Represents a sequence 's' of items those belongs to set of distinct items 'I', 'm' is total ordered items and $P(e_i)$ is a transaction, where e_i usage is true for that transaction.

$$S = \bigcup_{j=1}^{t} s_j$$

S: represents set of sequences, 't' represents total number of sequences and its value is volatile and s_j: is a sequence that belongs to S.

Subsequence: is a sequence s_p of sequence set 'S' is considered as subsequence of another sequence s_q of Sequence Set 'S' if all items in sequence S_p is belongs to s_q as an ordered list. This can be formulated as

If $$(\bigcup_{i=1}^{n} s_{pi} \in s_q) \Rightarrow (s_p \subseteq s_q)$$

Then $$\bigcup_{i=1}^{n} s_{pi} <: \bigcup_{j=1}^{m} s_{qj}$$ where $s_p \in S \text{ and } s_q \in S$

Total Support 'ts' : occurrence count of a sequence as an ordered list in all sequences in sequence set 'S' can adopt as total support 'ts' of that sequence. Total support 'ts' of a sequence can determine by fallowing formulation.

$$f_{ts}(s_t) = \mid s_t <: s_p \ (\text{for each } p = 1..\mid DB_S \mid) \mid$$

DB_S is set of sequences.

© 2011 Global Journals Inc. (US)

$f_{ts}(s_t)$: Represents the total support 'ts' of sequence s_t is the number of super sequences of s_t

Qualified support 'q_s': The resultant coefficient of total support divides by size of sequence database adopt as qualified support 'qs'. Qualified support can be found by using fallowing formulation.

$$f_{qs}(s_t) = \frac{f_{ts}(s_t)}{|DB_S|}$$

Sub-sequence and Super-sequence: A sequence is sub sequence for its next projected sequence if both sequences having same total support.

Super-sequence: A sequence is a super sequence for a sequence from which that projected, if both having same total support. Sub-sequence and super-sequence can be formulated as

If $f_{ts}(s_t) \geq rs$ where 'rs' is required support threshold given by user And $s_t <: s_p$ *for any p value* where $f_{ts}(s_t) \cong f_{ts}(s_p)$

IV. Closed Itemset Discovery

a) PEPP: Parallel Edge Projection and Pruning Based Sequence Graph protrude [28]

i. *Preprocess:*

As a first stage of the proposal we perform dataset preprocessing and itemsets Database initialization. We find itemsets with single element, in parallel prunes itemsets with single element those contains total support less than required support.

ii. *Forward Edge Projection:*

In this phase, we select all itemsets from given itemset database as input in parallel. Then we start projecting edges from each selected itemset to all possible elements. The first iteration includes the pruning process in parallel, from second iteration onwards this pruning is not required, which we claimed as an efficient process compared to other similar techniques like BIDE. In first iteration, we project an itemset s_p that spawned from selected itemset s_i from DB_S and an element e_i considered from 'I'. If the $f_{ts}(s_p)$ is greater or equal to rs, then an edge will be defined between s_i and e_i. If $f_{ts}(s_i) \cong f_{ts}(s_p)$ then we prune s_i from DB_S. This pruning process required and limited to first iteration only.

From second iteration onwards project the itemset S_p that spawned from S_p, to each element e_i of 'I'. An edge can be defined between S_p, and e_i if $f_{ts}(s_p)$ is greater or equal to rs. In this description S_p, is a projected itemset in previous iteration and eligible as a sequence. Then apply the following validation to find closed sequence.

iii. *Edge pruning:*

If any of $f_{ts}(s_{p'}) \cong f_{ts}(s_p)$ that edge will be pruned and all disjoint graphs except s_p will be considered as closed sequence and moves it into DB_S and remove all disjoint graphs from memory.

The above process continues till the elements available in memory those are connected through direct or transitive edges and projecting itemsets i.e., till graph become empty.

b) Inference Analysis:

Inferences:-

a. Pattern positive score is sum of no of transactions in which all items in the pattern exist, no. of transactions in which all items in the pattern does not exist.
b. Pattern negative score is no of transactions in which only few items of the pattern exist.
c. Pattern actual coverage is pattern positive score-pattern negative score.
d. Interest gain is Actual coverage of the pattern involved in association rule.
e. Coherent rule Actual coverage of the rule's left side pattern must be greater than or equal to actual coverage of the right side pattern.
f. Inference Support ia_s refers actual coverage of the pattern.
g. $f_{ia}(s_t)$ Represents the inference support of the sequence s_t.

V. Approach

For each pattern s_p of the pattern dataset, If $f_{ia}(s_t) < ia_s$ then we prune that pattern

a) PEPP[1] Algorithm:

This section describes algorithms for initializing sequence database with single elements sequences, spawning itemset projections and pruning edges from Sequence Graph SG.

Input: DB_S and 'I';
L1: For each sequence s_i in DB_S
Begin:
L2: For each element e_i of 'I'
Begin:
C1: if $\text{edgeWeight}(s_i, e_i) \geq rs$
Begin:
Create projected itemset s_p from (s_i, e_i)
If $f_{ts}(s_i) \cong f_{ts}(s_p)$ then prune s_i from DB_S
End: C1.
End: L2.
End: L1.

© 2011 Global Journals Inc. (US)

L3: For each projected Itemset s_p in memory
Begin:
$s_{p'} = s_p$
L4: For each e_i of 'I'
Begin:
Project s_p from $(s_{p'}, e_i)$
C2: If $f_{ts}(s_p) \geq rs$
Begin
Spawn SG by adding edge between $s_{p'}$ *and* e_i
End: C2
End: L4
C3: If $s_{p'}$ not spawned and no new projections added for $s_{p'}$
Begin:

Remove all duplicate edges for each edge weight from $s_{p'}$ and keep edges unique by not deleting most recent edges for each edge weight. Select elements from each disjoint graph as closed sequence and add it to DB_S and remove disjoint graphs from SG.

End C3
End: L3
If $SG \neq \phi$ go to L3.

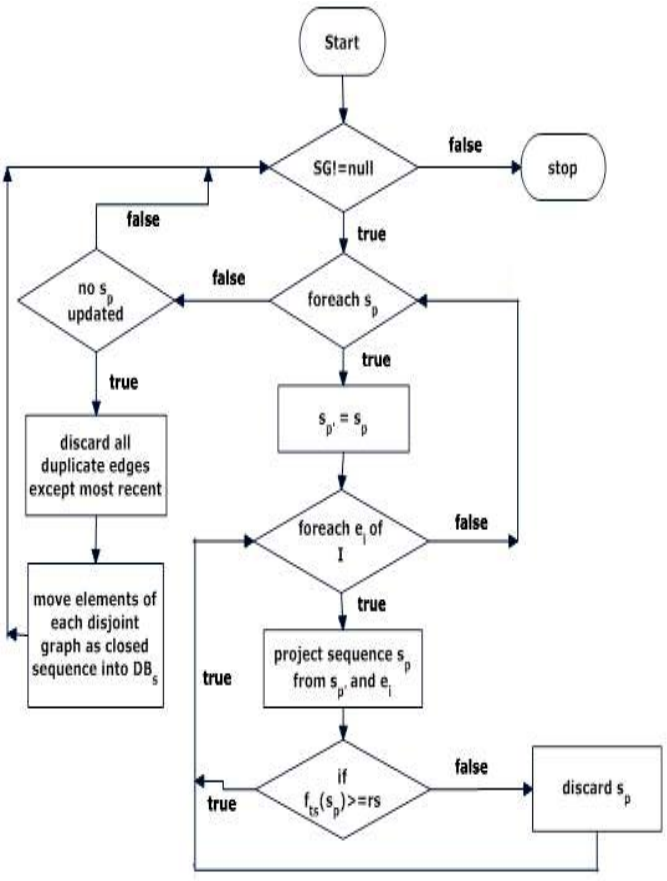


Fig. 1 : flowchart for PEPP Algorithm

b) Description of Inference Analysis

Set I = {i1, i2… im} be the universe of items composed of m different attributes, ik(k=1,2,..,m) is item. Transaction database D is a collection of transaction T, A transaction t = (tid, X) is a tuple where tid is a unique transaction ID and X is an itemset. The count of an itemset X in D, denoted by count(X), is the number of transactions in D containing X. The support of an itemset X in D, denoted by supp(X), is the proportion of transactions in D that contain X. The negative rule X⇒¬Y holds in the transaction set D with confidence conf (X⇒¬Y) = supp $(X \cup \neg Y)$ /supp (X).

In Transaction database, each transaction is a collection of items involved sequences. The issue of mining association rules is to get all association rules that its support and confidence is respectively greater than the minimum threshold given by the user. The issues of mining association rules can be divide into two sub-issues as follows:

Find frequent itemsets, Generate all itemsets that support is greater than the minimum support. Generate association rules from frequent itemsets. In logical analysis, the direct calculation of support is not convenient, To calculate the support and confidence of negative associations using the support and confidence of positive association that is known: set A, B⊂I , A∩B=Φ ,then:

$$\sup(\neg A) = 1 - \sup(A);$$
$$\sup(A \cup \neg B) = \sup(A) - Sup(A \cup B);$$
$$\sup(\neg A \cup B) = \sup(B) - \sup(A \cup B)$$
$$\sup(\neg A \cup \neg B) = 1 - \sup(A) - \sup(B) + \sup(A \cup B);$$

Based on the above formulas we perform the logical analysis to derive the actual support of the patterns that improves the rule coherency. Inference analysis by example: Let A,B∈I where I is itemset generated with the association of A,B are individual items or subsets.

Under logical analysis we determine $f_{ts}(\neg A \cup \neg B)$, $f_{ts}(A \cup \neg B)$ and $f_{ts}(\neg A \cup B)$. The support $f_{ts}(I)$, $f_{ts}(\neg A \cup \neg B)$ we consider as positive support and $f_{ts}(A \cup \neg B)$, $f_{ts}(\neg A \cup B)$ we consider as negative support. Finally we determine $f_{ia}(I) = f_{ts}(I) + f_{ts}(\neg A \cup \neg B) - f_{ts}(A \cup \neg B) - f_{ts}(\neg A \cup B)$;

© 2011 Global Journals Inc. (US)

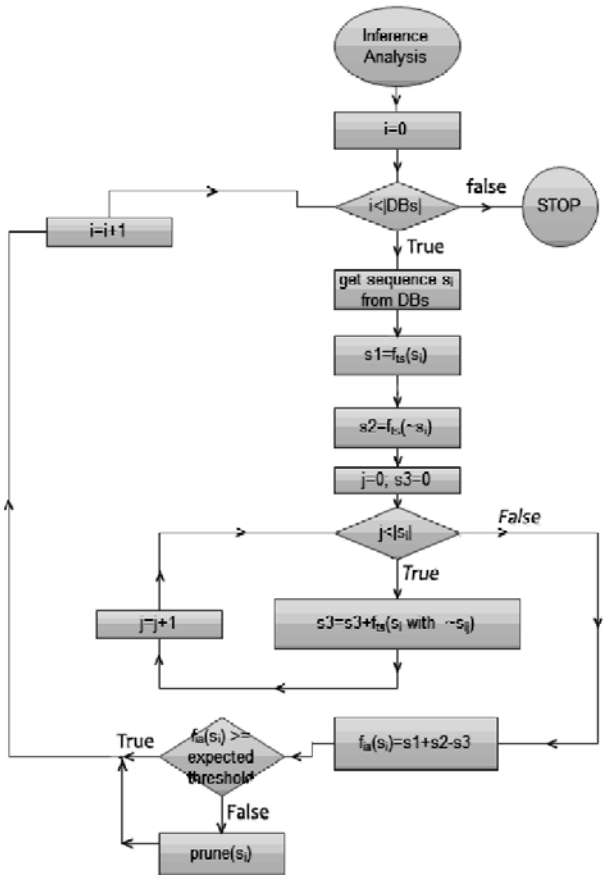


Fig.2 : flowchart for Inference Analysis.

VI. COMPARATIVE STUDY

This segment focuses mainly on providing evidence on asserting the claimed assumptions that 1) The PEPP is similar to BIDE which is actually a sealed series mining algorithm that is competent enough to momentously surpass results when evaluated against other algorithms such as CloSpan and SPADE. 2) Utilization of memory and momentum is rapid when compared to the CloSpan algorithm which is again analogous to BIDE. 3) There is the involvement of an enhanced occurrence and a probability reduction in the memory exploitation rate with the aid of the trait equivalent prognosis and also rim snipping of the PEPP with inference analysis for no coherent pattern pruning. This is on the basis of the surveillance done which concludes that PEPP's implementation is far more noteworthy and important in contrast with the likes of BIDE, to be precise.

JAVA 1.6_ 20th build was employed for accomplishment of the PEPP and BIDE algorithms. A workstation equipped with core2duo processor, 2GB RAM and Windows XP installation was made use of for investigation of the algorithms. The parallel replica was deployed to attain the thread concept in JAVA.

VII. DATASET CHARACTERISTICS

Pi is supposedly found to be a very opaque dataset, which assists in excavating enormous quantity of recurring clogged series with a profitably high threshold somewhere close to 90%. It also has a distinct element of being enclosed with 190 protein series and 21 divergent objects. Reviewing of serviceable legacy's consistency has been made use of by this dataset. Fig. 5 portrays an image depicting dataset series extent status.

In assessment with all the other regularly quoted forms like SPADE, prefixspan and CloSpan, BIDE has made its mark as a most preferable, superior and sealed example of mining copy, taking in view the detailed study of the factors mainly, memory consumption and runtime, judging with PEPP.

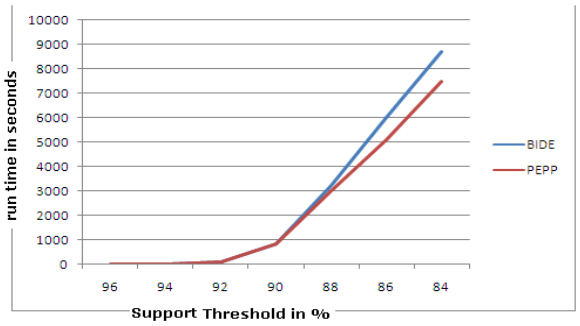


Fig.3 : A comparison report for Runtime.

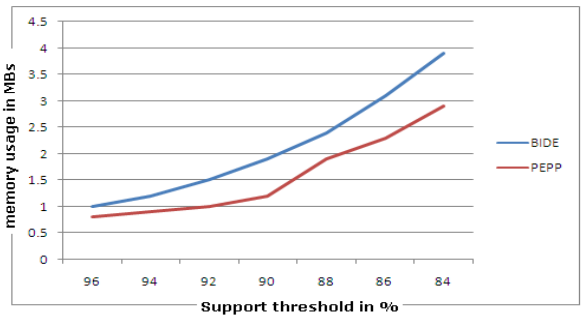


Fig.4 : A comparison report for memory usage.

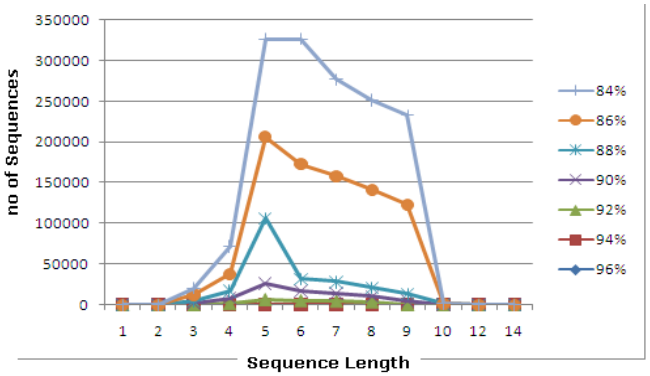


Fig.5 : Sequence length and number of sequences at different thresholds in Pi dataset.

© 2011 Global Journals Inc. (US)

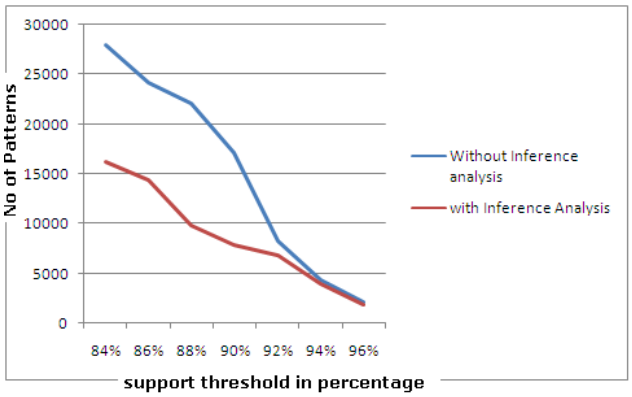


Fig.6 : No patterns detected by PEPP with and without inference analysis.

In contrast to PEPP and BIDE, a very intense dataset Pi is used which has petite recurrent closed series whose end to end distance is less than 10, even in the instance of high support amounting to around 90%. The diagrammatic representation displayed in Fig 3 explains that the above mentioned two algorithms execute in a similar fashion in case of support being 90% and above. But in situations when the support case is 88% and less, then the act of PEPP surpasses BIDE's routine. The disparity in memory exploitation of PEPP and BIDE can be clearly observed because of the consumption level of PEPP being lower than that of BIDE. The concept inference analysis we introduced here played a vital role in closed itemset detection. The significant improvement in closed itemset detection can be observable in our results, see the fig 6.

VIII. Conclusion

It has been scientifically and experimentally proved that clogged prototype mining propels dense product set and considerably enhanced competency as compared to recurrent prototype of mining even though both these types project similar animated power. The detailed study has verified that the case usually holds true when the count of recurrent moulds is considerably large and is the same with the recurrent bordered models as well. However, there is the downbeat in which the earlier formed clogged mining algorithms depend on chronological set of recurrent mining outlines. It is used to verify whether an innovative recurrent outline is blocked or else if it can nullify few previously mined blocked patterns. This leads to a situation where the memory utilization is considerably high but also leads to inadequacy of increasing seek out space for outline closure inspection. This paper anticipates an unusual algorithm for withdrawing recurring closed series with the help of Sequence Graph. It performs the following functions: It shuns the blight of contender's maintenance and test exemplar, supervises memory space expertly and ensures recurrent closure of clogging in a well-organized manner and at the same instant guzzling less amount of memory plot in comparison with the earlier developed mining algorithms. There is no necessity of preserving the already defined set of blocked recurrences, hence it very well balances the range of the count of frequent clogged models. A Sequence graph is embraced by PEPP and has the capability of harvesting the recurrent clogged pattern in an online approach. The efficacy of dataset drafts can be showcased by a wide-spread range of experimentation on a number of authentic datasets amassing varied allocation attributes. PEPP is rich in terms of velocity and memory spacing in comparison with the BIDE and CloSpan algorithms. ON the basis of the amount of progressions, linear scalability is provided. It is also proven that PEPP is efficient to find closed itemsets under inference analysis. It has been proven and verified by many scientific research studies that limitations are crucial for a number of chronological outlined mining algorithms. In addition we improved closed itemset detection performance by introducing inference analysis as an extension to PEPP. Future studies include proposing of post processing and pruning of the rules based on categorical relations between attributes.

References Références Referencias

1. F. Masseglia, F. Cathala, and P. Poncelet, The psp approach for mining sequential patterns. In PKDD'98, Nantes, France, Sept. 1995.
2. R. Srikant, and R. Agrawal, Mining sequential patterns: Generalizations and performance improvements. In EDBT'96, Avignon, France, Mar. 1996.
3. J. Han, J. Pei, B. Mortazavi-Asl, Q. Chen, U. Dayal, and M.C. Hsu, FreeSpan: Frequent pattern-projected sequential pattern mining. In SIGKDD'00, Boston, MA, Aug. 2000.
4. M. Zaki, SPADE: An Efficient Algorithm for Mining Frequent Sequences. Machine Learning, 42:31-60, Kluwer Academic Publishers, 2001.
5. J. Pei, J. Han, B. Mortazavi-Asl, Q. Chen, U. Dayal, and M.C. Hsu, Prefixspan: Mining sequential patterns efficiently by prefix-projected pattern growth. In ICDE'01, Heidelberg, Germany, April 2001.
6. J. Ayres, J. Gehrke, T. Yiu, and J. Flannick, Sequential Pattern Mining using a Bitmap Representation. In SIGKDD'02, Edmonton, Canada, July 2002.
7. M. Garofalakis, R. Rastogi, and K. Shim, SPIRIT: Sequential Pattern Mining with regular expression constraints. In VLDB'99, San Francisco, CA, Sept. 1999.
8. J. Pei, J. Han, and W. Wang, Constraint-based sequential pattern mining in large databases. In CIKM'02, McLean, VA, Nov. 2002.

© 2011 Global Journals Inc. (US)

9. M. Seno, G. Karypis, SLPMiner: An algorithm for finding frequent sequential patterns using length decreasing support constraint. In ICDM'02, Maebashi, Japan, Dec. 2002.
10. H. Mannila, H. Toivonen, and A.I. Verkamo, Discovering frequent episodes in sequences. In SIGKDD'95, Montreal, Canada, Aug. 1995.
11. B. Ozden, S. Ramaswamy, and A. Silberschatz, Cyclic association rules. In ICDE'98, Olando, FL, Feb. 1998.
12. C. Bettini, X. Wang, and S. Jajodia, Mining temporal relationals with multiple granularities in time sequences. Data Engineering Bulletin, 21(1):32-38, 1998.
13. J. Han, G. Dong, and Y. Yin, Efficient mining of partial periodic patterns in time series database. In ICDE'99, Sydney, Australia, Mar. 1999.
14. J. Yang, P.S. Yu, W. Wang and J. Han, Mining long sequential patterns in a noisy environment. In SIGMOD' 02, Madison, WI, June 2002.
15. N. Pasquier, Y. Bastide, R. Taouil and L. Lakhal, Discovering frequent closed itemsets for association rules. In ICDT'99, Jerusalem, Israel, Jan. 1999.
16. M. Zaki, and C. Hsiao, CHARM: An efficient algorithm for closed itemset mining. In SDM'02, Arlington, VA, April 2002.
17. Yan, J. Han, and R. Afshar, CloSpan: Mining Closed Sequential Patterns in Large Databases. In SDM'03, San Francisco, CA, May 2003.
18. J. Wang, J. Han, and J. Pei, CLOSET+: Searching for the Best Strategies for Mining Frequent Closed Itemsets. In KDD'03, Washington, DC, Aug. 2003.
19. R. Agrawal and R. Srikant. Fast algorithms for mining association rules. In VLDB'94, Santiago, Chile, Sept. 1994.
20. J. Pei, J. Han, and R. Mao, CLOSET: An efficient algorithm for mining frequent closed itemsets. In DMKD'01 workshop, Dallas, TX, May 2001.
21. J. Han, J. Wang, Y. Lu, and P. Tzvetkov, Mining Top- K Frequent Closed Patterns without Minimum Support. In ICDM'02, Maebashi, Japan, Dec. 2002.
22. P. Aloy, E. Querol, F.X. Aviles and M.J.E. Sternberg, Automated Structure-based Prediction of Functional Sites in Proteins: Applications to Assessing the Validity of Inheriting Protein Function From Homology in Genome Annotation and to Protein Docking. Journal of Molecular Biology, 311, 2002.
23. R. Agrawal, and R. Srikant, Mining sequential patterns. In ICDE'95, Taipei, Taiwan, Mar. 1995.
24. Jonassen, J.F. Collins, and D.G. Higgins, Finding flexible patterns in unaligned protein sequences. Protein Science, 4(8), 1995.
25. R. Kohavi, C. Brodley, B. Frasca, L.Mason, and Z. Zheng, KDD-cup 2000 organizers' report: Peeling the Onion. SIGKDD Explorations, 2, 2000.
26. Jianyong Wang, Jiawei Han: BIDE: Efficient Mining of Frequent Closed Sequences. ICDE 2004: 79-90.
27. Kalli Srinivasa Nageswara Prasad and Prof. S Ramakrishna. Article: Frequent Pattern Mining and Current State of the Art. International Journal of Computer Applications 26(7):33-39, July 2011. Published by Foundation of Computer Science, New York.
28. R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," Proc. ACM SIGMOD, pp. 207-216, 1993.
29. U.M. Fayyad, G. Piatetsky-Shapiro, P. Smyth, and R. Uthurusamy, Advances in Knowledge Discovery and Data Mining. AAAI/MIT Press, 1996.
30. A. Silberschatz and A. Tuzhilin, "What Makes Patterns Interesting in Knowledge Discovery Systems," IEEE Trans. Knowledge and Data Eng. vol. 8, no. 6, pp. 970-974, Dec. 1996.
31. M.J. Zaki and M. Ogihara, "Theoretical Foundations of Association Rules," Proc. Workshop Research Issues in Data Mining and Knowledge Discovery (DMKD '98), pp. 1-8, June 1998.
32. D. Burdick, M. Calimlim, J. Flannick, J. Gehrke, and T. Yiu, "Mafia: A Maximal Frequent Itemset Algorithm," IEEE Trans. Knowledge and Data Eng., vol. 17, no. 11, pp. 1490-1504, Nov. 2005.
33. J. Li, "On Optimal Rule Discovery," IEEE Trans. Knowledge and Data Eng., vol. 18, no. 4, pp. 460-471, Apr. 2006.
34. M.J. Zaki, "Generating Non-Redundant Association Rules," Proc. Int'l Conf. Knowledge Discovery and Data Mining, pp. 34-43, 2000.
35. N. Pasquier, Y. Bastide, R. Taouil, and L. Lakhal, "Efficient Mining of Association Rules Using Closed Itemset Lattices," Information Systems, vol. 24, pp. 25-46, 1999.
36. H. Toivonen, M. Klemettinen, P. Ronkainen, K. Hatonen, and H. Mannila, "Pruning and Grouping of Discovered Association Rules," Proc. ECML-95 Workshop Statistics, Machine Learning, and Knowledge Discovery in Databases, pp. 47-52, 1995.
37. B. Baesens, S. Viaene, and J. Vanthienen, "Post-Processing of Association Rules," Proc. Workshop Post-Processing in Machine Learning and Data Mining: Interpretation, Visualization, Integration, and Related Topics with Sixth ACM SIGKDD, pp. 20-23, 2000.

