

GLOBAL JOURNAL

OF COMPUTER SCIENCE AND TECHNOLOGY: E

Network, Web & Security

Routing Protocols and Metrics

Web Service Composition Approaches

Highlights

Security Algorithm in Cloud Using

Performance Study of Cryptography

Discovering Thoughts, Inventing Future

VOLUME 15

ISSUE 1

VERSION 1.0



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY

GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY

VOLUME 15 ISSUE 1 (VER. 1.0)

OPEN ASSOCIATION OF RESEARCH SOCIETY

© Global Journal of Computer Science and Technology. 2015.

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 distributed under "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: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America

USA Toll Free: +001-888-839-7392

USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin: 452009, 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: investors@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)

INTEGRATED EDITORIAL BOARD
(COMPUTER SCIENCE, ENGINEERING, MEDICAL, MANAGEMENT, NATURAL
SCIENCE, SOCIAL SCIENCE)

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 Finance
Professor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD
(Cambridge)

Dr. Carlos García Pont

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

Dr. Fotini Labropulu

Mathematics - Luther College
University of Regina
Ph.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windsor

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., Eötvös Loránd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram

Department of Accounting and Finance
Lancaster University Management School
Ph.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño

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

Philip G. Moscoso

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

Dr. Sanjay Dixit, M.D.

Director, EP Laboratories, Philadelphia VA
Medical Center
Cardiovascular Medicine - Cardiac
Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng

MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular
Medicine
Davee Department of Neurology and Clinical
Neuroscience
Northwestern 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

Suyash Dixit

(B.E., Computer Science Engineering), FICCTT

President, Web Administration and

Development , CEO at IOSRD

COO at GAOR & OSS

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

Luis Galárraga

J!Research Project Leader

Saarbrücken, Germany

CONTENTS OF THE ISSUE

- i. Copyright Notice
 - ii. Editorial Board Members
 - iii. Chief Author and Dean
 - iv. Contents of the Issue
-
- 1. The Literature Survey on Manet, Routing Protocols and Metrics. ***1-4***
 - 2. Performance Study of Cryptography Based Dynamic Multi-Keyword Searchable Security Algorithm in Cloud using CRSA /B+ Tree. ***5-16***
 - 3. Energy Utilization of TCP in Ad Hoc Networks. ***17-19***
-
- v. Fellows and Auxiliary Memberships
 - vi. Process of Submission of Research Paper
 - vii. Preferred Author Guidelines
 - viii. Index



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY

Volume 15 Issue 1 Version 1.0 Year 2015

Type: Double Blind Peer Reviewed International Research Journal

Publisher: Global Journals Inc. (USA)

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

The Literature Survey on Manet, Routing Protocols and Metrics

By Parvinder Kaur, Dr. Dalveer Kaur & Dr. Rajiv Mahajan

CKD Institute of Management & Technology, India

Abstract- Mobile Adhoc Network (MANET) is a collection of nodes or devices with wireless communications and nodes communicate with each other without any centralized support. Each node acts as a router in Mobile Adhoc Network. No wired infrastructure is required to form a network. Nodes form a wireless environment where nodes can communicate with each other without the restriction of the network topology. Examples of Mobile Adhoc Networks are laptops, mobile phones, PDA, Digital Cameras etc. It is also known as wearable and tearable networks, which are created when the requirement is generated.

Keywords: *manet, routing protocols, metrics.*

GJCST-E Classification : C.2.2



THE LITERATURE SURVEY ON MANET ROUTING PROTOCOLS AND METRICS

Strictly as per the compliance and regulations of:



The Literature Survey on Manet, Routing Protocols and Metrics

Parvinder Kaur^α, Dr. Dalveer Kaur^σ & Dr. Rajiv Mahajan^ρ

Abstract- Mobile Adhoc Network (MANET) is a collection of nodes or devices with wireless communications and nodes communicate with each other without any centralized support. Each node acts as a router in Mobile Adhoc Network. No wired infrastructure is required to form a network. Nodes form a wireless environment where nodes can communicate with each other without the restriction of the network topology. Examples of Mobile Adhoc Networks are laptops, mobile phones, PDA, Digital Cameras etc. It is also known as wearable and tearable networks, which are created when the requirement is generated.