© 2011 Global Journals Inc. (US)

This page is intentionally left blank

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

3D Array Block Rotation Cipher : An Improvement using shift

By Pushpa R. Suri, Sukhvinder Singh Deora
Kurukshetra University, Haryana, India

Abstract - This paper on Cipher based on 3D Array Block Rotation is in continuation with our earlier paper titled "A cipher based on 3D Array Block Rotation". It discusses a new rotation; lateral shift along with the earlier discussed rotation of the 3D Array block or circular shifting of plates of 3D Array in clockwise direction while enciphering and anticlockwise direction while deciphering. It also discusses the problem of relative bit positioning in the earlier specified algorithm and introduce shift rotations of the blocks as a possible solution to the problem. It uses a key of specified length which can be either transferred with the ciphertext or can be obtained by an agreed upon random bit generator. In all, it is a novel and effective cipher with good randomness property.

Keywords : *Encoding, Decoding, Block cipher, randomness, Random Number Generator, 3D Array, Confusion-Diffusion, Linear Feedback Shift Rotations (LFSR) , p-value.*

GJCST Classification : *E.3*

Strictly as per the compliance and regulations of:

© 2011l . Pushpa R. Suri, Sukhvinder Singh Deora. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

3D Array Block Rotation Cipher: An Improvement using lateral shift

Pushpa R. Suri [α], Sukhvinder Singh Deora[Ω]

Abstract - This paper on Cipher based on 3D Array Block Rotation is in continuation with our earlier paper titled "A cipher based on 3D Array Block Rotation". It discusses a new rotation; lateral shift along with the earlier discussed rotation of the 3D Array block or circular shifting of plates of 3D Array in clockwise direction while enciphering and anticlockwise direction while deciphering. It also discusses the problem of relative bit positioning in the earlier specified algorithm and introduce shift rotations of the blocks as a possible solution to the problem. It uses a key of specified length which can be either transferred with the ciphertext or can be obtained by an agreed upon random bit generator. In all, it is a novel and effective cipher with good randomness property.

Keywords : Encoding, Decoding, Block cipher, randomness, Random Number Generator, 3D Array, Confusion-Diffusion, Linear Feedback Shift Rotations (LFSR) , p-value.

I. Introduction

Communication involves conveying the information in one form or other to the intended receiver, using some medium. Internet, the fastest and most widely used medium of electronic information exchange, is also used for the same. However for the security of information, a technique of data encryption/ decryption is used in most of the cases.

II. Cipher

Cipher is a message written in a secret code. In a cryptographic system some specific units of plaintext, usually letters, are arbitrarily transposed or substituted according to a predetermined code (encoding technique) to convert it to a cipher text [1].

Fig.1 : Encoding

The ciphertext is then transferred over the non-secure medium of communication and received by the receiver. The receiver then applies the decoding technique in accordance to the encoding technique to get the actual plaintext communicated to him by the sender.

Fig. 2 : Decoding

The basic idea behind any cryptographic algorithm is same, using confusion and diffusion to change the actual information so that it is only the intended user who can decode and understand it. Some World War II ciphers using stuttered rotors are briefly described as natural predecessors [5]. There have been algorithms like the Hill Cipher and Vernam Cipher to the DES, AES and A5 algorithms in the literature [1]. The strength of these ciphers depends upon key length, processing and the use of operations like simple negation, shift, XOR and substitution [8].

III. 3D Array Block Cipher Problem

We have developed an algorithm which encrypts/decrypts the information in the paper titled "A cipher based on 3D Array Block Rotation". We have suggested the use of Plate-wise rotation along X/Y/Z axis, at random, for the diffusion of the bits/text contained in the 3D Array.

However, we have noticed that if such a rotation is performed then there is relative bit/char positioning (red dots), equidistant from the centre (magenta dot) in case of odd sized 3D array (see Fig. 3). This relative bit/char positioning can be exploited for decoding of ciphertext produced using 3D Array Rotations as suggested in previous paper. In our current paper, we discuss introduction of circular shift operation, which will remove this positional dependency problem in the 3D Array.

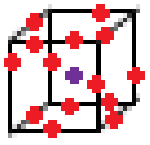


Fig.3 : Relative bit/char positioning around the centre of 3D Array

Author [α] : Associate Professor in the Department of Computer Science and Applications at Kurukshetra University, Haryana, India.
Author [Ω] : Assistant Professor in N.C. Institute of Computer Sciences, Israna, Panipat, India, is M.Sc. Mathematics, M.C.A., M.Phil. in Computer Science. Telephone: +919896310303
E-mail : sukhvinder.singh.deora@gmail.com

© 2011 Global Journals Inc. (US)

IV. Our Improved Algorithm

In this new version of our cipher based on 3D Array we are proposing the details of key length, number of rounds; which is some multiple of 8, the structure and its two kinds of rotations, the rotation policy as per the sub-keys, k-th iteration details and the overall encryption process shown through various figures and flowcharts.

a) The 3D Array Structure

We are proposing that the cipher can use a key of length, 8 X Number of Rounds, minimum of 256 bits which will be sufficient to encrypt 4096 data bits. The key may be produced by using some one time pad so that there is a different ciphertext of the same plaintext each time encoding is done. The key can also be generated at the receiver end using agreed upon Random Number Generator or communicated using some highly secure algorithm before transferring the actual data.

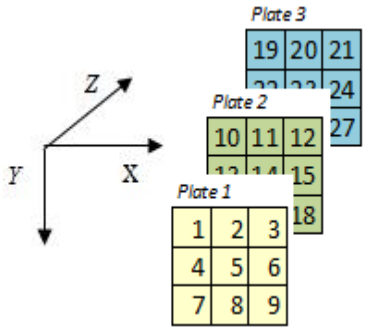


Fig. 4 : The Structure.

We can use a three dimensional array to store the initial plaintext. The plaintext may also be stored as row-major/column major fashion, as agreed between the sender and receiver. Considering the three axis as the axis of rotation, X, Y and Z, as shown in Fig. 4, and each layer as a rotatable plate. We can diffuse the text using clockwise rotation of 90/180/270° of particular plate at a particular axis or using linear shift rotation of the rows of the particular plate.

b) Axis-wise Plates of 3D Array

The Axis-wise plates of a 3X3X3 Array of integers is shown in Fig 5.

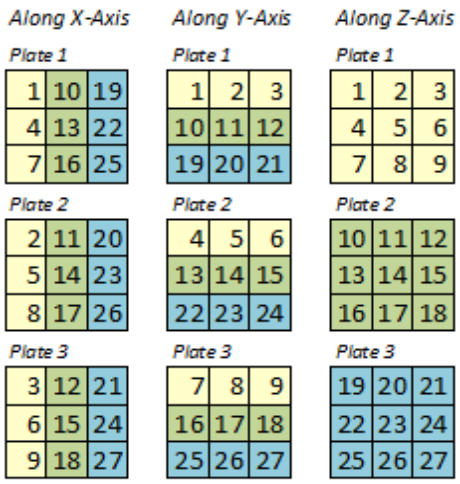


Fig. 5 : Axis-wise Plates view for a 3X3X3 Array

A three dimensional matrix may be used to store the initial plaintext. There will be three possible axis of rotation as shown in Fig. 4, and axis-wise layers, as shown in Fig. 5, as a rotatable plate as seen from the three different axis of rotation X, Y and Z respectively.

c) Operations

Diffusion of the text can be done using clockwise rotations (see Fig. 6) or shifting of elements of the plate (see Fig. 7) using clockwise/circular left shift rotations of a particular plate in a particular axis of rotation as per criteria defined below.

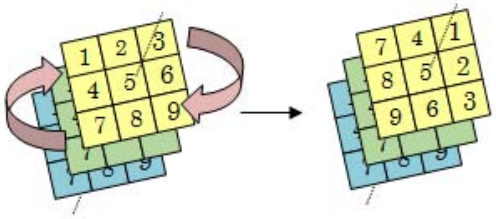


Fig. 6 : Clockwise rotation of Plate 1 along Z-Axis

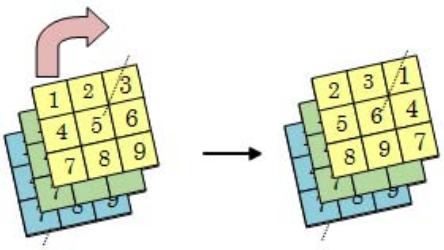


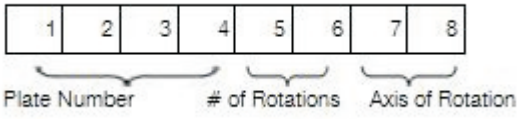
Fig. 7 : Clockwise shift rotation of Plate 1 along Z-Axis by a one unit

d) Key and Rotation Policy

The rotations can be done using a key of 512 bits for 64 rounds cipher. We may also have variable number of rounds by taking key of appropriate number of bits. Each 8 bits from the LSB side can be used to rotate once. Consider 8 bits as shown:

© 2011 Global Journals Inc. (US)

Table 1 : 8-bit subkey bit details



The Plate Number which is to be rotated is straight forward usage of the 4 bits- 1, 2, 3, 4 of the sub-key, whose value indicates the plate number which is to be rotated. In case of 5-6 bits to be 11, we will rotate in order of X, Y and Z axis, taking 5678 bit value number.

The Rotation policy/Number of Rotations can be decided by using 5, 6 bits of the sub-key calculated as described in Table 2:

Table 2 : Rotation Policy

Bit Value	Rotation Type	Clockwise/Shift Left Rotations
00	3D circular rotation	90°
01	3D circular rotation	180°
10	3D circular rotation	270°
11	3D circular shift left rotation	The number of shifts is decided by 5678 bits combination

Similarly, bits 7, 8 of the sub-key can be used to decide the Axis of rotation. The two bits can be used for four possible types of selections represented by 00, 01, 10 and 11 as described in Table 3.

Table 3 : Axis of Rotation Code

Bit Value	Axis of Rotation
00	X
01	Y
10	Z
11	X/Y/Z in rotation starting from X axis

e) Encryption-Decryption Process

The entire encryption process may be converted to a finite number of iterative steps. The encryption can be represented by the flowchart with n-iterations as shown in Fig. 8. It uses the subkey of 8 bit length and identifies the type of rotation to be performed and then do the rotations as described in iteration detail flowchart. Next iteration is carried out on the intermediate ciphertext produced in the previous iteration. This process is repeated n number of times to complete the encryption process.

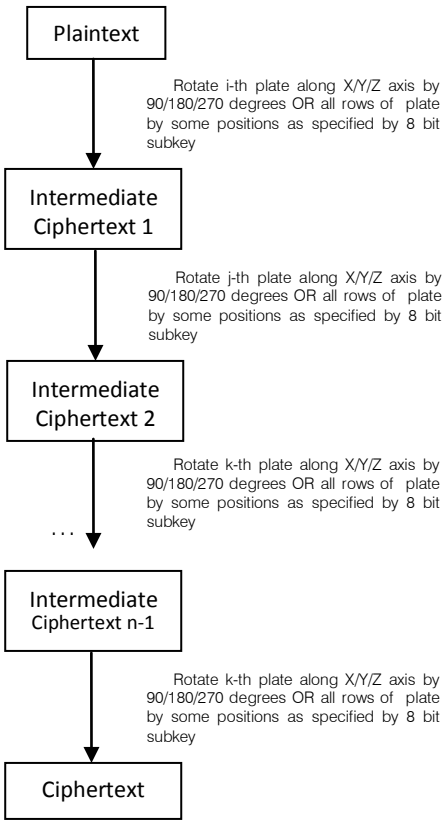


Fig. 8 : Encryption Process

Similarly, the decryption process is carried out exactly in the reverse manner, i.e. the n-th subkey is used first to reverse rotate the plate (in anti-clockwise direction or circular shift right rotation) and thereby obtaining the Intermediate Ciphertext (n-1). The reverse process is to be carried out for the same number of iterations with the same subkeys in reverse order as done in the encryption process. After completion of the n iterations in reverse order, we will obtain the original plaintext, refer Fig. 9.

© 2011 Global Journals Inc. (US)

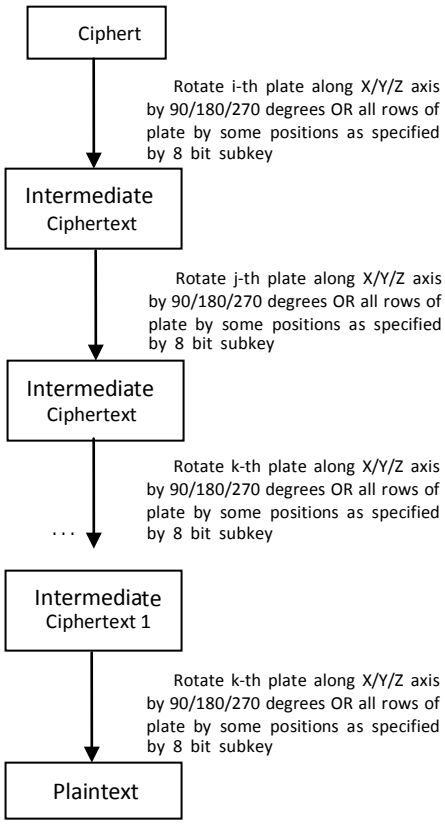


Fig. 9 : Decryption Process

f) Detailed Encryption Flowchart

We provide a flowchart (see Fig. 10) for k-th iteration during encryption process which can be repeated for the Number of Rounds to obtain the ciphertext. We are not providing the detailed decryption process as there is only the change in the rotation involved, i.e. clockwise while encryption and anti-clockwise while decryption. Other parameters like Axis of Rotation and Plate Number remain same while decryption.

`

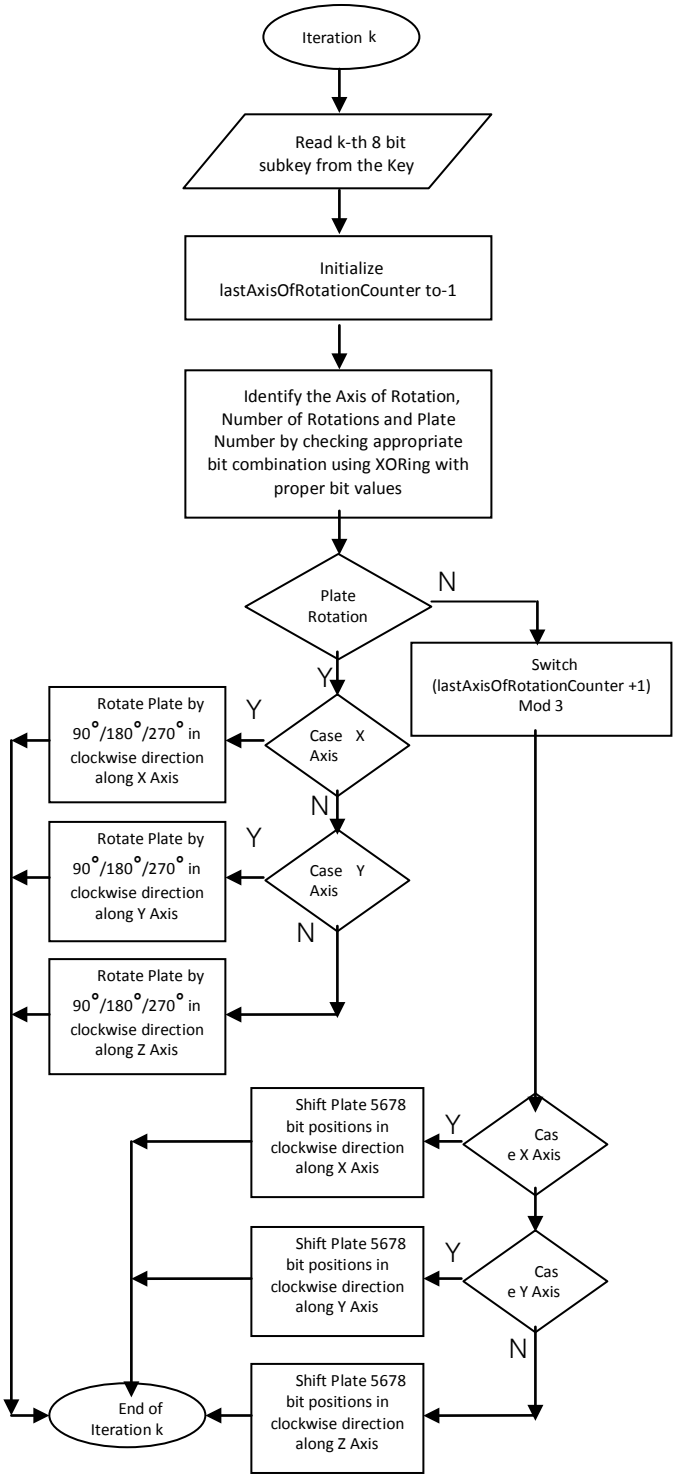


Fig. 10 : Flowchart of k-th iteration during Encryption

V. Experimentation

In order to check the goodness of the improved cipher, we conducted lab experimentations on data in which the plaintext contained two halves, first containing all 0s and second containing all 1s. We have used Turbo C's Random Number Generator to take our keys of desired lengths. Here it is noteworthy that Turbo C's random number generator is not very good RNG.

© 2011 Global Journals Inc. (US)

Here we present the pseudo-code of the algorithm in C. The code contains the major steps to be executed in which it reads the plaintext from a file and encrypt to a ciphertext in the file named out. The algorithm was executed several times to take some arbitrary selected bit lengths for inputs to the NIST tests.

```
#include <stdio.h>
#define size 10
#define ROTATIONS 64

FILE *out;
int i=0,j,k,l,m=1,temp, temp1,half=0,count=0, rot, axis;
//we have implemented using integer cubic array of any size3
int a[size][size][size];
int seq[2*ROTATIONS]={0};


//code for rotating the plate k along particular axis X/Y or Z
rotateX(int k, int ntimes);
rotateY(int k, int ntimes);
rotateZ(int k, int ntimes);

//code for reverse rotating the plate k along particular axis X/Y or Z
reverseRotateX(int k, int ntimes);
reverseRotateY(int k, int ntimes);
reverseRotateZ(int k, int ntimes);


//code for sliding the plate k along particular axis X/Y or Z
slideX(int k, int ntimes);
slideY(int k, int ntimes);
slideZ(int k, int ntimes);


//code for reverse sliding the plate k along particular axis X/Y or Z
reverseslideX(int k, int ntimes);
reverseslideY(int k, int ntimes);
reverseslideZ(int k, int ntimes);


void main(){
//code for initializing the block matrix with data values
while(count++ < ROTATIONS){
//use the 8bit subkey to identify
//Axis or rotation
//Plate Number
//Number of rounds
switch(axis){
        case 0:
                rotateX(rot);
                break;
        case 1:
                rotateY(rot);
                break;
        case 2:
                rotateZ(rot);
                break;
        }
      }else{
        switch ((lastAxisOfRotationCounter +1) mod 3){
        case 0:
                shiftrotateX(rot);
                break;
        case 1:
                shiftrotateY(rot);
                break;
        case 2:
                shiftrotateZ(rot);
                break;
        }
  }
    }
  }

  rotateX(int k, int ntimes){
        //repeat the following code for ntimes
        for(i=0; i<size/2; i++){
                for(j=i; j<size-i-1; j++){
                // code for rotating k-th plate ntimes in clockwise
                // direction
                }
        }
  }


   slideX(int k, int ntimes){
         //here we can put code for sliding each row of plate k of X axis
         for(i=0; i<size/2; i++){
                  for(j=i; j<size-i-1; j++){
                  // code for shifting the terms of each row ntimes
                  }
         }
   }
   //similarly we had coded for other encryption rotation in various axis and the decryption rotation code in reverse direction
```


© 2011 Global Journals Inc. (US)

NOTE: The code for the decrypting process will need the lastAxisOfRotationCounter value and the key. The key will be read in reverse order i.e. starting from 8 LSBs if encryption started from the 8 MSBs.

VI. Some Test Results

We implemented our improved algorithm in C, on a data input of the size 16X16X16 = 163 array upto 32X32X32=323 array. Subsequences from the resultant encrypted text are then used to test the randomness of the bits as follows.

The Initial set of bits taken in the proposed ciphering technique used equal number of 0s and 1s. After enciphering using the above mentioned revised technique, we tested randomly selected 1000 bits for tests of Randomness from NIST specifications. The various tests selected for use by us vary in their importance and hardness as randomness tests [4]. Randomness in the block ciphers is considered as an important aspect of its security. One may apply various tests to ensure that cipher can work like a Random Number Generator (RNG) [7].

a) Monobit Test

In order to determine the number of 0s and 1s in the randomly selected bits after enciphering is approximately the same in proportion or not. If the resultant sequence becomes a random sequence, then arbitrarily selected bits must have approximately equal proportion of 0s and 1s. The focus of the test is the proportion of zeroes and ones for the entire sequence. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same.

Table 4 : P-values for Monobit Test.

S No	p-value
1	0.230139
2	0.071861
3	1
4	0.230139
5	0.548506
6	0.317311
7	1
8	0.423711
9	0.317311
10	1

Result: Arbitrarily selected bits sequences from different length ciphers were selected for the Monobit tests and p-values show (Table 4) that all the tests were passed.

b) Frequency within a Block

Another test of randomness tests the frequency of bits within a block. The focus of this test is on proportion of 1s within M-bit blocks. The purpose of this test is to determine whether the frequency of 1s in an M-bit block is approximately M/2. Our improved algorithm gave p-values as shown (Table 5) for this test.

Table 5 : p-values for Frequency within a Block Test.

Test Number	p-value
1	0.596677
2	0.21934
3	0.688474
4	0.14923
5	0.276677
6	0.75472
7	0.369668
8	0.829425
9	0.428474
10	0.908275

Result: The p-values for this test also show that 100% of the random selected blocks from the encrypted sequence passed all the tests, which is a good improvement.

c) Run Test

The focus of this test is the total number of runs in the sequence, where a run is an uninterrupted sequence of identical bits. A run of length k consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. The test was applied to 10 randomly selected sequences of the encrypted data for which the p-values (Table 6) below.

Table 6 : p-values for Run Test.

Test No	p-Value	Test of Randomness
1	0.622762596	PASS
2	0.161513387	PASS
3	0.505676771	PASS
4	0.333302675	PASS
5	0.363302144	PASS
6	1	PASS
7	0.790469891	PASS
8	0.011561519	PASS
9	0.230139469	PASS
10	0.613523364	PASS

Result: All the ten tests have passed.

d) Random Excursions Test

The focus of this test is the number of cycles having exactly K visits in a cumulative sum random walk. The cumulative sum random walk is derived from partial sums after the (0,1) sequence is transferred to the appropriate (-1, +1) sequence. A cycle of a random walk consists of a sequence of steps of unit length taken at random that begin at and return to the origin. The purpose of this test is to determine if the number of visits

© 2011 Global Journals Inc. (US)

to a particular state within a cycle deviates from what one would expect for a random sequence. This test is actually a series of eight tests (and conclusions), one test and conclusion for each of the states: -4, -3, -2, -1 and +1, +2, +3, +4.

Table 7 : p-values for Random Excursions Test.

FAIL	0
PASS	180
Min	0.3683243
Max	1
Average	0.8612906

The above Table 4 shows the number of tests passed/failed and Min/Max/Average p-value. Out of the 180 tests applied on the random sequences, all tests have passed.

A plot of p-values of various tests other than the random excursions test is shown in Fig. 11. Having p-values≤ 0.1 means test of randomness has failed. The tested sample bits are having good randomness as all the p-values have been greater than 0.01. Although one may point that 4 p-values that are equal to 1, which is the upper limit of p.

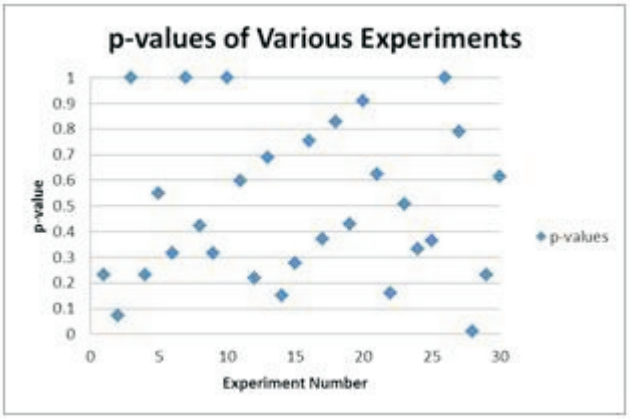


Fig. 11 : p-values of various tests of randomness

VII. Analysis

The above algorithm assumes a pre-requisite of having a good unique generating function for random numbers based on a seed value, the results show that the cipher based on the 3D matrix rotation technique works good and implements confusion/diffusion technique very effectively. This 3D Block ciphering technique can be used in everyday encryption/ decryption as it is having good encrypting/decrypting efficiency too.

VIII. Complex Forms

The reverse computational complexity of the proposed cipher for the interceptors and intruders can be further increased by introduction of XOR round before applying rotation in case of binary input plaintext. This can be done by making use of some agreed upon random number generator which generates unique 8 bit sequences with use of a seed. The generated bits can be XORed with some selected subset of the plate under operation. This will further increase the complexity of the cipher further and will be difficult to decrypt by the interceptors.

IX. Conclusions

The above tests show a high rate of randomness of the bits shuffled using the improved technique. Also since the bits were initially divided in equal numbers in the two halves of the array, this shows that the cipher produces a good confusion-diffusion. It only requires an agreed upon RNG or Key for encryption-decryption. Although the new cipher can have variable number of keys used while encrypting the message, we recommend at least 2n iterations for n^3 size array of input bits/text.

References References Referencias

1. Bruce Schneier: Applied Cryptography, John Wiley & Sons (Asia) Pte Ltd, ISBN 9971-51-348-X.
2. William Stallings: Cryptography and Network Security, Principles and Practices, Fourth Edition, Pearson Education.
3. Seymour Lipschutz: Data Structures, Tata McGraw Hill Publishing Company Ltd.
4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Specifications. SP800-22.
5. D. Gollmann and W.G. Chambers,: Clock-controlled shift registers: a review, IEEE Journal on Communications, VoL. : 7 , Issue : 4, May 1989.
6. P. R. Suri, Sukhvinder Singh Deora: A Cipher based on 3D Array Block Rotation, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010.
7. Mohammed M. Alani: Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
8. S. Dhall, S.K. Pal: Design of a New Block Cipher Based on Conditional Encryption, Seventh International Conference on Information Technology, pages 714, Las Vegas, NV, 12-14 April 2010.

© 2011 Global Journals Inc. (US)

This page is intentionally left blank

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Exploring a Hybrid of Geospatial Semantic Information in Ubiquitous Computing Environments

By Dr. Raghda Fouad, Mohamed Hashem, Nagwa Badr, Hanaa Talha

Ain Shams University

Abstract - Nowadays, geospatial information plays a critical role to each and every one of us. Searching and obtaining the right geospatial information, however, is a difficult and often very time-consuming task. The Semantic Web promises to facilitate this process by improving the capability to search for information by better expressing the context and meaning of the search query. Combining the two approaches to create a Geospatial Semantic Web is an idea that is gaining acceptance in both areas of Geospatial Information Science and Semantic Web Services. Here, we present a prototype that promises to prove that the meshing of these two fields is a promising field especially in conjunction with information retrieval and ubiquitous computing environments. The aim of this prototype is to exploit a hybrid of geospatial semantic information retrieved from multiple data sources in a mobile environment. Our prototype uses three geospatial data sources: GeoNames, LinkedGeoData, and DBpedia. Experimental results show how the merging of the three geospatial data sources and the use of more than one level of indexing is more effective in terms of recall and precision in comparison to another system.

Keywords : *Information Storage and Retrieval, Location-dependent and Sensitive Applications, Mobile Applications.*

GJCST Classification : *H.3.3*

Strictly as per the compliance and regulations of:

© 2011l . Dr. Raghda Fouad, Mohamed Hashem, Nagwa Badr, Hanaa Talha. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Exploring a Hybrid of Geospatial Semantic Information in Ubiquitous Computing Environments

Dr. Raghda Fouad[α], Mohamed Hashem[Ω], Nagwa Badr[β], Hanaa Talha[Ψ]

Abstract - Nowadays, geospatial information plays a critical role to each and every one of us. Searching and obtaining the right geospatial information, however, is a difficult and often very time-consuming task. The Semantic Web promises to facilitate this process by improving the capability to search for information by better expressing the context and meaning of the search query. Combining the two approaches to create a Geospatial Semantic Web is an idea that is gaining acceptance in both areas of Geospatial Information Science and Semantic Web Services. Here, we present a prototype that promises to prove that the meshing of these two fields is a promising field especially in conjunction with information retrieval and ubiquitous computing environments. The aim of this prototype is to exploit a hybrid of geospatial semantic information retrieved from multiple data sources in a mobile environment. Our prototype uses three geospatial data sources: GeoNames, LinkedGeoData, and DBpedia. Experimental results show how the merging of the three geospatial data sources and the use of more than one level of indexing is more effective in terms of recall and precision in comparison to another system.

Keywords : Information Storage and Retrieval, Location -dependent and Sensitive Applications, Mobile Applications.

I. Introduction

The idea of the Semantic Web [1] proposes that it is "a web of data that can be processed directly or indirectly by machines", thus bringing a higher degree of automation in exploiting and retrieving data in a meaningful and more useful way. Semantics is captured by associating formal descriptions to provide well defined meaning to data and other web resources so that information processing (retrieval or integration) can be based on meaning instead of on mere keywords. The W3C Semantic Web Activity Working Group [2] has been working on a series of standards such as the Extensible Markup Language XML, the Resource Description Framework RDF, and the Web Ontology Language OWL. Compared to normal keyword search, a semantic approach in search leads to higher quality of results and more relevant information.

On the other hand, the Geospatial Semantic Web provides better support for geographic information that the basic Semantic Web research has not addressed. In particular, there are three basic dimensions for geographic information on the semantic web: (a) Professional: which is structured geographic information stored in geographic databases which are indexed in web pages [3], (b) Naïve: which includes the retrieval of unstructured informal geographic information in web pages, and (c) Scientific: which is the geographic information science papers, models, and theories. Thus, establishing geographic information on the semantic web is a challenge worth research. Another motivation behind this work is the fact that there is an increasing role and importance of ubiquitous computing and mobile environments in our daily lives. This implies the need for new solutions. Nowadays, the trend is leaning towards processing more and more information using mobile phones. The first reason is because mobile phones have increased in terms of power and space capacity and the second reason is that mobile phones serve as personal computers on the go, offering mobile users all the processing and information they need anywhere.

This paper is structured as follows: Section 2 describes the background of the work. In Section 3, we describe the proposed system's architecture. In Section 4, we demonstrate how the system is implemented. In Section 5, experimental results are shown. The last section contains concluding remarks and recommendations for future work.

II. Background

With the growth of the World Wide Web has come the realization that the currently available methods for finding and using information on the World Wide Web are often insufficient. In order to move the Web from a data repository to an information resource, a totally new way of organizing information is needed. The idea of the Semantic Web promises better retrieval methods by incorporating the data's semantics and exploiting the semantics during the search process. Such a development needs special attention from the geospatial perspective so that the particularities of geospatial meaning are captured appropriately. The creation the Semantic Geospatial Web [3] needs the development multiple spatial and terminological ontologies, each with a formal semantics; the representation of those semantics such that they are

© 2011 Global Journals Inc. (US)

available both to machines for processing and to people for understanding; and the processing of geospatial queries against these ontologies and the evaluation of the retrieval results based on the match between the semantics of the expressed information need and the available semantics of the information resources and search systems. This will lead to a new framework for geospatial information retrieval based on the semantics of spatial and terminological ontologies. By explicitly representing the role of semantics in different components of the information retrieval process (people, interfaces, search systems, and information resources), the Semantic Geospatial Web will enable users to retrieve more precisely the data they need, based on the semantics associated with these data. Geospatial information is critical to every user [4]. Accessing the correct information is a complex task that often requires that the user understand more about the geospatial domain than their knowledge provides. Enabling a query process that allows effective retrieval of the required information is a positive step.

Analysts often need to deal with geospatial information in the course of their duties, such as ascertaining where events may occur and what facilities or logistically important environmental elements are present in an area of concern.

LinkedGeoData [5] transforms and publishes the OpenStreetMap data according to the Linked Data principles to add a new dimension to the Data Web: spatial data can be retrieved and interlinked on an unprecedented level of granularity. This enhancement enables a variety of new Linked Data applications such as geo-data syndication or semantic-spatial searches. The dynamic of the OpenStreetMap project will ensure a steady growth of the dataset.

DBpedia [6] is a community effort to extract structured information from Wikipedia and to make this information available on the Web. It allows users to ask sophisticated queries against datasets derived from Wikipedia and to link other datasets on the Web to Wikipedia data. It is a major source of open, royalty-free data on the Web. By interlinking DBpedia with other data sources, it could serve as a nucleus for the emerging Web of Data.

The GeoNames [7] geographical database contains over eight million geographical names and consists of 7million unique features and 2.8 million alternate names. All features are categorized into one out of nine feature classes and further subcategorized into one out of 645 feature codes. The data is accessible through a number of web services and a daily database export. GeoNames is already serving up to over 11 million web service requests per day. GeoNames is integrating geographical data such as names of places in various languages, elevation, population and others from various sources.

III. Architecture

Earlier work [8] proposed a hybrid of three location-rich data sources to be accessed and queried by mobile users based on their location as received via the GPS module attached to the mobile device. On system startup, the current location of the mobile device is captured from the GPS device and is displayed on a map. Once this is done, the three location-rich data sources, GeoNames, LinkedGeoData and DBpedia are queried for nearby locations of interests based on the longitude and latitude of the current location. Then, the results for the three data sources are parsed merged and displayed on the map to aid mobile uses to disambiguate their current place.

Figure 1 shows the final architecture of the discussed prototype to serve the searching process use case. This architecture demonstrates that the integrated data sources model can serve as a collective geospatial source to query the geospatial semantic web using a mobile device. The mobile user will use this prototype to explore the nearby landmarks around him according to the detected current location and to query the returned nearby results. Multiple levels of indexing are used to assure accuracy of the search results and moreover, better recall.

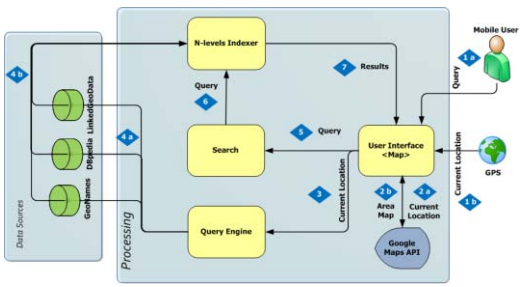


Fig.1 : Architecture of the Prototype for the Searching Process Use Case

The User Interface <Map> module accepts the mobile users' query along with the current location provided by the attached GPS device. Using the longitude and latitude of the current location, a map of the current area is displayed using a Google Maps API [9]. The Map module also serves a result viewer for the results returned from the N-levels Indexer module.

The Query Engine module uses the detected current location of the mobile user as inputs to reformulate the query to be sent to the three data sources. The Query Engine sends the requests to GeoNames, LinkedGeoData and DBpedia simultaneously to return the landmarks and places nearby the current location of the mobile user.

The N-levels Indexer module receives the results returned by each of the three data sources on its own. The first step is to parse the received outputs individually. Next,

© 2011 Global Journals Inc. (US)

the N-levels Indexer module merges the parsed results into one set of results to be indexed into multiple levels for later use by the Search module.

The Search module accepts the query of the mobile user from the User Interface <Map> module. The Search module uses this search query to query the N-levels Indexer to return the search results matching the entered search query.

IV. Implementation

The prototype's initial implementation is done on an iPhone, written in Objective-C [10] hosting an underlying Google Maps API. Experimental results of previous work examined precision and recall of the proposed prototype. For the aim of improving these information retrieval measures, we introduce semantic levels [11]. Semantic levels provide information about word meanings, as described in a reference dictionary, and named entities. Indexing will be performed at multiple separate levels: keyword, senses (word meanings), and entities. Our system will be able to combine keyword search with semantic information provided by the two other indexing levels.

Below is an attempt to detail the three indexing levels and to explain what every level does and how it works. Each level uses the results received from the data sources to index it in a different way thus providing more accurate results in the search process.

a) Keyword Level

The keyword level is the entry level in which the location is represented by the words occurring in its name. It will contain an inverted index structure that will link GPS locations (longitude and latitude pairs) with all the key words that are relevant to the location, that it, any key word that is contained in the name of the location as returned by any of the three data sources. For instance, the location with the following latitude and longitude pair (30, 31) is Maadi Grand Mall, a shopping mall in Maadi, a district in Cairo, Egypt. The following location will be indexed as shown in Figure 2.

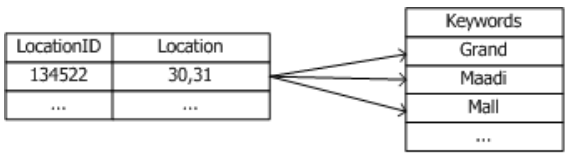


Fig. 2 : Linking between Locations and Keyword in the Keyword Level

b) Word Meaning Level

This level is represented through synsets words obtained by WordNet [12, 13], a semantic lexicon for the English language. Nouns, verbs, adjectives and adverbs in WordNet are grouped into sets of cognitive synonyms (synsets), each expressing a distinct concept. Synsets are interlinked by means of conceptual-semantic and lexical relations. WordNet's structure makes it a useful tool for computational linguistics and natural language processing.

Hence, each word of the query can be further expanded into its synonym words to generate more query words and thus more results, enhancing the recall of the search results. Figure 3 displays an example of the relationship between the keyword (as entered by the mobile user) and its synset (synonym words) in the physical database.

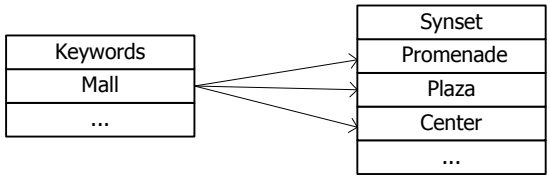


Fig. 3 : Linking between Keywords and Synsets in the Word Meaning Level

c) Named Entity Level

This level consists of entities recognized into the location name text. The integration of named entities and domain ontologies permits some reasoning over location name text. The scope of the work entailed in this paper does not include this level at this time. Yet, this level is left for future works.

V. Experimental Results

a) Experimental Conditions

The proposed system is implemented in Objective-C using Xcode IDE, iOS SDK 4.1 and iOS simulator. Experimental environments consisted of a built-in GPS unit attached to the iPhone used.

b) Introduction to Experimental Results

Figure 4 shows an example of mobile semantic retrieval using the proposed architecture. Figure 4 (a) shows the initial screen of the proposed system with the map centered on the current location of the mobile user with a zoom extent of 1kilometer. The current location of the mobile user is captured using the built-in GPS module in the used iPhone. The user enters the search query in the search area and presses the search button. The search query entered is composed of multiple words that describe a location that the mobile user is interested to find.

In Figure 4 (b) the system displays the search results queried from the three geospatial semantic data sources: LinkedGeoData, DBpedia and GeoNames according to the mobile user's entered search query. The search process relies on the underlying N-Levels indexing process that is composed of the keyword level and the word meaning level.

© 2011 Global Journals Inc. (US)

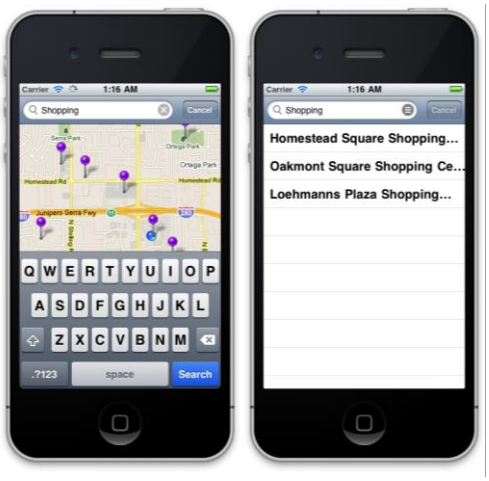


Fig. 4 : (a) Mobile User Entering Search Query, (b) Search Results

c) Information Retrieval Test

To evaluate the proposed system, we used 100 keyword queries and calculated the precision and recall of two systems; our proposed system and Siri [14], a personal assistant application for the iOS which uses natural language processing to answer questions, make recommendations, and perform actions by delegating requests to an expanding set of web services. The aim is to perform a comparison between the two systems. The 100 keywords were chosen so that they are all of known landmarks in California, America. Precision is a test that shows how accurate the search results are in comparison to the entered keyword query. A result is deemed as relevant if the user thinks it is of any relevance to the keyword query entered in search process. Precision is calculated as the number of results deemed as relevant in comparison to the number of results retrieved. Recall is a test that shows how well the search results yields. Recall determines how many relevant results are retrieved in the search process. The more relevant search results are presented, the better the retrieval process is. Precision and recall measures complement each other, that is, the higher the precision of an information test, the lower its recall is and vice versa. This is due to the fact that the more results presented, the less accurate they are. Figure 5 and 6 below display a comparison between the recall and precision measures computed of the two systems.

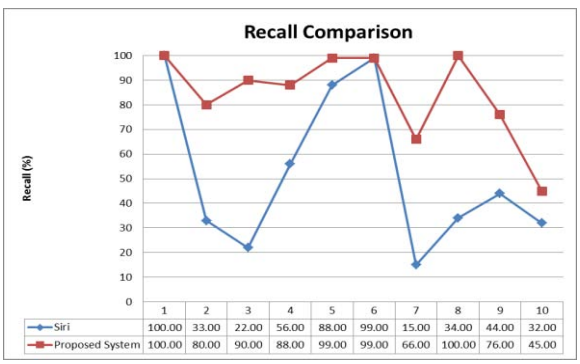


Fig.5 : Comparison between the Recall of our System and Siri

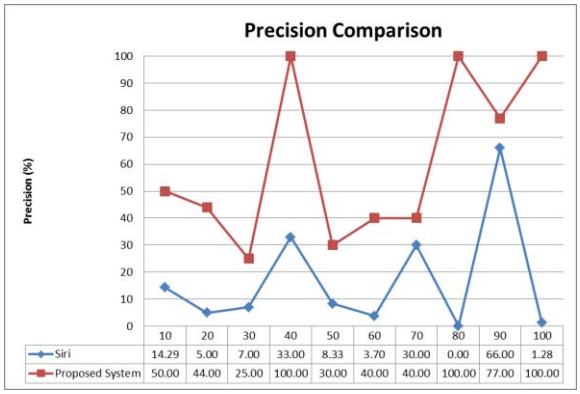


Fig. 6 : Comparison between the Precision of our System and Siri

As the graphs above show, the precision of our proposed system exceeds that of Siri, that is because of the merging between the keyword search and semantic search in the N-levels indexing process. Moreover, the word meaning levels provides for more query expansions for the entered query which improves the recall of our system.

VI. Conclusion

We have introduced an implementation of a prototype that aims to explore and examine the geospatial semantic information available and make the best use out of it. The prototype is composed of a location-centric mobile client application that provides the mobile user with rich location information around them. Based on the current GPS position of a mobile device, the application renders a map indicating the mobile devices current location and nearby locations of interest from the three data sources, GeoNames, LinkedGeoData and DBpedia.

Furthermore, the mobile user can search for locations of interest and view the search results in a timely manner. Starting from this map, users can explore information about locations and can navigate interlinked data sources.

Future work include the expansion of the multi-level indexing to include the named entity level that consists of entities recognized into the location name text. The integration of named entities and domain ontologies permits some reasoning over location name text.

References References Referencias

1. Tim Berners-Lee, James Hendler and Ora Lassila. The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. The Scientific American, 2001, 284: 34-43.
2. W3C Semantic Web Activity.http://www.w3.org/200/sw/
3. Max J. Egenhofer. Toward the Semantic Geospatial Web. In Proc. 10th ACM Int. Symp. on Advances in Geographic Information Systems, 2002.

© 2011 Global Journals Inc. (US)

4. Damian O'Dea, Sean Geoghegan and Chris Ekins. Dealing with Geospatial Information in the Semantic Web. In Proc.1st Australasian Ontology Workshop, Vol. 58, 2005.
5. Soren Auer, Jens Lehmann, and Sebastian Hellmann. LinkedGeoData - Adding a Spatial Dimension to the Web of Data. In Proc.7th International Semantic Web Conference, 2009.
6. Soren Auer, Christian Bizer, Georgi Kobilarov, Jens Lehmann, and Zachary Ives. DBpedia: A nucleus for a web of open data. In Proc. 6th International Semantic Web Conference, Springer, 2007, pp.11-15.
7. GeoNames. http://www.geonames.org/about.html
8. Raghda A. Fouad, Nagwa Badr, Hanaa Talha and Mohamed Hashem. On Location-Centric Semantic Information Retrieval in Ubiquitous Computing Environments. International Journal of Electrical & Computer Sciences IJECS -IJENS, 2010, Vol. 10 No: 06.
9. Google Maps JavaScript API V3. http://code.google.com/ apis/maps/documentation/javascript/
10. Mark Dalrymple and Scott Knaster. Learn Objective-C on the Mac, 2009.
11. Pierpaolo Basile, Annalina Caputo, Anna Lisa Gentile, Marco Degemmis, Pasquale Lops, and Giovanni Semeraro. Enhancing Semantic Search using N-levels Document Representation. In Proc. ESWC 2008 Workshop on Semantic Search (SemSearch2008).
12. George A. Miller (1995). WordNet: A Lexical Database for English. Communications of the ACM Vol. 38, No. 11: 39-41.
13. Christiane Fellbaum (1998, ed.) WordNet: An Electronic Lexical Database. Cambridge, MA: MIT Press.
14. Siri, Your Virtual Personal Assistant. http://www.siri.com

© 2011 Global Journals Inc. (US)

This page is intentionally left blank

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Segmentation of Microarray Image Using Information Bottleneck

By S.Raghavarao, M.S.Madhanmohan, Dr.G.M.V.Prasad

BVC Engineering College, Odalarevu

Abstract - DNA microarrays provide a simple tool to identify andquantify the gene expression for tens of thousands of genessimultaneously. The DNA microarray image analysis includes three tasks: gridding, segmentation and intensity extraction.Spots segmentation, which isto distinguish the spot signals from background pixels,is a critical step in microarray image processing. In this paper, new image segmentation algorithm based on the hard version of the information bottleneck method is presented. The objective of this method is to extract a compact representation of a variable, considered the input, with minimal loss of mutual information with respect to another variable, considered the output. The input variable here, is the histogram bins and the output variable is the set of regions obtained from the split and merge algorithm. The proposed method is compared with existing segmentation methods such as k-means and Fuzzy C-means. The experimental results show that the proposed algorithm has segmented spots of the microarray image more accurately than other segmentation methods.

Keywords : *Image Processing, Microarray, Image Segmentation.*

GJCST Classification : *I.4.5, I.4.4*

Strictly as per the compliance and regulations of:

© 2011I . S.Raghavarao, M.S.Madhanmohan, Dr.G.M.V.Prasad. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Segmentation of Microarray Image Using Information Bottleneck

S.Raghavarao [α], M.S.Madhanmohan [Ω], Dr.G.M.V.Prasad [β]

Abstract - **DNA microarrays provide a simple tool to identify andquantify the gene expression for tens of thousands of genessimultaneously. The DNA microarray image analysis includes three tasks: gridding, segmentation and intensity extraction.Spots segmentation, which isto distinguish the spot signals from background pixels,is a critical step in microarray image processing. In this paper, new image segmentation algorithm based on the hard version of the information bottleneck method is presented. The objective of this method is to extract a compact representation of a variable, considered the input, with minimal loss of mutual information with respect to another variable, considered the output. The input variable here, is the histogram bins and the output variable is the set of regions obtained from the split and merge algorithm. The proposed method is compared with existing segmentation methods such as k-means and Fuzzy C-means. The experimental results show that the proposed algorithm has segmented spots of the microarray image more accurately than other segmentation methods.**

Keywords : Image Processing, Microarray, Image Segmentation.

I. Introduction

Microarrays, widely recognized as the next revolution in molecular biology, enable scientists to analyze genes, proteins and other biological molecules on a genomic scale [1]. A microarray is a collection of spots containing DNA deposited on the solid surface of glass slide. Each of the spot contains multiple copies of single DNA sequence [2].

Microarray expression technology helps in the monitoring of gene expression for tens and thousands of genes in parallel. During the biological experiment, the mRNA of two biological tissues of interest is extracted and purified. Each of the mRNA samples are reverse transcribed into complementary DNA (cDNA) copy and labeled with two different fluorescent dyes resulting in two fluorescence-tagged cDNA (red Cy5 and green Cy3). The tagged cDNA copies, called the sample probe, are hybridized with the slide's DNA spots. The hybridized glass slides are fluorescently scanned at different wavelengths (corresponding to the different dyes used), and two digital images are produced, one for each population of mRNA. Each digital image contains a number of spots of various fluorescence intensities. The intensity of each spot is proportional to the hybridization level of the cDNAs and the DNA dots, the gene expression information is obtained by analyzing the digital images [3].

The processing of the microarray images usually consists of the following three steps: (i) gridding, which is the process of assigning the location of each spot in the image. (ii) Segmentation, which is the process of grouping the pixels with similar features and (iii) Intensity extraction, which calculates red and green foreground intensity pairs and background intensities.

Nowadays, segmentation algorithms such as K-means and Fuzzy C-Means have been used for the segmentation of spots of the microarray images. In this paper, we present a histogram clustering algorithm for segmentation of spots of the microarray image. The proposed algorithm is based on the minimization of the mutual information loss, where now the input variable represents the histogram bins and the output is given by the set of regions obtained from the split and merge algorithm.

The rest of the paper is organized as follows.

Section II presents K-Means Algorithm, Section III presents Fuzzy C-Means Algorithm, Section IV presents present Histogram Clustering algorithm for segmentation of spots in Microarray image, Section V presents experimental results and finally Section VI reports conclusion.

II. K-means Clustering Algorithm

K-means is one of the basic methods in clustering introduced by Hartigan et al. in 1979 [3]. This method is applied to microarray image segmentation in recent years [21]. K-means clustering algorithm implemented in this paper aims to group the pixels into two clusters. Given $x = \{x_1, x_2, \ldots, x_N\}$ and $c = \{c_1, \ldots c_j\}$ representing the pixels of microarray image and clusters respectively, the objective is to minimize the sum of squares of the distances given by the following:

$$d_{ij} = || x_i - c_j ||. \quad arg\ min \sum_{i=1}^{N} \sum_{j=1}^{C} d_{ij}^2 \qquad (1)$$

First two cluster centers c_1 and c_2, the centroid of spots and background have to be initialized at the outset. Iteratively, the pixels are assigned to the closest cluster and the new centroid of a cluster is calculated by the following: The k-means algorithm to segment microarray image is summarized as below:

Author α Ω β : BVC Engineering College, Odalarevu.

© 2011 Global Journals Inc. (US)

Algorithm KM(x,n,c)
Input:
N=number of pixels to be clustered;
x = {x_1,x_2 ,...,x_N} pixels of microarray image;
c=2: foreground and background clusters;
Output:
cl: cluster of pixels

Begin
Step_1: Cluster centroids are initialized,
Step_2: Compute the closest cluster for each pixel and classify it to that cluster,
Step_3: Compute new centroids after all the pixels are clustered,
Step_4: Repeat the Steps 2-3 till the sum of squares given in Equation
End.

III. Fuzzy C-Means Clustering

Algorithm Fuzzy C-Means(x,n,c,m)
Input:
N=number of pixels to be clustered;
x = {x1,x2 ,...,xN}: pixels of microarray image;
c=2: foreground and background clusters;
m=2: the fuzziness parameter;
Output:
u: membership values of pixels

Begin
Step_1: Initialize the membership matrix u_{ij} is a value in (0,1) and the fuzziness parameter m. The sum of all membership values of a pixel belonging to clusters should satisfy the constraint expressed in the following.

$$\sum_{j=1}^{c} u_{ij} = 1 \qquad (2)$$

For all i= 1,2,…….N, where c is the number of clusters and N is the number of pixels in microarray image.

Step_2: Compute the centroid values for each cluster c_j. Each pixel should have a degree of membership to those designated clusters. So the goal is to find the membership values of pixels belonging to each cluster. The algorithm is an iterative optimization that minimizes the cost function defined as follows:

$$F = \sum_{j=1}^{N} \sum_{i=1}^{c} u_{ij}^{m} \, || x_j - c_i ||^2 \qquad (3)$$

Where u_{ij} represents the membership of pixel x_j in the i^{th} cluster and m is the fuzziness parameter.