Keywords: manet, routing protocols, metrics.

I. INTRODUCTION

Mobile Adhoc Networks are created for temporary time where nodes can join and leave the created network without any restriction [1]-[3]. Nodes can communicate and route the data in any direction. Nodes which configured themselves with MANET environment may be part of small network or may be part of large network. In MANET type of communication is peer to peer.

Peer to Peer networks are “peers” of computers which are connected with each other with the help of Internet and P2P software. Systems in P2P environment act as a client and server by itself.

Main Challenging part of Mobile Adhoc Network is maintaining the routing information without losing it. Because nodes are arbitrary moving in Manet so required routing protocols which manage the route information in there table if particular node switch off from the Mobile Adhoc Network. Generation of error message should be there if communication link is broken between the nodes when they leave and join the selected network.

II. THE CLASSIFICATION OF ROUTING PROTOCOLS

To transfer data from one node to another node we need some routing protocols that will transfer data without any loss. Protocols are set of rules and regulations which are used in network communication.

Author α: Assistant Professor, CKD Institute of Management and Technology, Amritsar, Punjab, India. e-mail: jassi33@gmail.com

Author σ: Assistant Professor, PTU, PIT University Campus, Jalandhar-Kapurthala Highway, Punjab, India. e-mail: dn_dogra@rediffmail.com

Author ρ: Professor, GIMT, Amritsar, India. e-mail: rajivmahajan08@rediffmail.com

For this purpose routing protocols can be classified as described below:

a) Proactive Routing / Table Driven

These types of routing protocols maintains the list all the routes from source to destination in advance [2]. These types of protocols maintain fresh lists of routes by periodically distributing routing information throughout the network.

b) Reactive (On-Demand) Routing

These types of protocols find a route on demand by flooding the network with “Route Request” packets [2].

c) Hybrid (both pro-active and reactive) Routing

These types of routing protocols combine the advantages of proactive and reactive routing [3]. The routing is initially established with some proactively prospected routes and then serves the demand of additionally activated nodes through reactive flooding. The choice for one or the other methods requires predetermination for typical cases.

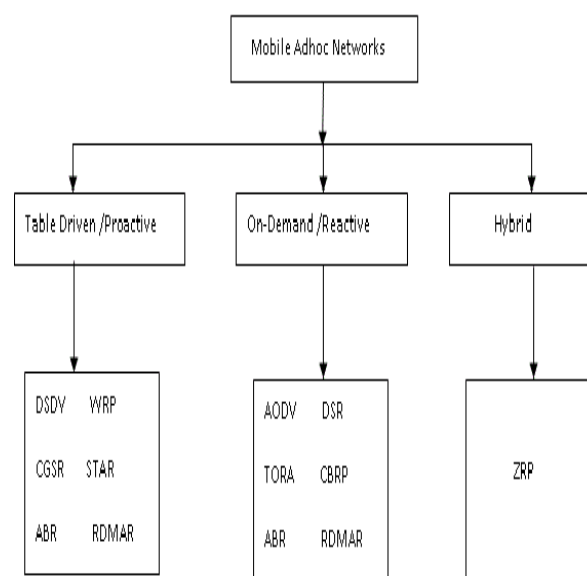


Figure 1 : Classification of Manet Routing Protocols

III. PROACTIVE ROUTING PROTOCOLS

a) Distance Source Initiated Vector (DSDV)

DSDV is table driven and source initiated routing protocols. In DSDV the information about

different paths are for each hop stored in routing tables in advance. When ever source want to send data to destination. It will search the path from the routing tables [1]-[3]. In DSDV each routing table contains the Hop count and Sequence Number. Hop count tells the number of hops occurs in the path for source to destination. Sequence Number is used to update path. The path with the old sequence number is replaced with the new sequence number. The New Sequence number defines the new path from source to destination.

i. *Advantages*

1. The Updation in routing tables regarding paths is done time to time by broadcasting of messages between the hops.
2. Paths are predetermined.

ii. *Disadvantages*

1. Not applicable for Large Networks.
2. Wastage of battery resources unnecessarily due to updation of paths.

b) *Wireless Routing Protocols (WRP)*

WRP is table driven or proactive routing protocol [2]. It is advancement of DSDV protocol. Information about different paths stored at the routing tables in advance. In WRP, Each hop contains shortest path from source to destination. This helps in reduction of about power consumption and loop free routing. WRP uses Distance Table, Routing Table, Link Cost Table and Message Transmission Table while creating paths from source to destination.

i. *Advantages*

1. It stores the information about previous node and next node in the Routing Table.
2. Path searching and path updation cost is less.

ii. *Disadvantages*

1. Required more space due to multiple tables.
2. Complexity is increases due to creation of shortest path in advance and storing the previous node and next node information in the Routing Table
3. Multiple Updation in multiple tables requires more power consumption.

c) *Fisheye State Routing Protocols (FSR)*

FSR is proactive and flat routing protocol. It is also known as Link State Routing Protocol because it uses topology information from source to destination for sending the data [15]. Link state defines the activeness of nodes while creations of path from source to destination. Inactive nodes are not part of the path. FSR also maintain the information about the nodes which are near to the focal point. To maintain the topology information WRP uses Link State Table.

i. *Advantages*

1. Applicable Large type of Networks.

2. Nodes are excluded in the routing tables which are not currently working.

ii. *Disadvantages*

1. Maintaining the topological information about nodes is difficulty which is far from the focal point.
2. It is wired routing protocols.

IV. REACTIVE ROUTING PROTOCOL

a) *Temporary Ordered Routing Protocols (TORA)*

TORA is reactive protocol and on demand routing protocol [3]. It is also known as Link reversal routing protocol. Path searching is based on the source initiation. In the TORA, the path search is performed from higher level to low level. Each node maintains multiple paths from source to destination. While transferring the data from source to destination, any path can be used, which is currently available for transfer the data. Shortest path method is not applicable in TORA. It performs Remote Creation, Route Maintenance and Route Erasure types of operations.

i. *Advantages*

1. Multiple paths available from source to destination.
2. Efficient and loop free routing.
3. Overhead reduce because of on demand creations of routes.

ii. *Disadvantages*

1. Non availability of paths when required.
2. Delay in the path searching.
3. Flooding of messages in the network while discovering of routes on demand.

b) *Adhoc on Demand Distance Vector Routing Protocols (AODV)*

The AODV routing protocol is an on demand routing protocol [8]. Therefore, routes are created only when the requirement is generated [2]. "Hello Messages" may be used to detect and monitor neighbors. Periodically nodes broadcast the "Hello Message" to determine the activeness of neighbor nodes [6]-[9]. This technique is used to know the status of active nodes for data transfer. It broadcasts a "Route Request" (RREQ) to each intermediate node. If the receiving node does not receive RREQ and there is no route to the destination rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP).

i. *Advantages*

1. The searching of paths are done when the requirement is generated.

ii. *Disadvantages*

1. Multiple route replies are generated for the same route request.
2. Time to time "hello" message is generated; which is wastage of resources like battery consumption.

c) Distance Source Routing Protocols (DSR)

DSR is an on demand based routing protocol that is based on source routing [2]. It is designed for use in multi-hop wireless adhoc networks of mobile nodes. DSR is based on the concept of "Route Discovery" and "Route Maintenance". In DSR the Route Discovery process is started by a packet that discovers the path from source to destination and accumulates the whole information about path into its header [2]. Route Reply is generated by the destination if the route is discovered from source to destination and If no path is found from source to destination then the error message is generated [2],[10].

i. Advantages

1. When the whole path is searched from source to destination, then reply is sent back to source. One source reply is generated for route request.
2. It is source generated type of routing protocol.
3. No beaconing technique is used.

ii. Disadvantages

1. Protocol is unable to find the broken links.
2. Full path searching is time consuming process.

d) Zone Routing Protocols (ZRP)

ZRP is hybrid protocol as it is combination of reactive and proactive [12]. Reactive Protocol is on demand protocol which finds the path from source to destination when requirement is generated. Proactive protocol means that information about each path is already stored in the tables. Based on zones, ZRP can also be divided into Intra Zone Routing Protocol (IARP) and Inter Zone Routing Protocol (IERP).

i. Advantages

1. It is combination of reactive and proactive.
2. If the nodes are within the zone table driven technique is used, if nodes are far from zone reactive path searching technique is used.

ii. Disadvantages

1. If the zones are overlapping, difficulty is in the path search.

V. METRICS IN MANET

Metrics are measurements in the manet used to analysis the performance of routing protocols. Metrics are required to evaluate the performance of network; metrics defines how well the network is doing under different parameters [16]. The metrics can be classified in two parts.