Step_3: Compute the updated membership values u_{ij} belonging to clusters for each pixel and cluster centroids according to the given formula.

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{\|x_j - v_i\|}{\|x_j - v_k\|} \right)^{2/(m-1)}},$$

and

$$v_i = \frac{\sum_{j=1}^{N} u_{ij}^{m} x_j}{\sum_{j=1}^{N} u_{ij}^{m}}. \qquad (4)$$

Step_4: Repeat steps 2-3 until the cost function is minimized.

End.

IV. Histogram Clustering Algorithm

We present a greedy histogram clustering algorithm that takes as input partitioned image and obtain histogram clustering based on the minimization of the loss of Mutual Information. The Mutual Information between two random variables X and Y is defined by

$$I(X,Y) = H(X) - H(X|Y)$$

$$\text{Where } H(X) = -\sum_{x \in X} p(x) \log p(x) \text{ and}$$

$$H(X|Y) = -\sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log p(y|x) \qquad (5)$$

That is we group the bins of the histogram so that the mutual Information is maximally preserved. From the perspective of the information bottleneck method the binning process is controlled by a given partition of the image. The histogram clustering algorithm is presented in [9].

Our Clustering algorithm is based on the channel G→R, and is defines by the conditional probability matrix p(R|G) which expresses how the pixels corresponding to each histogram bin are distributed into regions of the image . Bayes' theorem, expressed by p(g)p(r|g)=p(r)p(g|r), establishes the relationship between the conditional probabilities of both channels G→R and R→G. The basic idea underlying our histogram clustering algorithm is to capture the maximum information of the image with the minimum number of histogram bins. In general, if the two bins are very similar the channel can be simplified by substituting these two bins by their clustering, without a significant loss of information. The algorithm proceeds by merging the two bins so that the loss of information is minimum. During the clustering process H(R)=H(R|G) + I(G,R), where H(R) is the entropy of p(R) and H(R|G) and I(G,R) represent, respectively, the successive values of conditional entropy and MI obtained after successful clusterings. Observe also that H(R|G) is the average entropy of the bins and increases at each iteration.

© 2011 Global Journals Inc. (US)

V. Experimental Results

Segmentation steps of the microarray image processing are performed on a sample microarray slide that has 48 blocks, each block consisting of 110 spots. A sample block has been chosen and 108 spots of the block have been cropped for simplicity. The sample image is a 154*200 pixel image that consists of a total of 30800 pixels. The RGB colored image microarray image have been converted to grayscale image to specify a single intensity value that varies from the darkest (0) to the brightest (255) for each pixel shown in figure1.

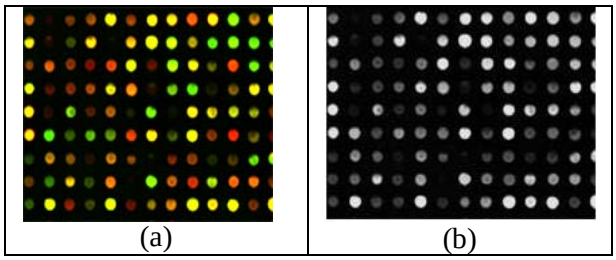


Fig1 : a) RGB Color microarray image b) Grayscale Image

The segmented microarray image using three different segmentation algorithms (K-means, Fuzzy c-Means and Histogram Clustering algorithm) is shown in figure 2.

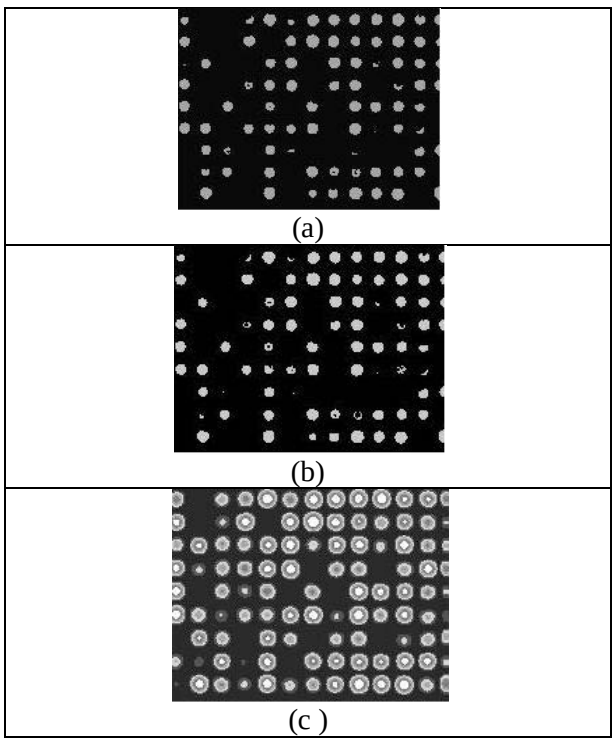


Fig2 : a) K-means b) Fuzzy c-means c) Histogram Clustering Algorithm

The histogram gives the distribution of intensity values for each cluster. The K-means have calculated mean of the spots as 25.32 and the mean of the background as 74.68 for this sample and clustered 7800 pixels as fore and 23,000 pixels as back. The Histogram Clustering has calculated mean of the spots as 40.64 and the mean of the background as 59.35 for this sample and clustered 12,520 pixels as fore and 18,280 pixels as back. The proposed algorithm have calculated mean of the spots as 49.35 and the mean of the background as 50.64 for this sample and clustered 15,200 pixels as fore and 15,600 pixels as back.

VI. Conclusion

Histogram clustering algorithm constitutes a valid tool to segment the spots of microarray image. Even though the mathematical bases for these techniques are complex, their implementation is simple, quick and easier on the user. The proposed segmentation algorithm has the advantage of processing spots of variable shapes and being insensitive to variations. In order to process the images of low intensity background correction is necessary. The proposed algorithm provides a more efficient way of segmenting the microarray image when compared with the segmentation achieved by K-Means and Fuzzy c-Means.

References References Referencias

1. M.Schena, D.Shalon, Ronald W.davis and Patrick O.Brown, "Quantitative Monitoring of gene expression patterns with a complementary DNA microarray", Science, 270,199,pp:467-470.
2. Wei-Bang Chen, Chengcui Zhang and Wen-Lin Liu, "An Automated Gridding and Segmentation method for cDNA Microarray Image Analysis", 19th IEEE Symposium on Computer-Based Medical Systems.
3. Tsung-Han Tsai Chein-Po Yang, Wei-ChiTsai, Pin-Hua Chen, "Error Reduction on Automatic Segmentation in Microarray Image", IEEE 2007.
4. E.Erguit, Y.Yardimci, E.Mumcuoglu, O.Konu, "Analysis of microarray imagesusing FCM and k-means Clustering Algorithm", in Proc IJCI, pp.116-121, 2003.
5. Volkan Uslan, Ihsan Omur Bucak, Clustering based Spot Segmentation of cDNA Microarray Images, IEEE 2010.
6. Rafael C.Gongalez, Richard E.Woods," Digital Image Processing ",Third Edition, Pearson Education.
7. T.Deng and H.Heijmans, " Grey-Scale Morphology Based on Fuzzy Logic", Journal of Mathematical Imaging and Vision, Springer Netherlands, vol 16, no 2, pp. 155-171, 2002.
8. M.A.Wirth, D.Nikitento ,"Application of Fuzzy Morphology to Contrast Enhancement", 2005 IEEE.
9. J.Rigau, M.Feixas and M.Sbert," An Information Theoretic Framework for image segmentation", IEEE 2004.

© 2011 Global Journals Inc. (US)

This page is intentionally left blank

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Key Issues in Information Systems Management: A Serbia's Perspective (Delphi study)

By Dr. Jelisavka Bulatovic

Abstract - Delphi study used by many authors to compile a list of key issues related to information systems (IS) management in the world, i.e. to classify them and display their meaning. A key focus in this paper was put on trial IS managers in all areas, with emphasis on identifying and explaining regional similarities and differences. The results presented and compared with those obtained in similar studies in the U.S. and other European and non-European countries. Our research evidence points to profound differences in IS management between Serbia, the U.S. and other countries. The aim of this study was to identify key issues in organizations for management information systems over the next 3 to 5 years.

Keywords : *key issues, information system, Serbian, Delphi study.*

GJCST Classification : *K.6.m*

Strictly as per the compliance and regulations of:

© 2011l . Dr. Jelisavka Bulatovic. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Key Issues in Information Systems Management: A Serbia's Perspective (Delphi study)

Dr. Jelisavka Bulatovic

Abstract - Delphi study used by many authors to compile a list of key issues related to information systems (IS) management in the world, i.e. to classify them and display their meaning. A key focus in this paper was put on trial IS managers in all areas, with emphasis on identifying and explaining regional similarities and differences. The results presented and compared with those obtained in similar studies in the U.S. and other European and non-European countries. Our research evidence points to profound differences in IS management between Serbia, the U.S. and other countries. The aim of this study was to identify key issues in organizations for management information systems over the next 3 to 5 years.

Keywords : key issues, information system, Serbian, Delphi study.

I. Introduction

Our intentions are modest, and the scope for detailed analysis is limited. So do not pretend to exhaust these issues, but a text we want to provide a contribution to the study of key issues in information management systems - Delphi studies in Serbia. In this regard we have attempted, through previous research and methodology, point out the similarities and differences in management information systems (IS) between Serbia, the U.S. and other European countries. Accepting such a criterion, we imposed the need to orient our study in two directions. The first direction, Serbian compared with those key issues that are defined in previous studies (which were conducted in different countries), and were primarily related to the different times. The second line refers to a shared vision of critical an issue information system applied at different levels of the organization. Therefore, the results not related to IS staff as a whole, but data collection is limited to IS managers. Moving to the collection of data at different levels allows IS staff to examine whether the "vision" at the top IS manager associated with the perspectives of IS professionals in other organizational levels. Depending on this, the question is whether Serbia has a unique set of circumstances in compared to other countries. Bearing in mind that the Serbian economy, from the sixties suffered a lot of negative impact because the period of industrialization, and the early nineties isolation, through social and economic crisis and lack of economic development strategy long-term, stopped its social, technical and technological development. In this regard, this work tries to answer the following questions:

1. What are the ten most critical management and technical issues, and the order of importance of these issues with staff that will in Serbia to face in the next 5 years?
2. What is the consensus between the different levels of IS staff and what their significance on the key issues of IS management?
3. What is the relationship between Serbian ten critical issues in comparison with data obtained in international studies or similar during different periods?

Serbia has a continental country in the Balkans - South Eastern Europe (about 80% of the territory) and the Pannonian plain - a region of Central Europe (about 20% of the territory). In the north of the Serbian, border with Hungary to the northeast and east Romania and Bulgaria. The southern boundary with the Republic of Macedonia, while in southwest Albania, Montenegro and to the west of Croatia and Bosnia and Herzegovina. However, geographical, and climate, one part is considered in Mediterranean countries. Total length of borders with neighboring countries is 2,397 km, of which 1,717 km land and 680 km of river. Serbia since the end of First World War was the founder and integral part of a joint state with most of the Balkan South Slavic originally in the Kingdom of Serbs, Croats and Slovenes, later renamed the Kingdom of Yugoslavia. Later he was an integral part of the Socialist Federal Republic of Yugoslavia, Federal Republic of Yugoslavia and the State Union of Serbia and Montenegro. Since 2006 as a successor is, Serbia and Montenegro became a sovereign and independent state. Serbian economy was in collapse during the 1990s. In 1993, he recorded the second highest inflation in the history of economics • 1023 2.35 per cent (64% daily). Serbia introduced general sanctions the UN Security Council 1992nd. Much of the sanction lifted in 1996, 2000, 2001 and 2005, when it is fully normalized trade with the United States. Agriculture accounts for 16.6% of national GDP, industry 25.5% and service sector 57.9%.

II. Previous Research

Problems of the key issues in managing information systems, today is definitely one of the most research areas, which attracts attention with its IT

© 2011 Global Journals Inc. (US)

actuality thought, both in highly developed countries, and in those that are traditionally referred to as developing countries - Serbia. Dealing with the analysis of key issues in managing information systems, many authors have also applied the Delphi method. We have deliberately called attention to this fact, to present a historical overview of major studies on the proposed topic.

Table 1 : A History of Key Issues Studies

Authors	Year of study	Country
Ball, L. & Harris, R.	1982	SAD
Martin, E.W.	1982	SAD
Dickson G.W., et al.	1984	SAD
Hartog, C. & Herbert, M.	1986	SAD
Brancheau, J.C. & Wetherbe, J.C.	1987	SAD
Rao K.V., et al.	1987	Singapore
Davenport, T. & Buday, R.	1988	Europe
Parker, T. & Idundum, M.	1988	United Kingdom
Watson, R.T.	1989	Australia
Harrison, W.L. & Farm, C.K.	1990	Taiwan
Kremar, H.O.A.	1990	Germany
Moynihan, T.	1990	Ireland
Deans P. C., et al.	1991	SAD
Zupančić, J., Leskovar, R.	1991	Slovenia
Caudle S.L., et al.	1991	SAD
Neiderman F., et al.	1991	SAD
Watson, R.T. & Brancheau, J.C.	1991	International comparison
Palvia P.C. & Palvia S. C.J.	1992	India
Badri, M.A.	1992	Gulf Coop`n Council
Clark, T.D.	1992	SAD
Doukidis G.I., et al.	1992	Greece
Pervan, G.P.	1993, 1994	Australia
Burn J., et al.	1993	Hong Kong
Dexter A.S., et al.	1993	Estonia
Wang, P. & Turban, E.	1994	Taiwan
Wrycza, S., Plata-Przechlewski, T.	1994	Poland
Galliers, R. D., et al.	1994	United Kingdom
Davis J.G., et al.	1995	New Zealand
Kim, Y.G. & Sato, O.	1995	Japan
Brancheau, J.C., et al.	1996	SAD
Deklava, S. & Zupancic, J.	1996	Slovenia
Moores, T.	1996	Hong Kong
Yang, H.L.	1996	Taiwan
Mata, F. J. & Fuerst, W.L.	1997	Costarica
Burn, J.M., Szeto C.	1998	Hong Kong
Chou, H.W. & Jou, S.B.	1999	Taiwan
Haynea, S.C. & Pollard, C.E.	2000	Canada
Gottschdk P., et al.	2000	Norwegian
Shi Y., et al.	2000	China
Berkowitz S., et al.	2001	South Africa
CSC Index	2002	World Wide
Palvia P.C., et. al	2002	International comparison
Armstrong T., et al.	2002	South Africa
Pimchangthong D., et al.	2003	Thailand
Keizer G.	2004	International comparison
Chen G., et al.	2005	China
Jerry Luftman, et al.	2005	South Africa
Dutta S., et al.	2006	International comparison
Jerry Luftman, et al.	2009	International comparison
Li D., et al.	2010	International comparison

© 2011 Global Journals Inc. (US)

In early eighties, the first study surveyed managers and IS managers to identify key issues in the management appeared in society for information management (SIM card) in the United States. Key issues in systems management information systems in the United States dealt with in the 1980s (Ball, L. & Harris, R., 1982, Martin, E.W. 1982, Dickson, G.W. et al., 1984, Hartog, C. & Herbert, M., 1986, Brancheau, J.C. & Wetherbe, J.C., 1987). Initially, a set of questions proposed by the Group of Experts for the SIM, and subsequently evaluated 417 members of the society. The analysis results show that the most important issues for the American organization at that time was MIS-term planning and integration, calibration MIS effectiveness and impact of communication at MIS. Later this method of collecting and reporting periodically repeated in the U.S.: Brancheau, J.C. & Wetherbe, J.C. (1987), Deans, P.C. et al. (1991), Niederman, F. et al. (1991), Caudle, S.L. et al. (1991), Brancheau, J.C. et al. (1996) and so on. Similar studies eighties carried out in several other countries, for example: Australia (Watson, R.T., 1989), United Kingdom (Parker, T. & Idundum, M., 1988), Singapore (Rao, K.V. et al., 1987) and Europe (Davenport, T. & Buday, R., 1988). Since the early nineties, the key issues in IS management dealt with other countries and regions of the world: Taiwan (Harrison, W.L. & Farm C.K., 1990, Wang, P. & Turban, E. 1994), Japan (Kim, Y.G. & Sato, O. 1995), Germany (Kremar, H.O.A., 1990), Slovenia (Zupancic, J., Leskovar, R., 1991), Estonia (Dexter, A.S., et al., 1993), Ireland (Moynihan, T. 1990), United Kingdom (Galliers, R.D. et al., 1994), Australia (Pervan, G.P., 1993.1994), New Zealand (Davis J.G. et al., 1995), Poland (Wrycza, S., Plata- Przechlewski, T., 1994), Greece (Doukidis, G.I. et al., 1992), USA (Clark, T.D., 1992, Badri, M.A., 1992).

In their study, Watson, R.T. & Brancheau, J.C. (1991) found that management information systems, depends on the degree of development and cultural environment. Meanwhile authors Deans, P.C. et al. (1991) explain the key issues in IS management and stress that depend on the political, legal, economic, cultural and technological environment in the country. In the same year (1991) in their study, Moeller, G.E.W., emphasizes that the main factors that will determine the market development of information technology (IT), German unification and the creation of Eastern Europe.

Restrictions on exports of high technology from the West built at the end of the Cold War. So Dyson, E. (1993) predicts that the development of computing - the future of the Eastern European countries, as long Kempfer, L. (1993) indicates that the fastest growth in value added in the retail business, be just in the Eastern European countries (the business is expected to expand at an annual rate of about 20%, over the next five years). Several researchers, among which mention Angus, J. (1990), Hotopf, M., 1992, Saunier, F., et al, 1993, note that the increased computer sales in Eastern Europe, the collapse of the centralized economy, produce a great demand for computer systems, and possibly because the technological infrastructure was severely neglected and all that is happening in Europe is obviously important for hightech vehicles from the west and the IT industry in general. Therefore, Dyson (1993) identifies two groups for the development of IT. In the first group of states: Slovenia, Hungary, the Czech Republic and Poland, and another one: the Baltic republics, Romania, Ukraine, Russia and other countries - the Commonwealth of Independent States, which have promising conditions for the development of IT.

The last two decades have witnessed tremendous success of information technology (IT), who are deeply change the way companies run their business. Information systems (IS) departments of organizations today face many challenges in a rapidly changing environment, from which it follows that it is important to answer all the challenges of managing IS (Niederman, F. et. al, 1991).

Key issues in systems management information systems, dealt with during the nineties and later in many countries: Canada (Haynea, S.C. & Pollard, C.E., 2000), India (Palvia, P.C. & Palvia, S.C.J., 1992), Central America (Mata, F.J. & Fuerst, W.L., 1997), Thailand (Pimchangthong, D. et al., 2003), Slovenia (Dekleva, S. & Zupancic, J., 1996), Hong Kong (Burn, J. et al., 1993, Moores, T., 1996, Burn, J.M., Szeto C., 1998), North Africa (Berkowitz S., et al ., 2001, Jerry Luftman, et al., 2005), Taiwan (Chou , H.W. & Jou, S.B., 1999, Yang, H.L., 1996). Thus, computer science Corporation (CSC) began to research the key issues in IS management systems in enterprises worldwide. In the period since 1987 the 2001 survey which referred to the key issues for IS management have been implemented 14 times, so rich in historical data accumulated, i.e. revealed some new trends in IS (CSC, 2002). Other investigators have compared the results of the above studies in different countries of the world and regions, seeking to identify and explain regional similarities and differences between them (Palvia P.C. et. al, 2002, Keizer G., 2004, Dutta S. et al., 2006, Jerry Luftman, et al., 2009, Lee D. et al., 2010). Thus, Watson, R.T. and associates (1991, 1997) points out that in both studies the key IS management issues affecting the four dominant factors: the economic structure, national culture, political / legal environment and technological status. On the other hand, Gottschalk, P. (2000) states that the key issues for the management of IS generally defined as a set of major challenges faced by IS managers in the next 3 to 5 years, which deserve the most resources, time and attention of management. The same allegations confirmed by Shi, Y. et al., (2000) and Chen G. et al., (2005) and related to the management of Chinese enterprises. However, during the nineties, the focus of IS managers has changed significantly, i.e. Right now the focus is on rapid development and construction of IT.

© 2011 Global Journals Inc. (US)

And that's number one issue at the beginning and middle of the 1990s, by analyzing Niederman, F. et al. (1991) in his book "The development of information architecture" and Brancheau, J.C. et al., (1996) in "Building IT infrastructure." However, the importance of computer issues, such as training of end users and IT satisfaction decreases dramatically. That is to say that facilitate organizational learning and the use of IT ranked number five in 1991 and 1996, but it turns out the Top 10 - the key IS management issues. Not only is the IS strategic planning, is no longer the number one issue in rank, but the number three on the list Niederman, F. et al. (1991), Brancheau, J.C. et al. (1996) and number nine on the list Brancheau, Janz and Wetherbe's (1987). Importance of the issue -proof of competitive advantage, falling to number two (Brancheau, JC & Wetherbe, J.C., 1987) to number eight on the list of key IS management issues (Niederman, F. et al. 1991). Above, by the fact that the IT industry in the United States, now more mature and the position of IS departments within the organization greatly strengthened. One interesting development in the early nineties of last century proceeded from the importance of the issue IS employees, recruitment, training and retention. Employment and Human Resources Development IS was ranked as number four in the early 1990s (Niederman, F. et al. 1991), but was completely knocked out of the top 20 key issues of IS management, several years later (Brancheau, J.C. et al. 1996).

III. Methodology

a) Delphi method

Delphi method used for organizing and prioritizing collective judgments and group means iteratively capture the same group (Scala, S., McGrath R., 1993, de Haan, J., Peters, R., 1993, Doke E.R., Swanson N.E., 1995). The starting point is the method of defining the problem for which the forecast. After is defining the problem, a group of experts who will participate in the forecasting. It is clear that the prerequisite conditions of choice of most competent experts in the subject area, those who know best studied phenomenon. Contacts with experts conducted through a series of questionnaires. Through the questionnaire, they asked a variety of information and forecasts, with the anonymity of the experts and forecasts obtained guaranteed.

The first series of questionnaires provided to the experts included the necessary information, and will ask to give their prognosis, which must supported by appropriate arguments. Based on the obtained forecasts, access to and forming a list of questions that are important for proper research.

In the second series of questionnaires that are sent to experts calculated the average forecast that represent the average of individual forecasts, as well as the variation around the mean forecast of forecast accuracy is a measure, calculated average forecast, forecast and measure the accuracy of their forecasts of extreme reasons. Since experts then asked to reconsider their initial prognosis, do the possible corrections and submit their opinions about extreme forecasts together with the appropriate arguments. This process is done in several steps - usually four, and the final forecast is obtained as the mean forecast from the latest series of questionnaires.

The advantage of Delphi method is that the common forecast gets organized, systematic harmonization of individual forecasts and the addition of quality, can obtained, and quantitative indicators predicted phenomena. Lack of Delphi method is unable to determine the optimal size of groups of experts. In fact, it seems that a large group of experts to enhance accuracy of predictions. However, it is very difficult to assemble large enough for a competent group of experts to study the phenomenon, so that a large group usually contains a small number of true experts, specialist the studied phenomenon. Delphi technique used in a series of studies in the United States is particularly suitable to explain the key issues in systems management information systems. In this way comparable, to accumulate information and knowledge of IS practices and regional differences can be determined. This study is a repetition of American Studies, but carried out in Serbia.

b) Method of research and data collection

Our study conducted in 2009 and 2010. With the help of the Commercial Register of the Republic of Serbia and the Statistical Yearbook of the Republic of Serbia elected a mailing list from Serbian 360 industrial, commercial and service organizations with more than 300 employees. Greater political and economic changes started in Serbia, a dynamic enterprise restructuring and adjustment to a new situation practically narrowed the market for the former Yugoslavia Serbian exporters, many organizations forced to reduce, close, or to compete in new markets restructuring. Although outdated, the best mailing list is available at this time.

In our study, companies has classified into six main sectors: business groups, IT and electronic sectors, traditional manufacturers, commerce, trade and services and agriculture. Distribution of our sample shown in Table 2 Traditional manufacturers make up a large part in our sample. This is consistent with the percentage of production among all Serbian companies, which is about 40%.

© 2011 Global Journals Inc. (US)

Table 2 : Sample distribution

Sector	Number	Percentage
Business Groups	45	12,6
IT and electronics	14	3,8
Traditional manufacturers	143	39,7
Commerce and trade	62	17,2
Service	78	21,7
Agriculture	15	4,2
Others	3	0,8
Total	**360**	**100%**

Table 3 shows the organizational position of respondents. It is not surprising given that almost two-thirds of the top executives or managers, because research sent to their address.

Table 3 : Position of respondents in IS unit

Position of respondents in IS unit	Number	Percentage
Top IS executive	101	64,3
IS department manager	27	17,2
Group leader	7	4,5
Systems analyst or programmer	10	6,4
Other	12	7,6
Total	**157**	**100**

Critical Issues

Round one: Addresses of 360 major Serbian organizations used to send in the first round of questionnaires IS managers. Managers were required to include five to ten questions that they thought it would be the most important period of three to five years in the future, and to state the reasons for their choice. One hundred and fifty-seven respondents provided the 784 questions, and about 5 statements per participant. Achieved a response rate of approximately 44% and therefore considered good.

Round two: the first round responses analyzed and suggested questions classified according to the scheme used by Niederman et al. (1991). All questions proposed at least five persons were involved, resulting in a list of 49 different issues (Table 4). The analysis performed independently by the author.

List of key issues in IS management Serbia was applied to the second round questionnaire. Space allows participants to add new concerns at that time. Since each respondent was asked to rate the following questions using a scale from one (unimportant) to 10 (most important) and to propose changes in the text. In the second round, questionnaires sent to IS managers from 360 organizations starting in February 2010. One hundred and seventy-eight respondents answered the rate of 49.5%.

© 2011 Global Journals Inc. (US)

Table 4 : Candidate issue list

No.	Issue
1.	The status and power of person in charge of IS departments in enterprises
2.	Organizational mechanism to manage the company IS department
3.	Internal managerial and organizational level of IS department
4.	The quality of input data
5.	Support and introduction of high-level IT managers (top management support)
6.	Support for mid-level managers
7.	The ability to use computers that do not belong to the staff IS department
8.	Technology competence of employees in the IS departments
9.	Application of advanced IT in enterprises
10.	Data Security
11.	Consistency of IT policy
12.	Assessing the effectiveness of information systems
13.	Inadequate understanding of IS managers and other users and their lack of involvement in the development of IS
14.	Education IS professionals (higher education of the head of MIS)
15.	Improving IS strategic planning
16.	Management information system function
17.	Organizational problems
18.	Education IS users (continuous training and education of staff MIS)
19.	Integration of subsystems into a comprehensive information architecture (system integration)
20.	Telecommunications infrastructure and its links with the world
21.	Executive IS
22.	National standards and ISO standards compliant IS
23.	Electronic Data Interchange (EDI) - electronic development strategy
24.	The use of integrated IS development methodology (methodology development)
25.	Using modern tools for the development of IS (Development tools)
26.	Choice of equipment
27.	The stability of national regulations
28.	Implementation of relational database
29.	Use of external databases
30.	Improving the productivity of IS development
31.	Evaluation and improvement of existing IS
32.	Legal protection
33.	Financial investments in IS
34.	Replacement of the mainframe to a PC and LAN
35.	Limited supply of quality products and services
36.	IS effectiveness and measurement
37.	IS cost control
38.	Establishing a national professional association for IS
39.	Development of an appropriate IT infrastructure
40.	Facilitating and managing business process redesign
41.	Development and management of distributed systems
42.	Improving the efficiency of software development
43.	Communication between the IS department and end users
44.	IS used for competitive advantage (competitive advantage)
45.	Improving information security and control
46.	Meeting the needs of users
47.	Planning and managing communication networks
48.	Optimizing the efficiency of the organization
49.	Recruiting and developing IS human resources (human resources / personnel MIS)

© 2011 Global Journals Inc. (US)

Round three: one hundred and fifty-eight organizations that have not responded to the first and second round questionnaires dropped from the study. The third round questionnaire sent in June of 2010 the remaining 202 participants. They again asked to evaluate problems and provide explanations for the low and high rates when their responses differed by three or more points (on a scale of ten points) in the second round group questionnaire. One hundred and thirty-nine Serbian IS managers responded, a rate of 68.8%.

Round four: a compilation of explanations for the discrepancies related to the fourth round of questionnaires, which sent to the remaining 202 participants in September 2010. They asked to read the reasons for disagreement and the exchange rate issue again. In this round 161 participants responded, a rate of 79.7%.

IV. Results

Critical management issues in information systems IS managers Serbian for the period 2009 to 2010 are shown in Table 5 The significance of all 10 questions was assessed with a score greater than seven, on a scale of ten points, so everything that is considered extremely important issues. In theory, the Delphi technique is gradually increasing consensus on key issues after several rounds of interviewing. The table below shows that consensus increased from the second to fourth rounds of interviewing. Standard deviation are increase from the second to the third round for only 1 out of 50 questions, and the third to the fourth round of the three different questions.

The ten most critical issues (after round four), which led the Serbian IS staff and what is expected to face over the next 5 years with their ranking and standard deviation are shown in Table 5, while the detailed analysis presented in Appendix A.

Table 5 : Key IS Management Issues in Serbia

Ranking	Mean	Standard Deviation	Issues*	Issue classification			
				M/T	P/C	I/E	Group
1.	8,40	2,86	IS cost control	M	C	I	BR
2.	8,09	2,93	Using modern tools for the development of IS (Development tools)	T	C	I	TI
3.	8,07	2,13	Management information system function	M	C	I	IE
4.	7,86	2,26	Improving IS strategic planning	M	P	E	BR
5.	7,83	2,64	Financial investments in IS	M	P	E	BR
6.	7,79	2,83	Education IS users (continuous training and education of staff MIS)	M	C	E	BR
7.	7,66	2,14	Organizational problems	M	C	E	BR
8.	7,63	2,37	Development of an appropriate IT infrastructure	T	C	I	TI
9.	7,36	2,93	Inadequate understanding of IS managers and other users and their lack of involvement in the development of IS	M	P	I	BR
10.	7,30	2,40	Education IS professionals (higher education of the head of MIS)	M	C	I	IE

* Issues classification (Niederman et al., 1991): M- management; T - technology; P - planning; C- control; I - internal to IS organization; E - external; Group: business relationship (BR); technology infrastructure (TI); internal effectiveness (IE); or technology application (TA);

a) Top ten issues

Each of the ten highest ranked key issues provides insight into the key issue and its relation to other matters. The most critical issues have proved to be a combination of technology management issues, strategic issues management, development of IT technology and training issues on computers of end users and managers. This shows the need to balance business, technical and human skills. Non-critical issues mainly related to the development of individual technologies must integrate to be able to provide the appropriate IT infrastructure.

i. *IS cost control*

Survey participants reported that IS cost control must be planned long-term costs because in many cases an obstacle to further development of information systems. They find that managers must have a more active role in planning and control of IS costs and the inadequate participation of users. This question is put in the first place because at the time of research the economic situation in Serbia is very unstable, while the political, social and economic changes in the subjects and therefore do not have much confidence in the IS cost control word present corruption in all spheres of society.

ii. *Using modern tools for the development of IS (Development tools)*

Most respondents believe that one of the most important questions the use of modern development tools that enable IS: improving the efficiency of software development (reducing the backlog by developing new methods and platforms), the selection and integration of

© 2011 Global Journals Inc. (US)

application software (which can reduce costs and increase productivity, but can lead to integration and maintenance problems), making efficient use of data resources (databases through appropriate technology and evaluate the data as a corporate asset), the management of existing legacy applications portfolio (which may affect the integration of new technologies and the transition to the new operational environment), development and management of distributed systems (where the client-server environment provides consistency of software problems and data, as well as challenges in project management), improving information security and control, planning and portfolio management applications and the planning and use of CASE technology (in order to reach a more efficient support the process of developing the system).

iii. *Management information system function*

Respondents suggest that the IS function should manage and organize as well as other business functions. This includes short-term planning, working in teams, motivating staff, project management, implementation methodology, quality control, planning, customer support, etc. Responses suggest that management education and practice, ARE professionals are not even close to the desired level.

iv. *Improving IS strategic planning*

The volunteers were told that the important information management tool and therefore must be identified and planned for the long term. It is necessary to improve the strategic planning of information systems. Several respondents believed that there was no general business associate for strategic planning and this situation identified with a lack of national long-term strategy. It should note that the economic situation in Serbia is very unstable at the time of research, and that political, social and economic changes are underway.

v. *Financial investments in IS*

Respondents suggested that Serbia is a country in which very little is invested in IS during the past decades. The average investment in IS are necessary to increase and define the levels of financial investment because the speed of adoption of IT in the world among industries such as retail, banking, e-commerce, telecommunications and e-Government accelerated in recent years.

vi. *Education IS users (continuous training and education of staff MIS)*

Respondents state that managers and other users need to be better understanding the role of information services. They need to make an informed decision on strategic goals and investment, to better determine the conditions, follow world trends and to make information technology more efficient. It believed that managers should also learn how to improve management practices because of the power of information technology. Most respondents believe that we need continuous training and education of staff MIS. A small number of respondents felt that users should be computer literate.

vii. *Organizational problems*

Most respondents stated that the appropriate organization structure, business process management, functions, and their stability are the essential foundation for the development of effective IS. Because the state of transition and instability this opinion is reflected as the historical neglect of issues such as organizational, information technology and management. They replied that the road and see it as something independently and in parallel with other business systems rather than as an integral part of them. Respondents suggest that critical business functions should properly positioned in the organizational structure.

viii. *Development of an appropriate IT infrastructure*

In developed countries, the construction of IT infrastructure is vital because of the changing needs of business organizations. IT infrastructure is an issue that is a combination of technological platform development, integration, custom, designed and packaged application software, as well as the rigidity of existing applications. Many leading IS organizations gradually realize that building an IT infrastructure that will support existing business applications is a key factor for long-term productivity of companies.

Respondents stated that building the appropriate IT infrastructure to: improve data integrity and quality assurance (to overcome inconsistencies between different sources of data and lack of control in the IS and user departments), the development and management of Electronic Data Interchange (to provide electronic communication with customers and suppliers), planning and integration of multi-vendor open systems technologies (in the face of a variety of operating environments and unstable conditions), the integration of data processing, office automation and telecommunications, data management and storage of documents, planning and management of networks, implementation and management of co-operation support systems (to help teams in sharing information and improve their efficiency) and the establishment of an effective Disaster Recovery options (in order to prevent risks and potential loss of business).

ix. *Inadequate understanding of IS managers and other users and their lack of involvement in the development of IS*

Subjects told that there is a general lack of understanding of relationship of strategic planning, control and growth companies. They find that managers play a more active role in planning and participation in the definition of user requirements is inadequate. Many people thought it was because of the lack of which relate to education and knowledge of IS users. One

© 2011 Global Journals Inc. (US)

participant explained that this gap has its roots in the previous economic system that ignores market competition and that it is necessary include IS users in their development.

x. *Education IS professionals (higher education of the head of MIS)*

The respondents were convinced that the future of IS as a discipline depends on the existence of highly skilled "professionals". They stressed the importance of universities and research institutions, and practices in the industry. While many participants were convinced that the most abundant of the seminar offered a very inefficient, few argued that there are opportunities for education, but are not enforced. A small number of respondents is of the opinion that it is not such a problem of inadequate education about IS professionals but lack of sophistication of IS users.

Non-critical issues

Matters that are rated and ranked ten least critical are shown in Table 6 From Table 6 shows that the difference of average values of the last ten issues are extremely small and amounts to 0.28 (between 40 to 49 questions). Five of the ten least critical issues related to nformation technologies, their implementation and consistency of its implementation (implementation of advanced IT in enterprises, use of external databases, data security, quality of input data, the consistency of IT policies), four related to human resources (internal managerial and organizational level of IS departments, support and introduction of high-level IT managers, support mid-level managers, status and power of person in charge of IS departments in companies) and one relating to the telecommunications infrastructure of Serbia and its links with the world. These results indicate that there is a problem of developing knowledge and understanding of IT in organizations.

Table 6 : The Ten Least

Ranking	Mean	Standard Deviation	Issues
40	**4,29**	2,36	Internal managerial and organizational level of IS department
41	**4,27**	2,42	Telecommunications infrastructure and its links with the world
42	**4,27**	2,37	Support and introduction of high-level IT managers (top management support)
43	**4,25**	2,44	Support for mid-level managers
44	**4,12**	2,46	Use of external databases
45	**4,22**	2,47	Application of advanced IT in enterprises
46	**4,09**	2,48	Data Security
47	**4,09**	2,80	The status and power of person in charge of IS departments in enterprises
48	**4,01**	2,48	Consistency of IT policy
49	**4,01**	2,57	The quality of input data

V. Comparison with Results Obtained in Other Countries

In order to compare the results obtained in Serbia with those of similar studies in the U.S. and other countries, the questions classified using the scheme Niederman et al. The classification scheme is give in Table 7. Significant differences can observed only if we make a comparison of all these studies as is done in Table 8 and show all the available key issues in different countries. It should noted that the displayed key IS management issues in different European and non-European countries, in different time intervals to determine at what level is a key issue in Serbia today are.

© 2011 Global Journals Inc. (US)

© 2011 Global Journals Inc. (US)

Table 7.: Key issues in Information Systems Management in other countries in different times

Rank	USA (1996) [a]	North America (2001) [b]	Slovenia (1996) [c]	Taiwan (1996) [d]	South Africa (2007) [e]	India (1992) [f]	Ireland (2001) [g]	Canada (2000) [i]	China (2005) [j]	Australia (2001) [k]	Hong Kong SAR (2004) [l]	Norway (2001) [m]
1.	Development of an appropriate IT infrastructure	Optimization of enterprise - wide IS Services	Inadequate understanding of IS managers and other users	Communication between the IS department and end users	Improving information security and control	Understanding / awareness of the contribution of MIS	IS effectiveness and measurement	Development of an appropriate IT infrastructure	Top management support	Organizing and using data	Harmonization of IS and corporate goals (goal alignment)	Alignment with organizations within the company
2.	Facilitating and managing business process redesign	Protecting and securing information systems	Education IS professionals	Top management support	Development of an appropriate IT infrastructure	Recruiting and developing IS human resources	Improving IS strategic planning	Improving IS project management in practice	Technology competence of employees in the IS departments	Optimization of enterprise - wide IS Services	Development of an appropriate IT infrastructure	IS used for competitive advantage (competitive advantage)
3.	Development and management of distributed systems	Harmonization of IS and corporate goals (goal alignment)	Improving IS strategic planning	Improving IS strategic planning	IT value management	The quality of input data	Service Delivery	Planning and managing communication networks	Internal managerial and organizational level of IS department	Connecting electronically with customers, suppliers and / or partners	Efficient use of data resources	Improving IS strategic planning
4.	Development and implementation of information architecture	Organizing and using data	Management information system function	IS used for competitive advantage (competitive advantage)	Service Delivery	Higher education of the head of MIS	Data Security	Improving the efficiency of software development	Support for mid-level managers	Harmonization of IS and corporate goals (goal alignment)	Improving IS strategic planning	Development and implementation of information architecture
5.	Planning and managing communication networks	Optimizing the efficiency of the organization	Organizational problems	Harmonization of IS and corporate goals (goal alignment)	Improving IS strategic planning	User friendliness of systems	Recruiting and developing IS human resources	Alignment with organizations within the company	Education IS users	Running cross-functional information systems	Improving the efficiency of software development	Development of an appropriate IT infrastructure
6.	Improving the efficiency of software development	Connecting electronically with customers, suppliers and / or partners	Education IS users	Computerization of routine work	Disaster recovery	Continuous training and education of staff MIS	Efficient use of data resources	Dealing with the degree and rate of technological change	Consistency of IT policy	Protecting and securing information systems	Improving information security and control	Recruiting and developing IS human resources
7.	Efficient use of data resources	Running cross-functional information systems	Integration of subsystems into a comprehensive information architecture	Development of an appropriate IT infrastructure	IS used for competitive advantage (competitive advantage)	Software Maintenance	Alignment with organizations within the company	Development and implementation of information architecture	Financial investments in IS	Optimizing the efficiency of the organization	Development and implementation of information architecture	Improving the efficiency of software development
8.	Recruiting and developing IS human resources	Implementation of business transformation initiatives	Telecommunications infrastructure and its links with the world	Integration of subsystems into a comprehensive information architecture	Alignment with organizations within the company	The standards in hardware and software	Organizational learning	IS used for competitive advantage (competitive advantage)	Assessing the effectiveness of information systems	Integrating systems to the Internet	Alignment with organizations within the company	IS effectiveness and measurement
9.	Alignment with organizations within the company	Updating obsolete systems	Executive IS	Improving the efficiency of software development	Efficient use of data resources	Data Security	Development of an appropriate IT infrastructure	Facilitating and managing business process redesign	Application of advanced IT in enterprises	Electronic development strategy	Planning and managing communication networks	Organizational learning
10.	Improving IS strategic planning	Integrating systems to the Internet	National standards and ISO standards compliant IS	User friendliness of systems	Development and implementation of information architecture	The availability of packaged software applications	IS used for competitive advantage (competitive advantage)	Development and management of distributed systems	Organizational mechanism to manage the company IS department	Implementation of business transformation initiatives	IS effectiveness and measurement	Efficient use of data resources

Issue name	Issue rank by year and country												
	Current issues	India	SAD	Slovenia	Taiwan	Canada	North America	Ireland	Australia	Norway	Hong Kong SAR	China	South Africa
	2011	1992	1996	1996	1996	2000	2001	2001	2001	2001	2004	2005	2007
	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank	Rank
IS cost control	1												
Using modern tools for the development of IS (Development tools)	2												
Management information system function	3			4									
Improving IS strategic planning	4		10	3	3			2		3	4		5
Financial investments in IS	5											7	
Education IS users (continuous training and education of staff MIS)	6	6		6								5	
Organizational problems	7			5									
Development of an appropriate IT infrastructure	8		1		7	1		9		5	2		2
Inadequate understanding of IS managers and other users and their lack of involvement in the development of IS	9			1									
Education IS professionals (higher education of the head of MIS)	10	4		2									
National standards and ISO standards compliant IS	11			10									
Improving information security and control	12										6		1
Implementation of relational database	13												
Meeting the needs of users	14												
Improving the efficiency of software development	15		6		9	4				7	5		
Choice of equipment	16												
Facilitating and managing business process redesign	17		2			9							
Development and management of distributed systems	18		3			10							
The use of integrated IS development methodology (methodology development)	19												
Legal protection	20												
IS used for competitive advantage (competitive advantage)	21				4	8		10		2			7
Communication between the IS department and end users	22				1								
Optimizing the efficiency of the organization	23						5		7				
Planning and managing communication networks	24		5			3					9		
Establishing a national professional association for IS	25												
The stability of national regulations	26												
IS effectiveness and measurement	27							1		8	10		
Recruiting and developing IS human resources (human resources / personnel MIS)	28	2	8					5		6			
Limited supply of quality products and services	29												
Electronic Data Interchange (EDI) - electronic development strategy	30								9				
Assessing the effectiveness of information systems	31											8	
Executive IS	32			9									
Integration of subsystems into a comprehensive information architecture (system integration)	33			7	8								
Organizational mechanism to manage the company IS department	34											10	
Replacement of the mainframe to a PC and LAN	35												
Technology competence of employees in the IS departments	36											2	
Improving the productivity of IS development	37												
The ability to use computers that do not belong to the staff IS department	38												
Evaluation and improvement of existing IS	39												
Internal managerial and organizational level of IS department	40											3	

© 2011 Global Journals Inc. (US)

© 2011 Global Journals Inc. (US)

NR: issues not ranked in previous studies in Serbia

Support and introduction of high-level IT managers (top management support)	41				2							1	
Telecommunications infrastructure and its links with the world	42			8									
Support for mid-level managers	43											4	
Application of advanced IT in enterprises	44											9	
Use of external databases	45												
Data Security	46	9						4					
The status and power of person in charge of IS departments in enterprises	47												
Consistency of IT policy	48											6	
The quality of input data	49	3											
Development and implementation of information architecture	NR		4			7				4	7		10
Efficient use of data resources	NR		7					6		10	3		9
Alignment with organizations within the company	NR		9			5		7		1	8		8
Optimization of enterprise - wide IS Services	NR						1		2				
Protecting and securing information systems	NR						2		6				
Harmonization of IS and corporate goals (goal alignment)	NR				5		3		4		1		
Organizing and using data	NR						4		1				
Connecting electronically with customers, suppliers and / or partners	NR						6		3				
Running cross-functional information systems	NR						7		5				
Implementation of business transformation initiatives	NR						8		10				
Updating obsolete systems	NR						9						
Integrating systems to the Internet	NR						10		8				
Computerization of routine work	NR				6								
The system of friendship	NR	5			10								
Understanding / awareness of the contribution of MIS	NR	1											
Software Maintenance	NR	7											
The standards in hardware and software	NR	8											
The availability of packaged software applications	NR	10											
Improving IS project management in practice	NR					2							
Dealing with the degree and rate of technological change	NR					6							
Service Delivery	NR							3					4
Organizational learning	NR							8		9			
IT value management	NR												3
Disaster Recovery	NR												6

[a] USA (1996): James C. Brancheau, Brian D. Janz and James C. Wetherbe
[b] North America (2001): CSC Index - 14th Annual Survey of IS Management Issues
[c] Slovenia (1996): Deklava S. and Zupancic J.
[d] Taiwan (1996): Yang, H. L.
[e] South Africa (2007): Johnston K., Muganda N. and Theys K.
[f] India (1992): Palvia P.C. and Palvia S.
[g] Ireland (2001): McDonagh et al.
[i] Canada (2000): Haynea & Pollard
[j] China (2005): G. Chen, R. Wu, and X. Guo
[k] Australia (2001): CSC Index - 14th Annual Survey of IS Management Issues
[l] Hong Kong SAR (2004): Louis C.K. Ma, Janice M. Burn and Eugenia M.W. Ng
[m] Norway (2001): Gottschalk P.

VI. Discussion and Implications

The results of this study are not surprising. Key issues in IS management in Serbia is in many ways different from other countries and the United States. These results are probably largely consistent with the other democracies of Eastern Europe, and especially the Balkans, which are at a similar stage of development.

IS cost control (# 1), the use of modern tools for the development of IS (# 2), IS management issues (# 3), financial investments in IS (# 5), organizational problems (# 7) and inadequate understanding of IS managers and other users and their lack of involvement in the development of IS (# 9) top the list, while the Serbian compared with other countries it does not belong to the key IS management issues except Slovenia, where the issue of management information systems ranked as the fourth issue of importance organizational problems were ranked Even as a fifth on the list as the first Slovenian issue is the question of inadequate understanding of IS managers and other users and their lack of involvement in the development of IS. The reason that the first three key issues to be ranked this way can be found in the fact that the Serbian economy was in collapse during the nineties, in 1993 recorded the second largest economy in the history of inflation (2.35 percent • 1023 (64% per day)) Serbia and introduced the general sanctions of the Security Council 1992nd The development of computer technology in Serbia is the last two decades was in decline and one of the reasons is that the U.S. imposed an embargo on the sale of computer technology in the former Yugoslavia. Many projects that require the use of modern tools for IS development are hampered by the lack of expertise and limited financial resources. The overlap of key issues with Slovenia can be found in the fact that she was an integral part of the former Yugoslavia, but it must be borne in mind that the research carried out in Slovenia in 1996 and is today Slovenia has made great economic growth and consequently the survey carried out today, it is certain that the key IS management issues differ greatly. Even a question on the Slovenian list of key issues among the non-critical issues listed on the Serbian and telecommunications infrastructure and its relationship with the world (# 41), while other issues are on the list of key issues in Serbia are just different ranks.

The issue of education of IS professionals (higher education leaders about MIS) (# 10) is on the list of key IS management issues in India as the fourth-ranked and Slovenia ranked second, while the education of IS users (continuous training and education of staff MIS) (# 6) overlaps with India and Slovenia as the sixth-ranked. However, five key issues in IS management have ranked India among the key issues in Serbia can be seen from Table 8 Studies in India have also done so far in 1992 we believe it is now the key IS management issues in India far more varied. The only question is information system's education emerges, as the fifth ranked China as the improvement of strategic planning ranked as the seventh, and other critical IS management issues in China are on the list of 49 questions received in Serbia can seen in Table 8 where research is carried out in 2005. The reason for this can found in the fact that more and more IT skills are becoming necessary for ordinary employees and training has become significant. Meanwhile, although the education system in China has produced a lot more IT professionals than ever before, IT training other staff remains relatively low and therefore this question is in fifth place. The issue of improving the strategic planning of IS (# 4) overlaps with research in other countries and it ranks as a 3-in Taiwan and Norway, four ranking in Ireland and Hong Kong, 5 ranks in North Africa, except in India, Canada, Australia and North America where it is not among the top ten key management issues in IS. Rapid changes of business environment, developing new technologies, IT training and human resource needs of developing and maintaining information systems requires technical director to focus on IS strategy alignment with its strategic business enterprise. Development of an appropriate IT infrastructure (# 8) is also an issue that is among the top ten key IS management issues in other countries and as a first in Canada (4 key issues in Canada are not ranked on the list of the Serbia - Table 8), second in North Africa and Hong Kong (6 key issues are not ranked in North Africa, 3 in Hong Kong - Table 8), fifth in Norway (4 key issues in Norway are not ranked on the list of the Serbia - Table 8), seventh in Taiwan-in (3 key issues are not ranked on the list in Serbia - Table 8). In India, North America, Australia, Slovenia and the issue is not among the top ten key management issues in IS. This question has traditionally been very important in most countries. An efficient IT infrastructure is still lacking in many organizations. In many companies, the infrastructure of various types of hardware, databases, mission-critical applications are varied and uncoordinated, have different operating system platforms, and integrate them into a highly productive network is a difficult task. Different computing needs, building massive networks, and harmonization of IS functions with business functions to make building a solid infrastructure of a complex problem.

Only a matter of optimizing the efficiency of the organization (# 5) considered a key in North America and Australia where they are located on the fifth and seventh in the key ARE management issues. The issue of e-Strategy is a key issue and is in ninth place in Australia while in Serbia on 30 places. Other key management issues in IS in North America and Australia were not ranked in the Serbian list of key issues, which shows that important issues depend on the level of economic development, culture and political life of a

© 2011 Global Journals Inc. (US)

country. This stems from the fact that some issues related to high-quality services that are abundant in North America and Australia are, of course, scarce in Serbia. The same is the case with the national IT infrastructure such as communications, supply products and external databases. Lack of managerial skills demonstrates the importance of key issues such as choice of product, productivity, and change and project management. In other words, some of the key management issues Serbian IS reflect the past neglect. One consequence is a lack of knowledge and skills, because of limited education. Research in the United States, which was conducted in 1996 shows that there are two key IS management issues that are among the top ten key issues in Serbia and to improve strategic planning as the tenth issue of the construction of appropriate IT infrastructure ranked as the first question but also on the other hand there are three issues that are not ranked and is not on the Serbian list of key issues and are located in the U.S. can be seen in Table 8.

The list of key management issues Serbian IS missing issues such as development and implementation of information architecture, optimization of enterprise-wide IS services, protection and security of information systems, harmonization of IS and corporate goals (goal alignment), organizing and using information, electronically connecting with customers , suppliers and / or partners, launch cross-functional information system, implementation of business transformation initiatives, updating obsolete systems and so on. Understand key issues in IS management in Serbia should help the Serbian and other Eastern European and Balkan leaders on what needs to focus and direct their attention. Domestic producers of IS technologies and services can benefit, as research shows the necessity of these products and services.

VII. Conclusion

This study represents the first research on key issues of IS management in Serbia. We investigated the key issues in IS management based on data collected from 360 Serbian companies. We got the ranking key IS management issues in Serbia and compare them with results of previous studies in other countries. Key issues in IS management Serbia differ from those in the U.S. and other countries. Our analysis suggests that three key issues in Serbia are not in most cases the top three issues in other countries, mainly due to centralized decision-making mechanism, management style, and less experience with IT / IS applications.