- a) Quantitative Metrics: It is numerical measurement of the network performance. It can be defined in numbers like Number of nodes, Number of delays; Number of bytes is transmitted etc.
- b) Qualitative Metrics It is quality measurement of your network performance. Quality can be measured on the basis of Throughput, Route Acquisition Time, and Packet out of delivery etc.

Some performance metrics are:

- i. Throughput: It defines the number of bits transferred per unit time.
- ii. Packet Delivery Ratio: It defines the total number of packet delivered out of total number of packet sent.
- iii. End to End Delay: It defines the time taken by the packet to reach the destination. There are four packets which affect the performance. like transmission delay, propagation delay, processing delay, average delay.
- iv. Jitter: Jitter is also known as delay .Delay occurred because of network congestion, improper setting of network etc.
- v. Packet Loss: It defines the how many bits are lost due to delay.

Table 1 : Performance Metrics In Manet

Metrics	Formula
Throughput	No. of packet received/No. of per Unit of time
PDR	No. of packet received/No. of packet sent
End to End Delay	Time the pkt sent-Time the pkt received
Jitter	$\frac{((PA+1)-(PS+1))-((PA)-(PS)))}{N-1}$
Packet Loss	No. of pkt sent-No. of pkt received
PA=Packet Arrival, PS=Packet Start	

VI. CONCLUSION

In this paper, we have surveyed the various routing protocols with their advantage and disadvantages. We analyzed the metrics which are used to analysis the performance of the network. As mobile adhoc network growing day by day. there are many area to review like routing protocols, types of attack, application, IDS etc.

REFERENCES RÉFÉRENCES REFERENCIAS

1. Rfc for Mobile Ad hoc Networks (MANET), "http://www.ietf.org/html.charters/manetcharter.html 1997".
2. Elizabeth M. Royer, (1999), "A Review of Current Routing Protocols for Adhoc Mobile Wireless Networks," International Journal Personal

- Communication, IEEE Computer Society, Volume: 6, Issue: 2.
3. Nagham H. Saeed, Maysam F. Abbod, Hameed Al-Raweshid, (2012), "Manet Routing Protocols Taxonomy," Proc. of International Conference Future Communication Networks (ICFCN), IEEE Computer Society, pp. 123-128.
4. Norsuzila Yaaco, Nurhazwani Rosli, Azita Laily Yusof, Mohd Tarmizi Ali, (2013), "Investigate the Performance metrics of Mobile Adhoc Networks (MANET)," International Symposium Wireless Technology and Application (ISWTA), IEEE Computer Society, pp. 22-25.
5. C. E. Perkins, E. M. Royer., (1999), "Ad-hoc On-Demand Distance Vector Routing," Proc. of 2nd International Conference on Mobile Computing System and Applications, IEEE Computer Society, New Orleans, LA, pp. 90-100.
6. Elizabeth M. Royer, Charles E. Perkins, (2000), "An Implementation Study of the AODV Routing Protocol," Proc. of International Conference on Wireless Communication and Networking, (Volume: 3).
7. Rfc for Adhoc on Demanding Routing Protocol, "http://www.ietf.org/rfc/rfc4728.txt.aodvr".
8. Jiao wen-cheng, PENG Jing, ZHENG, (2010), "Research and Improvement of AODV Protocol in Adhoc Network," Proc. of 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), IEEE Computer Society, pp. 23 – 28.
9. Umesh Kumar Chaurasi, Mrs. Varsha Singh, (2013), "MAODV: Modified Wormhole Detection AODV Protocols," Proc. of 6th International Conference on Contemporary Computing (IC3), IEEE Computer Society, pp. 239 – 243.
10. Rfc for Dynamic Source Routing, "http://www.ietf.org/rfc/rfc4728.txt.dsr".
11. Ana Cavalli, Cyril Grepel, Stephane Maag , Vincent Tortajada, (2004) , "A Validation Model for the DSR Protocol," Proc. of 24th International Conference on Distributed Computing, IEEE Computer Society.
12. Rfc for Zone Routing Protocols, "http://tools.ietf.org/html/draft-ietf-manet-zone".
13. Prasun Sinha, Srikanth V. Krishnamurthy, Son Dao, (2000), "Scalable Unidirectional Routing with Zone Routing Protocol (ZRP) Extensions for Mobile Ad-Hoc Networks," Proc. of International Conference on Wireless Communications and Networking, IEEE Computer Society, (Volume: 3).
14. Prasun Sinha, Srikanth V. Krishnamurthy, Son Dao, (2000), "Scalable Unidirectional Routing with Zone Routing Protocol (ZRP) Extensions for Mobile Ad-Hoc Networks," Proc. of International Conference on Wireless Communications and Networking, IEEE Computer Society, (Volume: 3).
15. Rfc for Fisheye State Routing Protocols, "https://tools.ietf.org/html/draft-ietf-manet-fsr-03".
16. Rfc for Routing Protocol Performance Issues and Evaluation Considerations, "https://www.ietf.org/rfc/rfc2501.txt"