These findings are likely to large overlap with other Eastern European democracies, especially in Macedonia, Montenegro, Albania, Croatia, at a similar stage of development. It is also evident that there are interesting differences between the perceptions of key IS management issues, and lower level management. Understanding these questions may provide more Serbian executive directors, as well as guidance on current and long-term goals of business practice. The importance of this study can significantly improved by increasing the motivation of participants and adoption of Delphi method. Though the nature of the research studies generally, this study represents the first step toward determining the critical issues in Serbia and IS management team issues.

There are several limitations to this study. First, this study uses the Delphi research method. The advantage of the Delphi method to get a list of questions companies through several rounds of research administration. This method requires entities wishing to participate in the study. This condition cannot exist in the current study. There is a lack of motivation to participate in the study. Many participants do not want to participate in the second or three round of research. Another limitation is that the results apply to randomly selected companies. About 72% of respondents were from large companies. This example may not be a representative sample of the population.

A third limitation is that the importance of the business environment should be determined by the situation with which the individual, i.e. executives face, not to determine the statistical average (Niederman, Brancheau and Wetherbe, 1991). Therefore, the interpretation of these results needs to be careful. The data suggest that IS managers around the world, have to pay more attention to software development and application of IT technologies. In addition, developing countries should pay attention to the development of telecommunications infrastructure. Collecting and analyzing data on key IS management issues in different regions and their comparison we concluded that the key management issues priority IS vary with the level of economic and economic development of countries.

References Referencias

1. Angus, J. (1990), "Japanese Decade Give Way to European Decade of `90`s", Computerworld, 24(40), pp.25.
2. Armstrong, T., Chamberlain, G., Moore, B., Hart, M. (2002), "Key information systems management issues for CEOs and other executives in South Africa", Unpublished Empirical Research Reports, Department of information systems, University of Cape Town.
3. Badri, M.A. (1992), "Critical Issues in Information Systems Management: An International Perspective", International Journal of Information Management, 12, pp.179-191.
4. Ball, L. and Harris, R. (1982), SMIS Members: a Membership Analysis, MIS Quarterly, 6(1), pp.19-38.
5. Berkowitz, S., Ryan, J., Waspe, K., Hart, M. (2001), "Key information systems management issues", Unpublished Empirical Research Reports,

© 2011 Global Journals Inc. (US)

Department of information systems, University of Cape Town.
6. Brancheau, J. C., Janz, B. D. and Wetherbe, J. C. (1996), "Key Issues in Information Systems Management: 1994-1995 SIM Delphi Results", MIS Quarterly, 20(2), pp. 225-242.
7. Brancheau, J. C. and Wetherbe, J. C. (1987), "Key Issues in Information Systems Management", MIS Quarterly, 11(1), pp.23-45.
8. Burn, J., Saxena, K. B. C., Ma, L. and Cheung, H. K. (1993), "Critical Issues of IS Management in Hong Kong: a Cultural Comparison", Journal of Global Information Management, 1(4), pp. 28-37.
9. Burn, J.M., C. Szeto, C. (1998), "Information systems management issues in Hong Kong: a contingency analysis and comparison with the UK", Journal of Global Information Technology Management, 1(1), pp. 5-16.
10. Caudle, S. L., Gorr, W. L. and Newcomer, K. E. (1991), "Key Information System Management Issues for the Public Sector" MIS Quarterly, pp. 171-188.
11. Clark, T.D., Jr.(1992), "Corporate Systems Management: An Overview and Research Perspective", Communications of the ACM, 35, pp.61-75.
12. Chou, H.W. and Jou, S.B. (1999), "MIS Key Issues in Taiwan's Enterprises", International Journal of Information Management, 19(5), pp. 368-387.
13. CSC (2002), 2001 Critical Issues of Information Systems Management (14th Annual Survey of IS Management Issues). http://www.csc.com.
14. Davenport, T. and Buday, R. (1988), "Critical Issues in Information Systems Management in 1988", Index Group.
15. Davis, J.G., Menon, R., Munday, S.R., Thomson, B.C. and Young, L.W. (1995), "Key Issues in eInformation Systems Management: A New Zealand Perspective", Proceedings of the PRHSM'95 International Conference, Maui, Hawaii, January 2-3, pp. 187-195.
16. Dickson, G.W., Leitheiser, R.L., Wetherbe, J.C. and Nechis, M. (1984), "Key Information Systems Issues for the 1980's", MIS Quarterly, 8, pp. 135-159.
17. Doukidis, G.I., Smithson, S. and Naoum, G. (1992), "Information Systems Management Issues in Greece: Issues and Perceptions", Journal of Strategic Information Systems, 1, pp. 63-75.
18. Deans, P. C., Karwan, K. R., Goslar, M. D., Ricks, D. A. and Toyne, B. (1991), "Identification of Key International Information Systems Issues in U.S.-Based Multinational Corporations", Journal of Management Information Systems, 7(4), pp. 27-50.
19. Dekleva, S. and Zupancic, J. (1996), "Key Issues in Information Systems Management: a Delphi Study in Slovenia", Information & Management, 31(1), pp. 1-11.
20. Dexter, A.S. Janson, M.A., Kiudorf, E. and Jüri Laast-Laas (1993), "Key information technology issues in Estonia", The Journal of Strategic Information Systems", 2(2), pp. 139-152.
21. Doke, E.R. and Swanson N.E. (1995), "Decision variables for selecting prototyping in information systems development: A Delphi study of MIS managers", Information & Management, 29(4), pp. 173-182.
22. Dutta, S. , Lopez-Carlos, A., Mia, I. (2006), Global information technology report 2005-2006 executive summary http://www.wetorum.org/pdf/Global_Competitiveness_Reports/Reports/gitr_2006/summary.pdf
23. Dyson, E. (1993), "How Eastern Europe is starting over", Datamation, 39(5), pp. 67-70.
24. De Haan, J. and Peters, R. (1993),"Technology: toys or tools? Results of a Dutch Delphi study", Information & Management, 25(6), pp. 283-289.
25. Galliers, R.D., Merali, Y. and Spearing, L. (1994), "Coping with Information Technology? How British Executives Perceive the Key Information Systems Management Issues in the Mid-1990s", Journal of Information Technology, 9, pp. 223-238.
26. Gottschalk, P. (2000), "Studies of Key Issues in IS Management around the World", International Journal of Information Management, 20(3), pp. 169-180.
27. Harrison, W. L. and Farn, C. K. (1990), "A Comparison of Information Management Issues in the United States of America and the Republic of China", Information & Management, 18(4), pp. 177-188.
28. Hartog, C. and Herbert, M.(1986), "1985 Opinion Survey of MIS Managers: Key Issues", MIS Quarterly, 10(4), pp. 351-361.
29. Haynea, S. C. and Pollard, C. E., (2000), "A Comparative Analysis of Critical Issues Facing Canadian Information Systems Personnel", Information & Management, 38(2), pp. 73-86.
30. Hotopf, M. (1992),"The East hungers for megabytes", International Management, 47(2), pp.48-49.
31. Kemfer, L. (1993), "Winds of Change", Computer-aided Engineering, 12(2), pp. 82.
32. Keizer, G. (2004), Survey: CIO's Say Security is a Top Priority http:// www.secirity pipeline.com
33. Kim, Y.G. and Sato, O. (1995), "Key Issues in Information Systems Management: A Japanese Perspective", Proceedings of the PRIISM'95 International Conference, Maui, Hawaii, January 2-3, pp. 167-174.
34. Kremar, H.O.A. (1990), "Information's management - zum problem - bewusstein deutscher DV -leiter", Wirtschaftsinformatik, 32(2), pp. 127-135.
35. Leskovar, R. & Zupancic (1991), "An analysis of key issues in information system development", in

© 2011 Global Journals Inc. (US)

Ceric,V., Luzar, V., Dobric, V., Ray, P. (Ed) Proceedings of the 13th International Conference, June 10-13, pp. 3-8.
36. Li, D., Huang, W.W., J. Luftman and W. Sha (2010),"Key Issues in Information Systems Management: An Empirical Investigation from a Developing Country's Perspective", Journal of Global Information Management, 18(4), pp. 19-35.
37. Luftman, J. (2005), "Key Issues for IT Executives 2004", MIS Quarterly Executive, 4(2).
38. Luftman, J., Kempaiah R., and Rigoni, E. (2009), "Key Issues for IT Executives 2008", MIS Quarterly Executive, 8(3).
39. Martin, E.W. (1982), "Critical Success factors of Key MIS/DP Executives", MIS Quarterly, 6, pp.1-9.
40. Mata, F. J. and Fuerst, W. L. (1997), "IS Management Issues in Central America a Multinational and Comparative Study", Journal of Strategic Information Systems, 6(3), pp. 173-202.
41. Moeller, G.E.W. (1991), "Europe: an expanding market for information technology", World of Banking, 10(3), pp. 30-31.
42. Moores, T. (1996), "Key Issues in the Management of Information Systems: a Hong Kong Perspective", Information & Management, 30(6), pp. 301-307.
43. Moynihan, T. (1990), "What Chief Executives and Senior Managers Want from Their IT Departments," MIS Quarterly, 14(1), pp. 15-25.
44. Niederman, F., Brancheau, J. C. and Wetherbe, J. C. (1991), "Information Systems Management Issues for the 1990s", MIS Quarterly, 15(4), pp. 475-500.
45. Palvia, P. C. and Palvia, S. C. J. (1992), "MIS Issues in India and a Comparison with the United States", International Information Systems, 1(2), pp. 100-110.
46. Palvia, P.C., Palvia, S.C, J., „ Whitworth, J.E. (2002), "Global information technology: a meta-analysis of key issues", Information & Management, 39(5), pp. 403-414.
47. Parker, T., Idundum, M. (1988), "Managing information systems in 1987: the top issues for managers in the UK", Journal of information technology, 3, pp. 34-42.
48. Pimchangthong, D., Plaisent, M. and Bernard, P. (2003), "Key Issues in Information Systems Management: a Comparative Study of Academics and Practioners in Thailand", Journal of Global Information Technology Management, 6(4), pp. 27-44.
49. Pervan, G.P. (1993), "Results from a Study of Key Issues in Australian IS Management",Proceedings of the fourth Australian Conference on Information Systems, Brisbane, Queensland, September 28-30, pp. 113-128.
50. Pervan, G.P. (1994), "Information Systems Management: An Australian View of the Key Issues", Australian Journal of Information Systems, 1, pp. 32-44.
51. Rao, K.V., Huff, P.P. and Davis, G.B. (1987), "Critical Issues in the Management of Information Systems: A Comparison of Singapore and the USA", Journal of Information Technology, 1, pp.11-19.
52. Saunier, F., Pepper, J., Yacco, W., and Brody, A (1993),"Brave new world", Marketing Computers, 13(2), pp. 18-26.
53. Scala, S. and McGrath R.Jr. (1993), "Advantages and disadvantages of electronic data interchange-an industry perspective", Information & Management, 25(2), pp. 85-91.
54. Shan, W. (2001), "the IT work force in China," Communications of the ACM, 44(7), pp.76.
55. Shi, Y., Chen, G. Q. and Jiang, Z. (2000), "Critical Factor in IS Application of Enterprises", Chinese Journal of Management Science, 3.
56. Wang, P. and Turban, E. (1994), "Management Information Systems Issues of the 1990s in the Republic of China: An Industry Analysis", International Journal of Information Management, 14, pp. 25-38.
57. Watson, R. T. (1989), "Key Issues in Information System Management: an Australian Perspective", Australian Computer Journal, 21(3), pp. 118-129.
58. Watson, R. T. and Brancheau, J. C. (1991), "Key Issues in Information Systems Management: an International Perspective", Information & Management, 20(3), pp. 213-223.
59. Watson, R. T., Kelly, G. G., Galliers, R. D. and Brancheau, J. C. (1997), "Key Issues in Information Systems Management: an International Perspective" , Journal of Management Information Systems, 13(4), pp. 91-115.
60. Wrycza S., Plata-Przechlevski T. (1994), "Key Issues in Information systems management: the case of Poland", In Proceedings of the Fourth International Conference on Information Systems Development, J.Zupancic, and S. Wrycza (eds.), Bled, Slovenia, pp. 289-296.
61. Yang, H. L. (1996), "Key Information Management Issues in Taiwan and the US", Information & Management, 30(5), pp. 251-267.

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Verification of Lost Data Packets and Regularizing Packets Transmission

By N Vinutha, G Varalakshmi
Aurora's Technological and Research Institute

Abstract - Security in the network remains a major challenge which is highly susceptible to maliciousness. The routers especially are a major threat to the network. They can be malicious enough to disrupt the transmission of the data in the form of packets. In this paper, along with the detection of a malicious router, the transmission of packets is regularized to maximum extent possible. A Conditional Packet Buffering (CPB) algorithm is used to increase the through put of the router.

Keywords : *Distributed systems, Data packets, malicious router, and Packet regularization.*

GJCST Classification : *C.2.1*

Strictly as per the compliance and regulations of:

© 2011l . N Vinutha, G Varalakshmi. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Verification of Lost Data Packets and Regularizing Packets Transmission

N Vinutha [α], G Varalakshmi [Ω]

Abstract - **Security in the network remains a major challenge which is highly susceptible to maliciousness. The routers especially are a major threat to the network. They can be malicious enough to disrupt the transmission of the data in the form of packets. In this paper, along with the detection of a malicious router, the transmission of packets is regularized to maximum extent possible. A Conditional Packet Buffering (CPB) algorithm is used to increase the through put of the router.**

Keywords : Distributed systems, Data packets, malicious router, and Packet regularization.

I. Introduction

A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. The routers play a major role to achieve this goal.

The router is a primary component in the infrastructure of today's Internet. Routing messages in a network is an essential component of Internet communication, as each packet in the Internet must be passed quickly through each network (or autonomous system) that it must traverse to go from its source to its destination. Network routers occupy a unique role in modern distributed systems. They are responsible for cooperatively shuttling packets amongst themselves in order to provide the illusion of a network with universal point-to-point connectivity. Although, a great deal of attention has been paid to securing network communication.

To a first approximation, networks can be modelled as a series of point-to point links connecting pairs of routers to form a directed graph. Since few endpoints are directly connected, data must be forwarded hop-by-hop from router to router, toward its ultimate destination. Therefore, if a router is compromised, it stands to reason that an attacker may drop, delay, reorder, corrupt, modify, or divert any of the packets passing through. Thus network routing is vulnerable to disruptions caused by malfunctioning or malicious routers that draw traffic towards them but fail to correctly forward the traffic. In this paper, two queues are maintained to hold the packets – one which holds the regular packets sent by the previous router and the other to hold the packets that may have been maliciously dropped by the router or due to time out. This ensures that maximum packets are sent to the destination in a scenario where the router turns out to be malicious.

The protocol used in the network is Transmission control Protocol. The TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major Internet applications such as the email, remote administration, file transfer and World Wide Web rely on.

The reminder of this paper is organized as follows. In section II, I put my ideas within the context of prior and ongoing research related to malicious router detection. In section III, discuss the technique in regularization of the packets and shows the comparison of an existing solution and the proposed solution in which the increase in the throughput of the router is highlighted. In section IV the results achieved are put in the form of a graph. The conclusion is presented in section V.

II. Related Work

Based on my literature survey I have analyzed that attempt was only made to detect the packet loss. There is no attempt to regularize the packet loss. In this paper the packet loss is minimized by transmitting them in case they are dropped maliciously or due to time out.

In an earlier work [1], a compromised router detection protocol (X) is developed that dynamically infers the precise number of congestive packet losses that will occur. Once the congestion ambiguity is removed, subsequent packet losses can be safely attributed to malicious actions.

In [2], a protocol was developed that detects and reacts to routers that drop or misroute packets. The protocol WATCHERS is based on the principle of conservation of flow in a network: all data bytes sent into a node, and not destined for that node, are expected to exit the node. WATCHERS track this flow, and detect routers that violate the conservation principle. The WATCHERS has several advantages over existing network monitoring techniques. The WATCHERS protocol impact on router performance and WATCHERS' memory requirements are reasonable for many environments. However, the WATCHERS protocol had many limitations in both its traffic validation mechanism and in its control protocol.

Author α: M.Tech (CSE) Aurora's Technological and Research Institute, Hyderabad, India. E-mail : Vinnu.ncs@gmail.com
Author Ω: Associate Professor, ATRI, Uppal, Hyderabad, AP. Email : varacse@gmail.com

© 2011 Global Journals Inc. (US)

The problem of detecting routers [3] [4] [5] with incorrect packet forwarding behaviour and the design space of protocols that implement such a detector is explored. A protocol that is likely inexpensive enough for practical implementation at scale is presented. A prototype system called Fatih that implements this approach on a PC router is explained.

The algorithms [6] that form the basis of the protocols such as OSPF, RIP, and IEGP are not secure, however, and have even been compromised by routers that did not follow the respective protocols correctly.

Robust routing requires [7] [8] not only a secure routing protocol but also well-behaved packet forwarding. To this end, the paper proposes an approach to robust routing in which routers, assisted by end hosts, adaptively detect poorly performing routes that appear suspicious, and use a secure trace route protocol to attempt to detect an offending router. This approach complements efforts that focus on securing the routing protocol itself. The secure trace route is a general technique with wide applicability, and is presently investigating it in the context of multi-hop wireless networks.

The paper [9] considers the impact of systemic noncongestion related packet loss on the effectiveness, fairness, and efficiency of parallel TCP transmissions. The results indicate that parallel connections are effective at increasing aggregate throughput, and increase the overall efficiency of the network bottleneck. In the presence of congestion related losses, parallel flows steal bandwidth from other single Stream flows. A simple modification is presented that reduces the fairness problems when congestion is present, but retains effectiveness and efficiency.

RED gateways [10] [11] keep the average queue size low while allowing occasional bursts of packets in the queue. During congestion, the probability that the gateway notifies a particular connection to reduce its window is roughly proportional to that connection's share of the bandwidth through the gateway. RED gateways are designed to accompany a transport-layer congestion control protocol such as TCP. The RED gateway has no bias against busty traffic and avoids the global synchronization of many connections decreasing their window at the same time. Simulations of a TCP/IP network are used to illustrate the performance of RED gateways.

Random Exponential Marking [12] [13], aims to achieve both high utilization and negligible loss and delay in a simple and scalable manner. The key idea is to decouple congestion measure from performance measure such as loss, queue length, or delay. While congestion measure indicates excess demand for bandwidth and must track the number of users, performance measure should be stabilized around their targets independent of the number of users.

All the above related work only presents the detection of malicious router and provides an alternate method to avoid malicious router. This paper goes an extra step to detect the malicious router and also regularize the packet losses so that the confidence in the packet transmission is maintained. This helps in critical applications being implemented, especially those applications that require data integrity.

III. Regularization of Packets

In a network, the packets are sent from a source router to destination router through the intermediate routers. A routing table exists for every router. The routing table maintains the source, destination and route of the packets in the network. It is frequently updated with the latest information.

In the proposed system, the router works in three modes - Mode 1, Mode 2, and Mode 3. The router can work in any one of the three modes individually by setting the router properties. These properties are set manually. When a router property is set to Mode 1, there is no differentiation of the packet loss. It may be due to overflow or may be due to maliciousness of the router.

In mode 2, based on the traffic parameters such as router buffer load (inflow), router buffer capacity, network bandwidth, queue size etc, a dynamic threshold is set. This threshold is used to remove the ambiguity between the packet loss due to congestion and router maliciousness. Also, a single queue is used to maintain the packets at the router.

In mode 3, along with the differentiation of the packet loss due to congestion and router maliciousness, the packets are also regularized. Unlike the mode 2, there are two queues maintained at each of the router–Accepted Queue (AQ) and Rejected Queue (RQ).

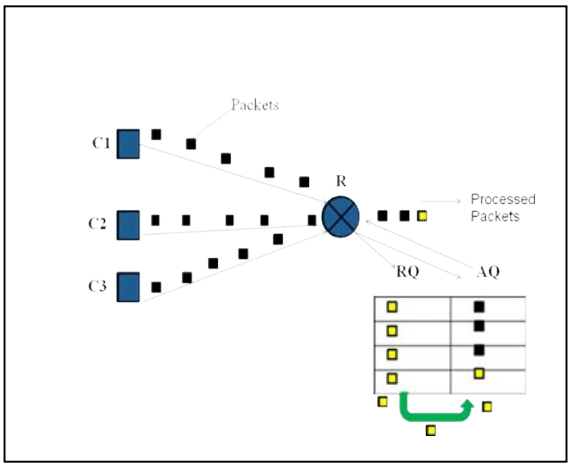


Figure 1 : Router working on mode 3

In the above figure 1 where the router works on mode 3, C1, C2, C3 are the client which sends packets

© 2011 Global Journals Inc. (US)

(P) to the router (R). Two queues, AQ – Accept Queue and RQ – Reject Queue are maintained at each router. Based on the below algorithm – Conditional Packet Buffering (CPB) - at the router, the packets are sent to either the AQ or RQ. A packet consists of attributes like the packet id, source and destination address, packet lifetime etc. The router Consider the packet's life time from its attributes and performs the below algorithm as follows

a) Conditional Packet Buffering (CPB) Algorithm

Sum (Packet Process Time and Current Waiting Time) > Packet Lifetime = RQ

Sum (Packet Process Time and Current Waiting Time) < Packet Lifetime = AQ

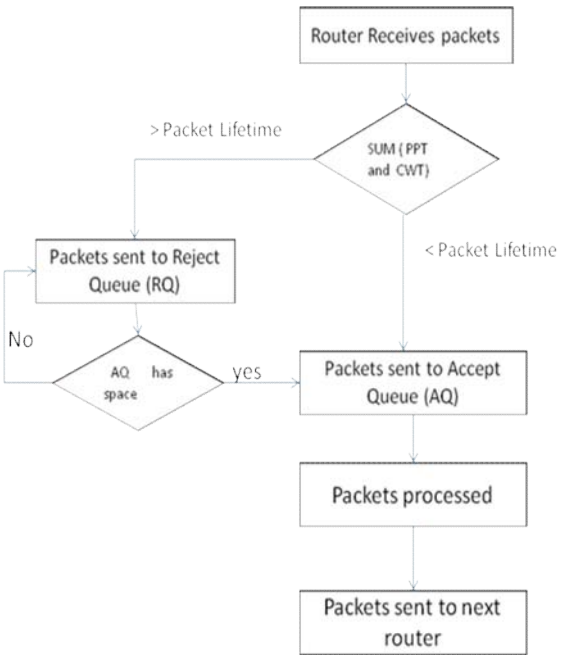


Figure 2 : Flow chart for CPB Algorithm

The router takes the current waiting time and the packet process time of the packets which are in the buffer and does the summation of the packet process time and current waiting time. If the summed up value is greater than the packet's life time then the router send the packet to the Reject Queue (RQ). If the summed up value is less than the packet's life time then the router send the packet to the Accept Queue (AQ). If at any time, the AQ is either empty or has place to accommodate a packets to process, the router takes the packets from RQ which has less lifetime and sends it to the AQ where the packets are processed and sends them towards the destination.

Table I : Comparission With Existing Solution

Status	Mode 1	Mode 2	Mode 3
Total packets sent to router	1000	1000	1000
Total packets processed(throughput)	608	629	680
Total packets dropped	392	43	51
Total Packets maliciously dropped	0	328	269

The above table which gives information that existing solution which is represented in mode 1 and mode 2 and the proposed solution in mode 3 in which the total packets processed are more i.e., throughput is increased.

IV. Performance Analysis

In existing solution the ambiguity between the packet loss due to congestion and maliciousness of the router is determined in which the throughput of the router is less. In the proposed solution along with the differentiation of the packet loss due to congestion and maliciousness of the router, the packets are regularized where the throughput is increased compared to the existing solution. The benchmark results after executing the algorithm in the three different modes shows the increase in the throughput of the router packet processing. From below graph I can conclude that mode 3 has high throughput than mode 1 and mode 2.

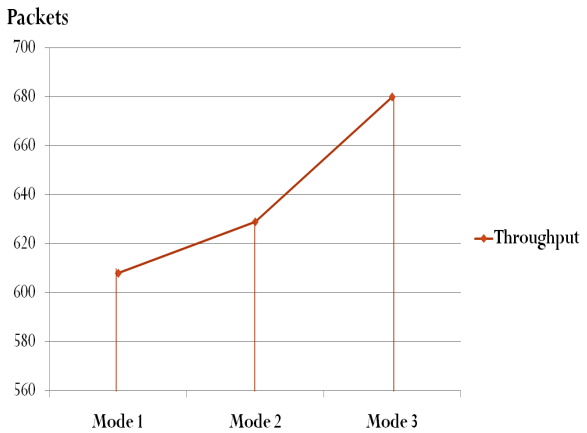


Figure 3 : Throughput increase at the router in three different modes Mode 1, Mode 2 – Existing Solution and Mode 3 – Proposed Solution

V. Conclusion

This paper makes an attempt to propose a solution to increase the throughput of the routers in the network by taking into consideration the packets that may have been dropped due to congestion or maliciousness of the router. The packet loss is thus minimized by regularizing.

© 2011 Global Journals Inc. (US)

Acknowledgment

I would like to thank Sr.Asst.Prof G. Varalakshmi, Sr. Asst.Prof A. Poongodai and Prof D. Sujatha (Aurora's Technological and Research Institute, Hyderabad, India) for their careful reading and valuable suggestions. I would also like to thank the anonymous referees for their helpful comments and suggestions to improve this work.

References References Referencias

1. Alper T. M Zrak, Student Member, IEEE, Stefan Savage, Member, IEEE, and. Keith Marzullo, Member, "Detecting Malicious Packet Losses" IEEE-26 Feb 2009.
2. K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson,"Detecting Disruptive Routers: A Distributed Network Monitoring Approach," Proc. IEEE Symp. Security and Privacy (S&P '98), pp. 115-124, May 1998.
3. A.T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, "Detecting and Isolating Malicious Routers," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 3, pp. 230-244, July-Sept. 2006.
4. S. Cheung and K. Levitt, "Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection," Proc. New Security Paradigms Workshop, 1997.
5. D. Taylor, "Using a Compromised Router to Capture Network Traffic," unpublished technical report, July 2002, http://www.netsys.com/library/papers/GRE_sniffing.PDF.
6. M.T.Goodrich, "Efficientand and Secure Network Routing Algorithms", Jan. 2001.
7. V.N. Padmanabhan and D. Simon, "Secure Trace route to Detect Faulty or Malicious Routing," SIGCOMM Computer Comm. Rev., vol. 33, no. 1, pp. 77-82, 2003.
8. S. Kent and R. Atkinson. "Security Architecture for the Internet Protocol", RFC 2401, November 1998
9. T.J. Hacker, B.D. Noble, and B.D. Athey, "The Effects of Systemic Packet Loss on Aggregate TCP Flows," Proc. ACM/IEEE Conf. Supercomputing (SC '02), pp. 1-15, 2002.
10. S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," IEEE/ACM Trans. Networking (TON '93), vol. 1, no. 4, pp. 397-413, 1993.
11. K. Bala. I. Cidon. and K. Sohraby. "Congestion control for high speed packet switched networks," in Proc. INFOCOM '90. pp. 52CL526, 1990.
12. S. Athuraliya, S. Low, V. Li, and Q. Yin, "REM: Active Queue Management," IEEE Network, vol. 15, no. 3, pp. 48-53, 2001.
13. S. Athuraliya and S. H. Low," Optimization Flow Control, II: Implementation.Submitted for publication, http:// netlab.caltech.edu, May 2000.
.

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Efficient HMAC Based Message Authentication System for Mobile Environment

By Kavitha Boppudi
Aurora's Technological and Research Institute

Abstract - Computationally constrained environments like Rfid, sensors and hand held devices require noncontact automatic identification technology. The wireless communication channel of these systems is vulnerable to various malicious attacks and has limited calculation resources and small storage capacity, aimed at these problems, a HMAC-based lightweight authentication protocol has been proposed. The main aim of the proposed protocol is that the calculation capacity and storage space of reader should be utilized efficiently, and the demand for the capacity of calculation and storage of device should be reduced. The analysis of security and performance show that the new protocol can resist some malicious attacks, such as spoofing attack, replay attack, tracking, etc., and is suitable for low-cost and computationally constrained system.

Keywords : *Secured Communication, MAC, HMAC, Stream ciphers, Signcryption Challenge response, Digital –Signatures.*

GJCST Classification : *D.4.6, K.6.5*

Strictly as per the compliance and regulations of:

© 2011l . Kavitha Boppudi. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Efficient HMAC Based Message Authentication System for Mobile Environment

Kavitha Boppudi

Abstract - Computationally constrained environments like Rfid, sensors and hand held devices require noncontact automatic identification technology. The wireless communication channel of these systems is vulnerable to various malicious attacks and has limited calculation resources and small storage capacity, aimed at these problems, a HMAC-based lightweight authentication protocol has been proposed. The main aim of the proposed protocol is that the calculation capacity and storage space of reader should be utilized efficiently, and the demand for the capacity of calculation and storage of device should be reduced. The analysis of security and performance show that the new protocol can resist some malicious attacks, such as spoofing attack, replay attack, tracking, etc., and is suitable for low-cost and computationally constrained system.

Index Terms : *Secured Communication, MAC, HMAC, Stream ciphers, Signcryption Challenge response, Digital–Signatures.*

I. Introduction

Security and authentication features were rudimentary in the original analog cellular phones. Authentication and security in cellular phones are important, and there is existing and ongoing work both in the United States and Europe. Secured communication means when the two parties are participating in the communication the messages should be authorized and visible to only two parties. When message are transferring between two parties the security place very important role. The authentication, snooping attacks and replay prevention are essential in secured communications. When we are checking for the message integrity the receiver able to identify the message is getting from valid resource and is that message is not modified. For the above concerns we have symmetric and asymmetric cryptographic schemes. Here when we dealing with constrained environment like hand held devices have limited resource and capacity is small, but these application wants support Authentication and Integrity.

MAC (M, K) is the technique to transfer the message M and a secret key K with the verifier .The verifier gets the cipher along with the message and key. The receiver again encrypts the message and compare with received cipher text HMAC is the one which is the implementation of MAC .The hash function is used to generate the digit .Hash function H ( ) is a one-way function which take variable length message, M as input and produce a fixed length output value, h=H (M).The digit is alphanumeric and it should be fixed length. It is varies from one message to one message. The HMAC is the best technique in cryptographic.

We have so many encryption/decryption methods. Like block cipher, CBC, Stream cipher. When we referring the previous papers the researchers saying that stream cipher is more essential that the block cipher. The block cipher not suitable when we are dealing with long message. The long message takes much time to generate cipher text. A stream cipher is a symmetric encryption technique i.e. shares the same secret key between sender and receiver. The RC4 cipher and one time pad are also stream ciphers. In stream cipher the Initial vector (IV) is encrypted to get output block which is the key, this output block encrypted to get another output block .The sequence of these output blocks are called key streams .These key streams are XOR with plaintext to get cipher text.

Challenge response approach gives the lesser performance in wireless communication when we compare to wired communication because it requires the overhead of handshake before any message shared between sender and receiver. But we want to achieve the better authentication .i.e. identifying the attacker we must use the technique challenge response.

The signcryption is a public-key primitive that performs functions of both digital signatures and encryption. The encryption and digital signatures are basic fundamental tools can guarantee the confidentiality, integrity and non-repudiation .In previous researcher papers many signcryption schemas to achieve the all security issues .The signatures schemes prevents the repudiation because any one can verify a signature using only the senders public key. When we want to authenticate the parties we can achieve by using the best technique signcryption.

The organization of this paper is given as fallows. In section II, provide an overview of cryptograph mechanisms and how the HMAC is extensively using to full fill the security applications. In section III, discussed some security issues rectified using by the appropriate security mechanism. In section IV, shows the work flow of HMAC algorithm, while in section V, discussed how signcryption works between two users to provide authentication. In section VI, how much security is

Author : *M.Tech (CSE) Aurora's Technological and Research Institute, Hyderabad, India. E-mail : boppudikavitha@gmail.com*

© 2011 Global Journals Inc. (US)

improved by using HMAC based protocol. Conclusion in section VII.

II. Related Work

Now days the security place very important role in all the communication systems. The wireless communication system has to support the security mechanisms because the ubiquitous nature of the wireless communication system susceptible to security attacks. The encryption and decryption are done in two ways i.e. Symmetric and asymmetric schemas As the previous research papers gave the some of the efficient algorithms for encryption are DES, AES [8] .Some suggested papers AES is the best algorithm when we compare with DES because the size key in DES support on 56-bit key, but AES can support any length of key and it can be implemented in Hardware and software. Most of AES calculations done at finite state. The AES giving the better performance than DES [6] in the constrained environment.

In paper [6] the three security techniques show the different behavior. The constrained environment uses the steam cipher for the encryption for this the data should be in binary form. This paper attempts to declare which mechanism is suitable for the constrained environment. They concluded AES giving the better performance because it can implement in software not only in hardware.

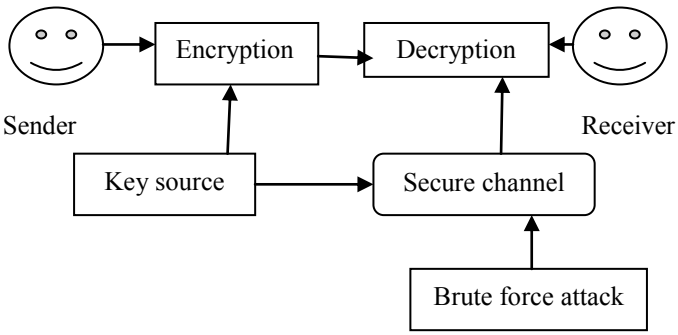


Figure 1 : MAC and Brute force attack.

According to my survey I analyzed that attempts was made in cryptographic system to provide the security applications. Before introduced the concept HMAC the people extensively using the MAC for communications between two parties. The message and key shared between sender and receiver. The sender encrypts the message with his key and send the cipher along with the message, the key also shared by using suppurate channel. In some previous stated that MAC does not guarantee the accompanying message is authentic because of the attacker can identify the key he can access the message. The brute force attacks can modify the message. However various security papers have suggested this mechanism vulnerability to malicious attacks.

The above figure represents the MAC schema work flow and why MAC does not guarantee the security, the attacker can get the key form secure channel.

All the previous research papers attempts was made pointing to HMAC algorithm is mainly for provide the message authentication and preventing the snooping attacks. The design of HMAC specification was motivated by the existence of attacks on more trivial mechanisms for combing a key and a hash function [2][3][4]. No attempts to be found for authorizing the sender and as well as receiver .The previous papers done attempts about the HMAC and signcryption techniques separately. The HMAC can be an implementation of any function like MD5, SHA-1.

The message digest is based on one way function it takes the long plain text as input and produces the fixed length bit of output.

Suppose X is message and MD(X) gives the fixed length of output, if any attacker changes even one bit also it is going to give a different output.

Keyed Hash Message Authentication Code (HMAC) is approved by Federal Information Processing Standards as best mechanism using cryptographic hash functions [7] .It can be used with any iterative hash function in combination with key. The HMAC's was designed with two functionality distinct parameters .a message input and a secret key known only to the message originator and intended receivers.

III. Security Consideration

Security play very important role in current constrained environments, the constrained environment cannot support some complex computations and has limited resources and these systems must support the security applications message authentication, integrity and replay attacks [1].The previous research papers aimed to declare the one-way block information based in stream cipher is fulfill the all security applications.

A stream cipher exhibits the fallowing behavior:

a. The stream cipher initial using the one vector value to generate the pseudorandom stream which is strongly dependent on a secret key.
b. The security of cipher is measured in term of rotation of the message key stream to generate pseudorandom.

The above mechanism is suitable when the short string of message should be transformed, when we want share the short length of string random key generation is not required .In cryptographic system so many type of attacks, one of those attacks are based on establishing the validity of partial guess of secret key the attacker can guess with the given output string .The attacker can get the value only when the output string is considerably higher than the guessed value. To prevent

© 2011 Global Journals Inc. (US)

these attacks by compressing the string into too short that is not longer than secret key. The HMAC can resist the key related attacks. These types of attacks are plays critical role, here the key is which are the one important to generate the MAC value. In HMAC schema the key is divided and each key again XOR with some text. This is the way of showing how the HMAC can resist the related–key attacks.

$$HMAC\ (text) = H\ [Kout \parallel H\ (Kin \parallel text)]$$

Security has become an important issued in the constrained environments .In wireless communication security can achieve by using the some specific procedures and methods. The security applications can achieve by using DES is a big deal. It is a big headache to the parties. To overcome this headache the previous research papers attempted to achieve the security application by using the AES, because of AES can implement in hardware and as well in software [6] [9].

IV. HMAC Based Protocol and Signcryption

I analyzed previous attempts made on HMAC and signcryption [2][3][4][5].The attempts made individually and not constrained environment. One paper [1] made attempts on only HMAC i.e. they aimed to provide the security for the message .No one made attempts to authenticate the parties those are participating the communication.

The constrained environment like hand held device, Sensor networks and Rfid these wireless environments require non- contact automation. Such components should support the security application like message authentication, integrity, time stamping and snooping attacks. These components cannot support the complex computations, high communication overhead and has limited resource. The paper [1] attempts made to get the authentication in Rfid environment. I proposed the mobile environment is the one of constrained environment because of the resource very limited in mobile environment and also high over headache for complex computations. The HMAC can be used to provide the security for message which is part of transmission. As part of HMAC we can deal with any algorithm MD5 or SHA-1.The difference between these two algorithms is the only length of generated output stream and can be used based on the requirement.

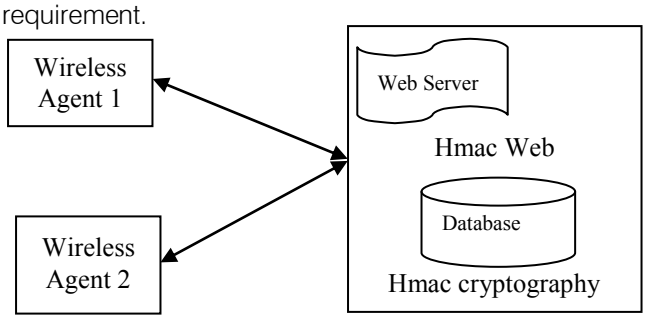


Figure 2 : Architecture of proposed protocol

In the above architecture the communication established between two wireless agents. The protocol is developed based on the HMAC this protocol should be mutual authentication protocol between the sender and receiver. HMAC algorithm is developed by referring the paper [4].I used the algorithm which proposed in paper [4]. I have taken the approach described in that paper I used the MD5 algorithm to get the hash value for the string. The hash-function methods require constant monitoring, maintenance, and updates to maintain integrity.

a) Work flow of HMAC algorithm

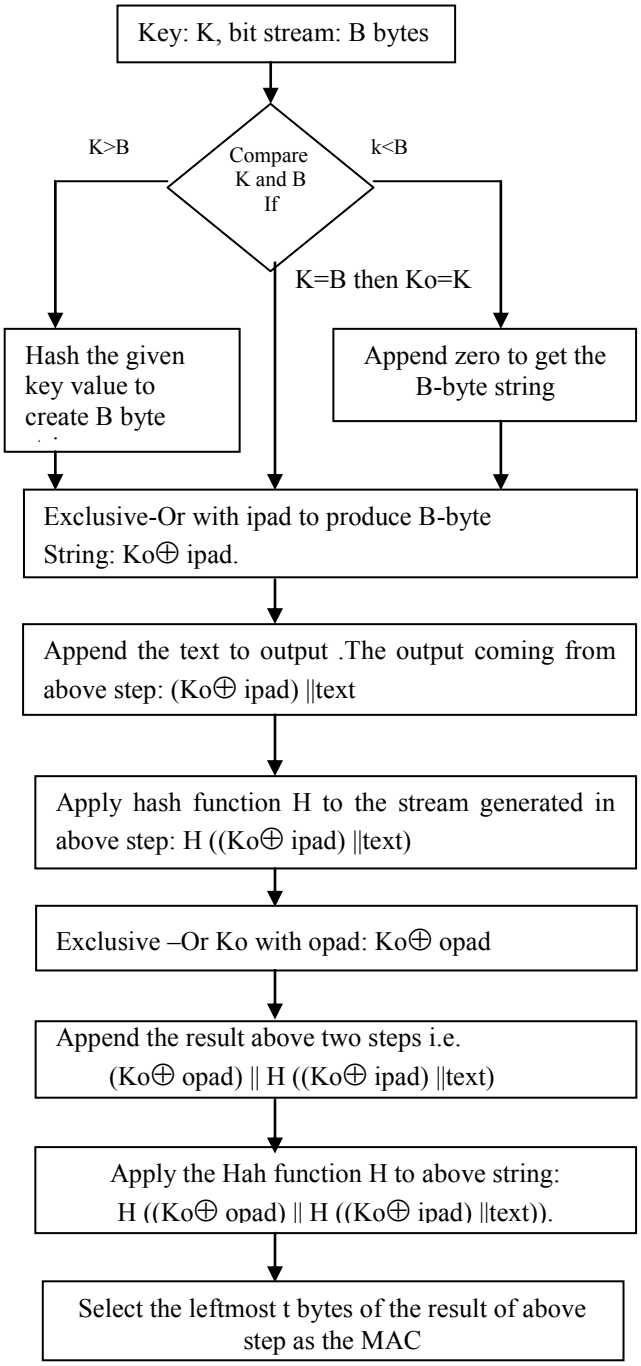


Figure 3 : Internal flow HMAC Algorithm

© 2011 Global Journals Inc. (US)

Addition to above proposed algorithm I enhanced the protocol for Authorization of parties i.e. sender should be authenticated and as well as receiver also should be authorized this enhancement I did by using the RSA algorithm. In wireless communication before sharing the message the handshake process is done by using RSA.I suggest the RSA algorithm is best when want verify the sender and receiver is valid source or not .In RSA algorithm the sender should generate the challenge value before sending the message .This challenge is sent to receiver, the receiver again generate one response and send back to sender by this flow the sender and receiver both authorized.

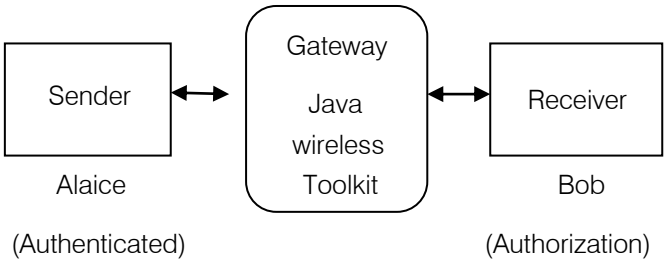


Figure 4 : The architecture of protocol with Enhanced work

V. Implementation Setup

This section describes implementation of HMAC based protocol .This protocol developed in mobile environment by using JME.As part of JME API one of the most useful class us MIDlet. This web application can be developed by using the javax. microedition interface. The class in java.io package is used to develop the cryptographic functions. In HMAC based protocol developed as web application the complete security as developed as part of web server. This is part of providing the security for the message.

Table 1 : Procedure to develop the signcryption

Steps	Step-by-step Description (Aliace-Bob)
Step1:	The users Aliace has to create or generate the keys
Step2:	Bob has to generate the keys.
Step3:	Aliace should be registered with gateway
Step4:	Bob also registered with the gateway by giving his identification i.e. he must entre his Unique ID
Step5:	Aliace make the contract signing with the Bob
Step6:	Finally bob prepare the Initial challenge value.

In enhancement of HMAC based protocol, the sender and racier both should be authorized .I suggest the asymmetric algorithm RSA for this enhancement. In a above table 1: Aliace and Bob are two parties whose generate the challenge response. The users must register with gateway for sharing the message, and receiver has to give his identification to sender. The implementation of this handshake process between Aliace and Bob as shown above Figure c and d.Aliace and Bob generating the keys and sharing the challenge values to verify whether the originator is valid resource or not.

VI. Performance Analysis

The performance analysis done by considering the some scenarios.

1. Only MAC
2. HMAC with DES
3. HMAC with AES
4. HMAC with AES and Signcryption

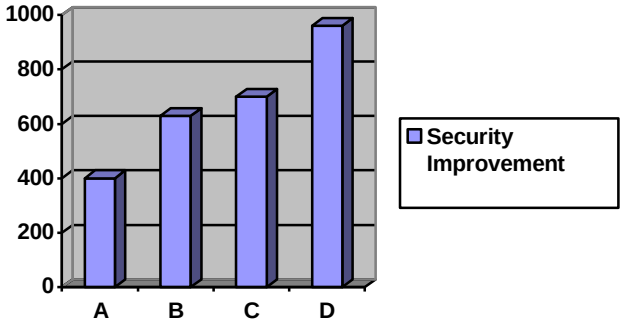


Figure 5 : Security Improvement

A -MAC, B -HMAC with DES, C -HMAC with AES, D-HMAC with AES and Signcryption

The above graph represents cryptographic mechanisms support the security application i.e. message authentication, integrity, and time stamping and snooping attacks. In existing system the block cipher along with DES also gives the less performance than AES. Security improves more when we use the HMAC along with the signcryption. In my proposal system along with the security of message by using HMAC, we are authenticating the parties who are involved in the communication.

VII. Conclusion

Hand held devices and Wireless Sensor Networks pose a need for efficient implementation of MAC. To achieve efficiency, while not sacrificing security, there is a need to evaluate new approaches, while also utilizing any characteristic of the specific implementation of MAC that can enhance efficiency. A complete highly compact MAC implementation, based on stream ciphering, was presented. The principle was

© 2011 Global Journals Inc. (US)

to implement a hash transformation based on the stream cipher, where the strength of the hash is associated with the underlying security of the cipher. The hash is then utilized to implement HMAC based on standard 5 procedures. The HMAC based protocol with signcryption can prevent the attacks and gives the guarantee for authentication and integrity. A specific implementation, based on DECIM (v2) [1], a highly scrutinized stream cipher, was presented and analyzed in detail.

Acknowledgment

I would like to thank Sr.Asst.Prof V.Sathish, Sr. Asst.Prof A. Poongodai and Prof D. Sujatha (Aurora's Technological and Research Institute, Hyderabad, India) for proposing the concept of HMAC with signcryption in constrained environment as well as providing their careful reading and valuable suggestions. I would also like to thank the anonymous referees for their helpful comments, correction and suggestions to improve this work.

References References Referencias

1. Benjamin Arazi, Senior member,IEEE,"Message Authenticaiton in Computationally Constrained Environments",IEEE Trans. Mobile Computing ,Vol.8 ,No.7 July 2009.
2. Smith- Mstr Thesis," Digittal signcryption " ,thesis presented on Combinatorics and Optimization Waterloo,Ontario ,Canada,2005.
3. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functionsfor Message Authentication," Proc. Ann. Int'l Cryptology Conf.(CRYPTO '96), pp. 1-15, 1996.
4. H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashingfor Message Authentication," IETF RFC 2104, 1997.
5. ANS Institution, "Keyed Hash Message Authentication Code," ANSI X9.71, 2000.
6. Majithia Sachin, Dinesh kumar,"Implementation and analysis of AES, DES ,and Triple DES on GSM Network",IJCSNS ,Vol.10,No.1,January 2010.
7. National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB 198, Information Technology Laboratory, 2002.
8. National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-1, Information Technology Laboratory, 1995.
9. "Wireless Security Handbook," Acerbic Publications 2005.
10. L. Talavera and J. Bejar, "Generality-Based Conceptual Clustering with Probabilistic Concepts," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 23, no. 2, pp. 196-206, Feb. 2001.
11. H. Jin, M.-L. Wong, and K.S. Leung, "Scalable Model-Based Clustering for Large Databases Based on Data Summarization,"IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27, no. 11,pp. 1710-1719, Nov. 2005.
12. T. Honkela, S. Kaski, K. Lagus, and T. Kohonen, "WEBSOM—Self-Organizing Maps of Document Collections," Proc. Workshop Self-Organizing Maps (WSOM '97), 1997.
13. M. Junker, M. Sintek, and M. Rinck, "Learning for Text Categorization and Information Extraction with ILP," Proc. First Workshop Learning Language in Logic, 1999.

© 2011 Global Journals Inc. (US)

This page is intentionally left blank

© 2011 Global Journals Inc. (US)

Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

e-Governance in Technical Education- "roadmap" to efficient management of Technical Education In India

By Priyanka Mahendru, Prof. D.V.Mahindru

E.I. Deptt. SRMGPC, Tewari Ganj, Lucknow

Abstract - The governance of Technical Education in a developing country like India is a challenge, because during the recent past, there has been a phenomenal growth of technical Institutions, without proper rules and regulations. All those connected with Technical education are passing through the worst ever trauma as the Governors (policy & decision makers) through statutory bodies viz AICTE,UGC ,Universities etc have miserably failed to protect the interest either of governors or governed. More so, in India, where the governments are formed through democratic means, the challenge of governance is much larger as the governors themselves are at times not very clear on various rules and procedures and sometimes because of the vested interest of a few unscrupulous, non professional, non-academic, semi literate and illiterate people having taken over the control of technical education with their money power/muscle power. Further, at times, the rules and procedures, though explicitly defined in the constitution, statutes or ordinances, by themselves become hindrances in the path of governance due to lack of transparency and procedural clarities. Moreover, governance is a dynamic process, that cannot be handled through static rules and procedures. Here is the necessity of E-governance or electronic governance - True e-Governance with focus on Transparency, Integrity, gender equity, women empowerment, Processes, Security, Accountability, protection of the interest of students and accessibility: E-governance uses modern information and technologies such as internet, mobile etc for effective, efficient and transparency in information and communication. E-governance is a mechanism that is quick, interactive and provides a clear repository of rules and regulations, which extend help in decision making for both the governors and the governed. The mechanism has the benefit of providing clear cut, transparent, interactive, easy to implement and just solutions (in dynamic mode) in the quickest possible time frame. The technical education in India is passing through the most fluid stage requires this mechanism (across the board) ensuring "Cradle to grave" control of quality. The paper suggests the role of the statutory bodies i.e. Central Government through AICTE/NBA at National Level, the affiliating University at State Level and the Governing Council of the concerned College through Faculty ,Administrative Staff, Students, their parents/ Guardians, citizens and society as a whole at the Institution Level, to ensure the technical education to be e-governed.

Keywords : *e-governance, technical, education, professional, corruption, corporate, multi-disciplinary.*

GJCST Classification : *J.1*

Strictly as per the compliance and regulations of:

© 2011l . Priyanka Mahendru, Prof. D.V.Mahindru. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

e-Governance in Technical Education- "roadmap" to efficient management of Technical Education In India

Priyanka Mahendru[α], Prof. D.V.Mahindru[Ω]

Abstract - The governance of Technical Education in a developing country like India is a challenge, because during the recent past, there has been a phenomenal growth of technical Institutions, without proper rules and regulations. All those connected with Technical education are passing through the worst ever trauma as the Governors (policy & decision makers) through statutory bodies viz **AICTE,UGC** ,Universities etc have miserably failed to protect the interest either of governors or governed. More so, in India, where the governments are formed through democratic means, the challenge of governance is much larger as the governors themselves are at times not very clear on various rules and procedures and sometimes because of the vested interest of a few unscrupulous, non professional, non-academic, semi literate and illiterate people having taken over the control of technical education with their money power/muscle power. Further, at times, the rules and procedures, though explicitly defined in the constitution, statutes or ordinances, by themselves become hindrances in the path of governance due to lack of transparency and procedural clarities. Moreover, governance is a dynamic process, that cannot be handled through static rules and procedures. Here is the necessity of E-governance or electronic governance - True e-Governance with focus on Transparency, Integrity, gender equity, women empowerment, Processes, Security, Accountability, protection of the interest of students and accessibility: E-governance uses modern information and technologies such as internet, mobile etc for effective, efficient and transparency in information and communication. E-governance is a *mechanism* that is quick, interactive and provides a clear repository of rules and regulations, which extend help in decision making for both the governors and the governed. The *mechanism* has the benefit of providing clear cut, transparent, interactive, easy to implement and just solutions (in dynamic mode) in the quickest possible time frame. The technical education in India is passing through the most fluid stage requires this *mechanism* (across the board) ensuring "Cradle to grave" control of quality. The paper suggests the role of the statutory bodies i.e. Central Government through AICTE/NBA at National Level, the affiliating University at State Level and the Governing Council of the concerned College through Faculty ,Administrative Staff, Students, their parents/ Guardians, citizens and society as a whole at the Institution Level, to ensure the Technical Education to be e-governed.