Performance Study of Cryptography Based Dynamic Multi-Keyword Searchable Security Algorithm in Cloud using CRSA /B+ Tree

By Prasanna B T & C B Akki

East Point College of Engineering and Technology, India

Abstract- Today, Cloud computing is a buzz word in IT industry. Cloud, a shared pool of computing resources, allows access to needed resources on demand through internet and web applications. Since data is outsourced to third party, user needs to maintain the accountability of their data in cloud. Hence preserving the confidentiality and securing the sensitive data in cloud is a major concern. Many cryptographic techniques have been proposed by researchers to assure the confidentiality of the user's data in cloud. But, the challenging task is to provide the secure search over this preserved data which has been encrypted so as to retrieve the effective data. Hence, we are proposing a system to have a secure search over the encrypted data on the cloud which preserves its confidentiality. In our system, a noble approach has been made using the Commutative-RSA algorithm, a cryptographic technique where the dual encryption takes place thus reducing the overall computation overhead. The search operation over the encrypted data is based on the tree search algorithm which supports multi-keyword search. Based on the relevance score, the more appropriate data is retrieved on the search operation. Using this approach, the information is not leaked when the encrypted data is searched by users and also the queries are handled in an efficient way. Finally, we demonstrate the effectiveness and efficiency of the proposed schemes through extensive experimental evaluation.

Keywords: cloud, searchable encryption, CRSA, B+ tree.

GJCST-E Classification : C.2.0



Strictly as per the compliance and regulations of:



RESEARCH | DIVERSITY | ETHICS

Performance Study of Cryptography Based Dynamic Multi-Keyword Searchable Security Algorithm in Cloud using CRSA /B+ Tree

Prasanna B T^α & C B Akki^σ

Abstract- Today, Cloud computing is a buzz word in IT industry. Cloud, a shared pool of computing resources, allows access to needed resources on demand through internet and web applications. Since data is outsourced to third party, user needs to maintain the accountability of their data in cloud. Hence preserving the confidentiality and securing the sensitive data in cloud is a major concern. Many cryptographic techniques have been proposed by researchers to assure the confidentiality of the user's data in cloud. But, the challenging task is to provide the secure search over this preserved data which has been encrypted so as to retrieve the effective data. Hence, we are proposing a system to have a secure search over the encrypted data on the cloud which preserves its confidentiality. In our system, a noble approach has been made using the Commutative-RSA algorithm, a cryptographic technique where the dual encryption takes place thus reducing the overall computation overhead. The search operation over the encrypted data is based on the B+ tree search algorithm which supports multi-keyword search. Based on the relevance score, the more appropriate data is retrieved on the search operation. Using this approach, the information is not leaked when the encrypted data is searched by users and also the queries are handled in an efficient way. Finally, we demonstrate the effectiveness and efficiency of the proposed schemes through extensive experimental evaluation.

Keywords: cloud, searchable encryption, CRSA, B+ tree.