They have got a very powerful arm i.e. a statutory body by the name and style of **AICTE** packed with the professionals of International Level, with teeth, fully aware of their responsibility and competent enough to implement the rules and regulations. The concerned state government through the affiliating University has all the powers to control and regulate these technical institutions through this powerful tool of e-governance. It must be noted that the very existence of these technical institutions very well depends upon the **"NOC"** issued by the state Govt. The e-governance is not the magic wand to streamline the administration of technical education but there is hope in it. The success depends upon the efficacy of the "e-tools employed", "across the board" and whole hearted cooperation of one and all i.e. from "Peon to the Chairman of the all powerful Governing Council" . We have everything at our disposal with a history of success stories but the only lacking factor is "Political Backing" and "Will to Do" and above all prevailing corruption *–a stark reality.*

The paper describes the ways and means to eradicate mismanagement with case studies from technical education. Every management has got the right to "Manage" but not to"Mismanage", to fulfill collective aim of:

"College to Corporate as New Kind Of System Thinking Employable professionals"

Keywords : e-governance, technical, education, professional, corruption, corporate, multi-disciplinary.

I. Introduction

The education being on the **concurrent list**, the Central (National) Government has all the powers to control and regulate technical Education in India (**right from establishment of Technical Institution to exit of Employable Professionals).** They have got a very powerful arm i.e. a statutory body by the name and style of AICTE packed with the professionals of International Level, with teeth, fully aware of their responsibility and competent enough to implement the rules and regulations. The only lacking thing is "Political Backing" and "Will to Do" and above all prevailing corruption *–a stark reality .* The immediate problems to be addressed are shortage of talent, new kind of engineer with system thinking, and multidisciplinary, innovative approach to meet the challenges ahead. The paper lays the roadmap suggesting the ways and means to meet the challenge with effective management of technical institutions ;

Author[α] : Sr. Lecturer (E&C Engg.) in E.I. Deptt. SRMGPC, Tewari Ganj, Lucknow-227 105 U.P. (India).
Author[Ω]: Professor (Mech. Engg.) in Mech. Engg. Deptt., SRMGPC, Tewari Ganj, Lucknow-227 105 U.P. (India)

© 2011 Global Journals Inc. (US)

CHALLENGES-AHEAD

a) Shortage of Talent

All the private-public partnership projects are highly complex, are high-tech and impact a phenomenal number of Indians. As more such initiatives get under way, the effort will require an enormous increase in the engineering workforce. Because organizations and the environment in which they operate are changing fast, the chasm between the skills required and skills available is widening rapidly. In the power sector, for example, the total additional manpower required for the 11th plan period is of the order of one million. In 'Power Generation' related projects the requirement for entry level people is7,308 but only 5,040 are available. The shortfall is about 31%. At senior levels the shortfall goes up to 34%. There is a demand for 8,000 to 10,000 engineers in the embedded software and chip design space, but the supply is just a third of that number. In telecom, the wireless segment, there is an annual shortfall of 8,000 engineers. How will we as a nation address this shortfall?

b) Engineering Landscape in India (IIT Bombay Study)

To get a better handle on the problem, IIT Bombay undertook a study on the engineering landscape in India.

The study aimed to answer questions such as:

- Has the engineering education system been able to provide, quantitatively and qualitatively, the engineers required for the growth of the Indian economy?
- Has it provided the research and development leadership required for our industry?
- In the context of globalization, is there a need to modify the higher engineering education system in India?

The study shows that against the sanctioned seats of 6.57 lakh for Under Graduate Engineering education in India, only 2.37 Lac engineering degrees were awarded in 2007-08. This very clearly highlights the shortfall. In2006, India awarded about 2.37 lakh engineering degrees, 20,000 engineering Masters degrees and 1000 engineering PhDs, which means a total of 2.58 lakh engineering degrees of all types. This is clearly not enough! The awarding of degrees is also not evenly distributed across India. Five states – Tamil Nadu, Andhra Pradesh, Maharashtra, Karnataka and Kerala are said to account for almost 69% of the country's engineers. It is estimated that about 30% of the fresh engineering graduates are unemployed even one year after graduation; **and this is even as many sectors complain of lack of talent.** This clearly points that there is definite scope to improve quality of engineering education. Let us also look at the gender factor. At IIT Bombay, the percentage of women graduates to the total is about 8% at the B.Tech. level, 9% at the M.Tech level and about 17% at the Doctoral level including Science, Humanities and among the faculty – only about 10% of the IIT Bombay faculty comprises women. Gender disparity in the engineering stream exists around the world, not just in India, and special efforts are being made by institutions, Governments and professional organizations to rectify these. Some Indian states have provided incentives like free tuition for women studying engineering. Overall, the study rightly points out that India has the potential to be a leading research and design hub in the world. For this, we need to have a mechanism to identify important areas and develop policies and institutions accordingly. Situations and problems we confront today demand composite responses and solutions.

c) New Kind of Engineer

Globalization has enabled a new place for India, the challenges facing our country are new, and the market is highly dynamic and complex. In this scenario, the industry demands a new kind of Engineer.

d) Systems Thinking

This complexity demands a new way of thinking – it requires a Systems Thinking approach to macro level challenges and requires Engineers to keep one eye on the big picture even as they tackle specific tasks. Systems thinking provides a conceptual framework that helps make full patterns clearer and helps one to see how to modify these patterns more effectively.

This type of thinking is tricky to most of us because As Peter Senge says, it is a "discipline for seeing the whole". We are taught to break problems apart, to fragment the world! This appears initially to make complex tasks more manageable; but we pay a hidden price: we can no longer see the consequences of our actions, and we lose our intrinsic sense of connection to a larger whole. When we want to see the big picture, we try to reassemble the fragments and organize all the pieces. The task is futile– similar to trying to reassemble the fragments of a broken mirror!

e) Multi-Disciplinary Approach

Today's Engineers must also be able to view management activities through different lenses and work with people from different disciplines and diverse fields such as business, banking services and medicine. Even the software development process can incorporate complementary techniques from other disciplines, such as, accounting, product management, marketing, economics, and organizational behavior. Situations and problems we confront today demand composite responses and solutions. A multi-disciplinary approach involves

© 2011 Global Journals Inc. (US)

absorbing from multiple disciplines to define and apply new ways of understanding complex situations. The great advances of recent times – nano devices, telecommunication engineering – affirm that these come about from people who understand engineering systems as a whole.

India is becoming professional, it is also eager to go global. The technologies ,We need today should address poverty, pollution, illiteracy, congestion in urban areas etc. It is the wholly Indian Company, TCS that designed and developed an internationally recognized **"Adult Literacy Program"** based upon cognitive and Linguistic principles, cutting edge software technologies and some standard hardware platforms. It is not low technology but cutting edge high technologies that are going in to making simple utilities that addresses needs of rural people. In India, due to its size, diversity and complexity, we do not have to go looking around for challenges, these are plenty. We do not have to look around and we will find something that needs improvement. We also have great minds, great thinkers. We just have to look for ways to bring them together. It is this fraternity of Engineers that will determine.

"INDIA OF TOMORROW".

"Yesterday's collaborators are today's Competitors".

We have travelled a very long journey and our "Intellect" is second to none. What we need is to mould young professionals to the needs of our Industry. The eyes of the world are on us. We have the opportunity to become a superpower. We all owe it to ourselves to shoulder the responsibility.

We will decide our role on the global stage

f) Innovation-Led Growth

India's future growth will be **driven not by cost but by innovation** in terms of product offerings, process efficiency, value engineering and cost reduction. It is realized that India's rural population of almost over 700 million is "heavily under banked" . TCS has proved that banking can be conducted without a **brick and mortar** branch. Agents are provided with a handheld device to carryout the transactions in the field. Smart Cards were issued to unbanked customers and agents. Why can't we think of providing **Smart Card to each and every person** connected with technical education i.e. from security Guard at the gate to"**Technocrat/Professional"** going out of the institution giving complete history of:

i) Demographic details of the Members of various Governing bodies/Faculty/Staff etc
ii) Financial Accounts giving complete history of all the financial transactions from day one.
iii) Fingerprints
iv) Academic record.
v) Default List.
vi) Achievements.
vii) Failures.
viii) Punishments/Awards etc

g) Developmental Challenges

Even as we reach for the moon, there are millions here on earth for whom basic needs are elusive. No country can afford a skewed growth. If India has to achieve a 7% to 8% sustained growth, it needs not just **"Corporate India"** but the rural sector, the agricultural sector to grow as well. It is these areas that badly need engineering talent. The government, we and all of us together have to find ways to make it an attractive option for engineers to take up these challenges.

h) Corruption

The corruption a **stark reality** is cancerous that needs to be addressed. Various initiatives by the government viz RTI, SMART government, Integrity pacts, CVC, NHRC,AICTE,UGC etc have instead of solving the problem ,added to the corruption. All these bodies have miserably failed to address these problems. No half hearted approach can address this problem. Our hon'ble President Pratibha Patil in her address to the nation has dealt with the issue of corruption calling it a cancer. There cannot be just one panacea or remedy to deal with it but a system of transparency and accountability put in place at various levels and then enforced. It requires **"Preventive" and "Punitive"** measures, as well as adoption of rational approaches as we pursue our national agenda.

i) Fight for Survival

This uncontrolled growth of technical Institutions and now Universities has put the promoters in a very precarious situation. They are fighting a pitched battle of survival because of non-availability of the students coupled with dropouts. To start an IIT, in the first phase , you require nearly 800 crores, whereas a private University does not require even 8 crores, to impart global education. In reality there is nothing of that sort. I will be failing in my duty, if I don't place on record the wonderful job done by some of the private Institutions.

j) Can't Be a Commercicail Venture

It may please be brought to the notice of everybody on this earth that opening of " Technical University/Institution" **can't be a commercial venture**. It is a task of philanthropists (Like the one done by the promoters of SRMGPC), who having achieved excellence in different fields are there to contribute to this noble cause. What matters is not how much you have taken out of these institutions, the important thing is how much , you have pumped in these institutions. This is what has been done by Thapars,Birlas and TATA's to name a few. Their contribution to the cause of education and to the society is unparallel.

© 2011 Global Journals Inc. (US)

k) Deterioration of Standards-Govt as Leader

It is eye opener for all of us what these Govt Institutions could not do in 80 years of standing has been done by these Private Institutions within a span of less than 10 years. Most of the Govt. institutions are affected by the following shortcoming. The government/ municipal/government aided schools are testimony to the callous attitude of authorities. There are no buildings for primary/high schools, what to talk of infrastructure. The classes are being run under a tree . It is a common scene one can have in a most prosperous states like Punjab/Haryana. These private Institutions have done yeoman's service to the nation/society. These government institutions are the victims of the following :

i) Shortage of staff.
ii) Ad-hocism
iii) No upgrading of infrastructure
iv) Poor upkeep of Labs/workshops.
v) Politics
vi) Vested Interest in not filling up the posts.
vii) Practically No-Governance
viii) God may care attitude.
ix) Drop-out
x) Insecurity
xi) Poverty
xii) Poor academic level of students.
xiii) Language problem.

II. State's Responsibility

The concerned state government through the affiliating University has all the powers to control and regulate these technical institutions through this powerful tool of e-governance. It must be noted that the very existence of these technical institutions very well depends upon the "NOC" issued by the state Govt. The affiliating University has the following role to play in the conduct of these institutions to safeguard the interest of students, teachers, parents/guardians, society as a whole:

a) Students

i) To conduct entrance examination at the state level to ensure fair and smooth admission of students as per the statues and ordinances of the University. This is being done meticulously by most of the Universities in the country.
ii) To fix reasonable fees for each course per semester. This is not being done honestly. There are certain loopholes/loose ends that are yet to be plugged. The present fee structure hardly has any place for the poor student. This aberration needs to be corrected.
iii) To safeguard the interest of the students so as to ensure that they are being provided with promised facilities/teaching infrastructure.
iv) To conduct the fair/ smooth examination in time and as per the laid down rules and regulation of the University.
v) Declaration of results in time.
vi) Distribution of mark sheets .
vii) Conduct of convocation to distribute degrees in time.

All the above activities are being done by most of the Universities in time except the fixation of fees. There is lack of transparency in this activity. It will not be wise to pass any judgment on this aspect except to suggest more transparency in this activity.

b) Faculty/Staff

They are worst sufferers. As per the commitment of these institutions, they are supposed to be managed as per the AICTE/UGC norms. But nothing is followed by any institution except a few. They are being hired/fired like casual Labors (Adda Labors). There is unbearable suffering through which these people are passing. In most of the institutions there are:

i) No Leave rules.
ii) No service rules of their own as the statutory norms of the AICTE/UGC are not followed.
iii) No salary rules (All discretionary)
iv) No security of service.
v) No terminal benefits .
vi) No norms of workload.
vii) No dignity of teachers
viii) Lack of proper seating arrangement for teachers.

After going through the working conditions, one wonders whether We are living in a free and democratic country, Father of the nation, Gandhi, Pt. J.L. Nehru, Netaji Subhash Chandra Bose, Shaheed Bhagat Singh ,had dreamt of ,or pre-independence era ruled by Britishers.

All these sufferings are to be addressed by none other than the statutory bodies of the state Governments concerned without loss of time. It is practically not possible for the ill equipped state technical Universities. They hardly have any permanent machinery/staff to ensure implementation and monitoring the progress. The concerned state Governments who are supposed to provide the necessary infrastructure are hand in glove with the managements /promoters of these technical institutions. Most of the Universities hardly have any staff of their own .They are depending upon casual/temporary staff working from camp /rented offices. Even the Vice Chancellor/Registrar is on deputation. They have no power to recruit even a peon. They are just helpless personalities entrusted with the task for which they have:

I. All the "authority" but no resources.
II. Ability but no machinery to act.

© 2011 Global Journals Inc. (US)

It is not that state governments have no power/facilities/capability to do this gigantic task, the fact is there is " **NO WILL"** to do this. They have developed vested interest to maintain **"Status Quo"** , keep the situation like this because there is hardly any politician who does not have one or group of Technical Institutions /Universities owned by him irrespective of political affiliation . As such nothing can be expected from the change of guard at state government level or change of political governors because no purpose will be served by changing the **" bottle when the liquor is same".**

The state Governments have very accurately controlled the system of revenue collection like Electric billing/water Tax/house Tax etc .There is absolutely no corruption in collection of revenues in this head.

The implementation of e-governance in revenue collection by the state machinery is almost total, then why not **technical education**. Ultimately every state government has to go for this. There is no substitute for this. It can be delayed but not avoided because management of such vast and important wing of our economy cannot be left at the mercy of destiny.

What We **"NEED IS POLITICAL WILL AND SINCERITY OF PURPOSE"** on the part of the state Government- Everything can't be controlled by e-governance only overnight but a set of measures. The task is gigantic and the state governments are engaged in various pitched battles to tackle with poverty, unemployment, corruption, Nepotism, favoritism and political compulsions. Added to this is the **"uncontrollable growth of institutions"** producing an army of Non-employable Technocrats year after year etc. The task is "Big" but not lacking solution. There is a hope in e-governance.

III. Institutional Responsibility

The total success of this e-governance depends upon ,apart from the positive attitude of one and all especially the Governing Councils of the Institutions , efficacy of the e-tools, the **"across the board"** whole hearted cooperation of one and all i.e. from "Peon to the Chairman of the all powerful Governing Council" at the institution level. The honest and the highly professional are worst hit by the "corruption". It has been rightly pointed by the President of India, corruption is affecting nation's political, economic, cultural and social life. **It is like a cancer, There cannot be just one panacea or remedy to deal with it but a system of transparency and accountability put in place at various levels and then enforced. It requires "Preventive" and "Punitive" measures, as well as adoption of rational approaches as we pursue our agenda. Every politicians/ Bureaucrat/Management is not corrupt .It is result of their "Vision" that technical education has been groomed to this level.**

The role of private managements in the growth of technical education during the last decade is worth appreciating. Some of the institutions have done wonders in putting the "**Fully Transparent"** system in place. They have established an international brand. To name a few

i) BITS
ii)Thapars
iii)SRMGPC
iv)Galgotia's
v) BBD group

Within a span of 10 years, apart from meeting the requirement of world class technical manpower, they have developed an Infrastructure that can match any International standards.

They have rendered yeoman's service to the mankind. It is shear their enterprise and acumen that the technical education is today. Nation is indebted to these entrepreneurs and salutes them for their contribution.

a) Software Application for E-Governance in Technical Education-Case Study

In SRMGPC, likely to be upgraded to University, is using software Newton ERP6.1 (ORACLE), OracleAS Form Services, Nippondata Systems Limited, 44, Community Centre, Naraina Industrial Area, Phase-1, New Delhi-110028 for entire e -governance. The activities listed below are electronically controlled.

b) Students

i) Admision process right from counselling to issue of admit card.
ii) Attendance record.
iii) Lecture schedule
iv) Course curriculum.
v) A ssignment/Tutorial/Quiz Schedule//Lab/Work shop record
vi) Fees record
vii) Internal Assessment record (Marks Record)
viii) Feed back about teacher's performance in the class.
ix) Student's default record.
x) Achievement record.
xi) Digital Library/ Library feed back using Libsys/web-opac software.
xii) Academic Calendar
xiii) Extra curricular activities
xiv) Facilities for Research & Development.
xv) Hobby Club like photography.
xvi) Sports
xvii) Awards for Academic Excellence
xviii) Scholarships for meritorious students
xix) Innovation awards.
xx) Various types of Leaves.
xxi) Financial support to encourage Innovative Projects.

© 2011 Global Journals Inc. (US)

xxii) Sponsoring the students to attend seminars, inter college competitions.
xxiii) Arranging and involving students in International/National seminars.
xxiv) Stores
xxv) Purchase of items.

c) Faculty/Staff

i) Appointment letter with terms and conditions.
ii) Leave rules (Various types of Leaves).
iii) Duty hours.
iv) Attendance records.
v) Gratuity rules.
vi) Terminal benefits.
vii) Dress code.
viii) Salary Slip.
ix) Leave Record.
x) Leave Encashment.
xi) Student's feedback about the faculty.
xii) Alternative arrangement during leave.
xiii) Course Plan.
xiv) Lecture Schedule.
xv) Attendance record of Tutorials/Lectures/Labs/workshops.
xvi) Assessment record of students (Quiz Tests,Surprize Quiz Test,Mid-sem. Exam)
xvii) Defaulters List giving details about the latest status of academic commitments.
xviii) Teaching plan and the performance report.
xix) Promotion rules

Everything is fully transparent and accessible to each and every Student/Faculty/Staff. There is mechanism to address the grievances of Students/Faculty/Staff and to ensure that everything committed is fulfilled. Name the issue involving the above, it is e-governed. This institution is a role model for others to follow as far as e-governance of Student/Faculty/Staff is concerned. It is an institution that is "Customer Driven" where system has been put in place to address the various issues .I would like place on record the words of President of India, Hon'ble Pratiba Patil, "there should be no effort, consciously or otherwise, that will lead to the erosion of Institutional authority'. Further I would like to remind you the words of our Prime Minister, where he has rightly said there is no magic wand that can solve these long drawn problems overnight. After all the mission of each technical Institution is to produce world class technocrats so as to fulfill our dream of

"From College to world class Employable Professionals"

IV. E-Governance – Success Stories

To address the above cited problems, we need a mechanism to identify important areas and develop policies and institutions accordingly. Such level of voluminous task cannot be accomplished accurately by any government that too manually, how so ever efficient it may be. In the present scenario, when various IT tools are available and they must be used under the umbrella of e-governance. The information and Communication Technology (ICT) and Innovation with sincerity of purpose are the real enablers to tackle this gigantic problem. The assistance of some software giant can be taken to develop dedicated software to put in place and monitor the implementation of various statutory ordinances, rules and regulations especially with respect to the following factors. It may be recalled that concept of smarter government has done wonders, SAHANA, an open source of disaster management system ,deployed by national and state governments has been a boon to citizens affected by natural disasters in the wake of Bhuj earthquake of 2001 and the pan-Asian tsunami in 2004. It has helped millions of people in rebuilding their lives after Bihar Floods of 2008.

Smarter Govt. has also inspired one of the largest transport networks in the world-Indian Railways. The living example is railway reservation –the rampant corruption is thing of the past. Today more than 100,000 employees use the Crew Management System (CMS) that automates and regulates the day to day management of Staff on board the trains coupled with direct data access over mobile phones. CMS helps crew deployment more effectively and improves visibility of information to the right person at the right time, resulting in new efficiencies for the railway system.

Smarter governments also provide up-to-the-minute offering valuable and sometimes critical support to citizens. Today a real time Crime Centre System helps the New York city police analyze crime information to improve public safety with a 27% drop in crime since 2001. It has made New York, the safest large city in the U.S. Data analysis also helps find problems of daily life such as traffic grid locking. This has paved the way for traffic system of Singapore, Brisbane and Stockholm to reduce both congestion and pollution.

a) Application with Impact on Administrative Corruption

- BHOOMI, CARD (registration), e Seva, SETU
- E-procurement: Mexico, Philippines, Bulgaria, Chile
- Tax collection State Border Check Posts, Gujarat
- Customs on-line: India, Philippines, Jamaica
- OPEN, Seoul Municipality, Ahmedabad, Vijayvada
- Teacher's Transfer in Karnataka
- CVC Web site in India, CRISTAL in Argentina
- Drishtee, nLogue, Gyandootin India
- Domestic LPG Gas booking
- Telephone complaint/enquiry system.

© 2011 Global Journals Inc. (US)

4. E-Governance – A solution

To solve this gigantic problem , the following actions are required to be taken:

b) Immediate Action

The statutory requirement is that educational Institutions can be run by "Charitable Societies" only and it is the responsibility of state government to ensure:

i) Constitution of the Charitable Society to be strictly as per the statues. It should not be converted in to private limited company of particular family.

ii) Fulfillment of all the norms by the concerned society before granting letter of intent and finally permission to open a technical institute by the AICTE. If at a later stage it is found that there was relaxation /violation of the set ordinances in granting clearances,

iii) Exemplary punishment must be awarded to the guilty (The Culture of Briefcase to be discontinued).

iv) The interest of the Managements must be thoroughly protected. Honest managements must not be subjected to third degree harassment by the custodians of law. Those following norms must be rewarded.

v) The message must go to the managements they are the "Custodians" and not the "Owners" or Masters. Any lapse on their part can lead them to loosing this status. Let us

Not institutionalize corruption.

vi) Nothing to be left to the discretion of any body because "Power Corrupts a man and the absolute power absolutely corrupts a man"

vii) Application of 2 T formula which would ensure selection through transparent and fair process and also meet the TINA (There is no alternative) criteria which would impel the selection of the right person only.

c) Projected Benefits/Results

- Enhancement of access to quality education.
- Making available knowledge modules in cyber space.
- Optimal utilization of available resources by using ICT

V. Conclssions

There is hope in e-governance and e-governance only. This task of technical education can be very nicely handled by this tool of e-governance. It has already proved its application in various areas of economy. The Central Government, State Government, Technical Institutions and Academia should take the lead and play a pivotal role in inspiring and influencing all those connected with technical education to implement e-governance to enhance the quality of technical education and to root out mismanagement. During last decade, the nation has made marvelous achievement in producing the best (second to none) and largest number of Technical manpower in the world. Our engineers have done wonders in various walks of life either as professional or entrepreneurs. In some cases they have established the standard, their **footsteps have become milestones.** The nation is proud of them. We salute them as achievers. The need of the hour is to consolidate our achievement. The process of consolidation has already started and we are going to be at the top. We have the opportunity to become **"SUPERPOWER"**. I am quite confident of making it.

References References Referencias

1. S.Ramadorai, CEO & MD,TCS: ICT and Innovation : enablers for Economic Transformation; 30th Sir Rajendra Nath Mookerjee Memorial Lecture delivered at 23rd Indian Engineering Congress.
2. Opportunities and Challenges in E-governnce: Subhash Bhatnagar Advisor eGovernment, ISGIA, World Bank, Washington DC (Adjunct Professor Indian Institute of Management, Ahmedabad) sbhatnagar@worldbank.org.
3. Address of President of India on 65th Independence day on 15th Aug'2011.
4. Address to the nation by the Prime Minister of India on 65th Independence day 15th Aug'2011.
5. Smarter government for a smarter Planet by IBM.ibm.com/smartplanet/in/government.
6. Kaylor, C., Deshazo, R. and Van Eck, D. Gauging e-government: A report on implementing services among American cities. Government Information Quarterly, 18 (2001), 293–307.
7. Deloitte Research – Public Sector Institute At the Dawn of e-Government: The Citizen as Customer, 2000.
8. OECD. The e-government imperative: main findings, Policy Brief, Public Affairs Division, Public Affairs and Communications Directorate, OECD, 2003.
9. Koh, C.E., Prybutok, V.R. "The three-ring model and development of an instrument for measuring dimensions of e-government functions", Journal of Computer Information Systems, Vol. 33 No.3, pp.34-9, 2003.
10. Gartner Group, "Key Issues in E-Government Strategy and Management," Research Notes, Key Issues, 23 May 2000.
11. National knowledge commission report.
12. K.N.Gupta, Principal, Govt. Girls Polytechnic, Allahabad. E – Governance: Application in Technical Education Department of, UP Government.
13. Prof. D.V.Mahindru, SRMGPC, Lucknow and Priyanka Mahendru, Sr. Lecturer, "E-Governance in Technical Education- National, State and Institutional Perspective" National Seminar at NITTTR, Chandigarh.

© 2011 Global Journals Inc. (US)

Global Journals Inc. (US) Guidelines Handbook 2011

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

© Copyright by Global Journals Inc. (US) | Guidelines Handbook

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

© Copyright by Global Journals Inc.(US)| Guidelines Handbook

AUXILIARY MEMBERSHIPS

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJMBR 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) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

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

(B) If you are using Internet Explorer, 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.

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

© Copyright by Global Journals Inc.(US)| Guidelines Handbook

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 Swis 721 Lt BT.
- 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 three 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 Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) 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 Inc. (US) 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 Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

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 Inc. (US) 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 Inc. (US), 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 Inc. (US) 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 Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) 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 Inc. (US) 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 Inc. (US) 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 Inc. (US).

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 Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) 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 .

© Copyright by Global Journals Inc.(US)| Guidelines Handbook

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.

© Copyright by Global Journals Inc.(US)| Guidelines Handbook

- 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 Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

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.

© Copyright by Global Journals Inc.(US)| Guidelines Handbook

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

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 Inc. (US).

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

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

© 2011 by Global Journals