1. INTRODUCTION

Cloud computing is getting popularity because of its user friendly nature. IT industry leaders believe that cloud will change the approach of IT business. Reduced cost for storing data in and retrieving data from cloud is the biggest driver for its expected growth. This technological methodology can save a lot of infrastructure cost. Pay-as-you-use model can also be offered through the cloud computing solutions. According to Gartner Inc. Cloud computing is a disruptive technology, with the potential to make IT organizations more responsive than ever [8]. Cloud computing promises scalability, reliability, flexibility, availability and security of data along with economic advantages to the end user. Through web based applications one can access the shared resources from cloud on demand. IDC India lead analyst (software and services research), Kamal Vohra in an interview with

leading paper during 2010 quoted, "The most attractive feature of this new technology is the prospect of converting large, upfront capital investments in IT infrastructure into smaller, manageable 'pay-per-use' annuity payments." In 2013 IDC in a press release revealed that spending on public IT cloud services will reach \$58.4 billion in 2015 and is expected to be more than \$107 billion in 2017. Over the 2013–2017 forecast period, public IT cloud services will have a compound annual growth rate (CAGR) of 23.5%, five times that of the industry overall. Software as a service (SaaS) will remain the largest public IT cloud services category, capturing 59.7% of revenues in 2017. IDC predicts that by 2017, 80%+ of new cloud apps will be hosted on six PaaS platforms [1].

Along with benefits, cloud computing also has its own challenges and issues that need to be tackled. International Data Corporation (IDC) identified some of major challenges in cloud like Security, Performance, Availability, Integration and Cost. Among other challenges mentioned, privacy and security of data in cloud is the prime most concern where in research community needs to look in. Since cloud is basically based on a trust model, where client and provider must trust each other, we need to consider the issues related to security before making cloud a successful technology. Constant efforts have been put to ensure the privacy and confidentiality of the data at rest since long time.

Access to physical resources like servers is not under the control of an organization that outsources data on to the cloud for storage [18]. This in turn makes organization sensitive data vulnerable to risk [4] [19] [5]. Data in the cloud is typically in a shared environment along with the data from other resources. Cryptography is one effective way of securing user data in cloud. Before the data is been hosted or stored onto the cloud, the sensitive data is encrypted to protect the data privacy [2]. To preserve privacy many techniques in the literature have been proposed to carry out work on encrypted data. In [23][24][25], extensive literature review has been done. Most of the research on encrypted data is concentrated on homomorphic encryption (HE) and searchable encryption (SE) techniques. The mathematical complexity involved in designing homomorphic encryption methods led

Author α σ: e-mail: prasi.bt@gmail.com

researchers to concentrate on searchable encryption methods. Searchable encryption schemes work on encrypted data at rest and perform search operation on encrypted data. There may be situations, where in an organization the end users may have to perform the search operation on the daily basis for their business needs which also may involve some queries or multiple-keyword [17] to search in a huge set of cloud data. As a result, privacy assured multiple-keyword search operation over the encrypted data must be performed in the cloud data which assures that the sensitive data is not leaked [16]. The existing Multi Ranked Keyword Searchable Encryption (MRSE) mechanism [6] is not able to process the performance of system where the computation is more.

The need for efficient high performance multi-keyword search over the encrypted cloud data which assures privacy is evident. Thus, here we aim at providing such mechanism in the cloud in an efficient way so that the most relevant document is retrieved. Achieving this is a challenging task. Due to the complexity of both, preserving the data and secure multi-keyword search, the methods we have proposed here is organised in an adaptive manner. A novel technique like commutative RSA algorithm for the encryption of document can be used to preserve privacy/security of the data. This enables the cloud service to efficiently process the encryption method on the documents to be outsourced on cloud which also proves through extensive tests that this approach is dynamic.

Now the cloud service should perform the search operation on the encrypted data in an efficient way, so as to retrieve only the particular data. Here we propose the tree search algorithm due to its performance, system usability and scalability which enables data users to find the most relevant information quickly, rather than in a group of retrieved documents [3]. The search operation is performed by the two main cloud workers. One worker is in charge of constructing the tree structure where each block (node) of data chunks represents whether corresponding keyword is contained in the document. The other worker takes care of the query keyword search on the tree based with the relevance score. The search result of the query represents whether corresponding keyword appears in this search data request, so the similarity could be exactly measured by the data chunks based on the query. The analysis of effectiveness of the privacy and efficiency of the proposed system is performed. Hence, the experimental result proves the low computational overhead and the high efficiency.

The research paper is organized as follows. Section II discusses the related work. A brief note on the Commutative-RSA along with the working of search operation based on tree is discussed in section III. Section IV discusses the search framework on Azure

platform using tree. The analysis is done in section V. The experimental results and comparisons are presented in section VI, to prove the efficiency of our proposed system. The concluding remarks and references are provided in the last VII and VIII sections of the paper respectively.

II. RELATED WORK

More research has been done in privacy preserving single-keyword and multi-keyword search on encrypted data in cloud. In [5], a practical symmetric searchable encryption method is proposed for the first time. The first public key encryption with keyword search (PEKS) was proposed by in [15]. In [7] [9] [10] [11] [12] [13] [15] [20] extensive research has been done to make searchable encryption practical. Later, the schemes in [6] [22] use multi keyword search technique for search.

In [23] [24] [25], authors have discussed about the different techniques used to work on encrypted data, extensive survey of different searchable and homomorphic encryption schemes with their benefits and limitations.

To overcome all these issues, we have proposed a system of privacy preserving multiple-keyword ranked search over encrypted cloud data which is secure and has efficient search method. Thus, a high performance security model with multi-keyword search evaluation mechanism is proposed.

III. PROBLEM FORMULATION

Searchable Encryption (SE) schemes maintain the confidentiality and privacy of owner's data by facilitating searching keywords directly on encrypted data. Users can upload their encrypted data to cloud. Later, the authorized users can perform private keyword search on encrypted data in cloud. Multiple domains like cryptography, indexing, storage etc. are involved in devising efficient, secure, SE algorithms over encrypted files. The participants of a secure search model in a cloud, typically involves data owner, data user and cloud server. Data owner encrypts the files and corresponding keywords based index files by using any known cryptographic algorithms. Both the encrypted files and index files are uploaded to the cloud server. The trapdoors (encrypted keywords) are used to search encrypted files by cloud server in cloud database.

a) System Model

Our system consists of 3 entities data owner, data user and the cloud server as shown in Figure 1.

1. Data owner encrypts the data files for securing the data in cloud using Commutative RSA (CRSA) before uploading into the cloud. They also define the access rights for the user who want to access those documents. The access right is a 2-state variable: permission granted or permission denied.

Data owner creates an index tree based on B tree and encrypts the tree using CRSA.

2. Cloud server stores the encrypted data files and encrypted index tree. It accepts the encrypted keywords (trapdoor) and returns the matching data file based on their relevance.
3. Data user can search for encrypted data files in cloud with encrypted keywords (trapdoor). The purpose of using encrypted keywords is that even the cloud server must not be able to infer the contents of data files.

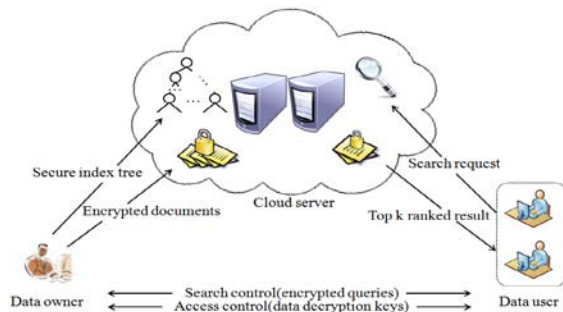


Figure 1 : Searchable Encryption Architecture using CRSA

b) Design Goals

The proposed solution addresses the following requirements

1. The search on encrypted document/file must be fully secure and cloud server must not be able to infer the contents of the documents in any way.
2. The search results must be ranked in order of relevance.

To enable ranked searchable encryption for effective utilization of outsourced and encrypted cloud data under the aforementioned model, our system design should achieve the following security and performance guarantee. Specifically, we have the following goals: 1) Ranked keyword search: to explore different mechanisms for designing effective ranked search schemes based on the existing searchable encryption framework; 2) Security guarantee: to prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the “as-strong-as-possible” security strength compared to existing searchable encryption schemes; 3) Efficiency: above goals should be achieved with minimum communication and computation overhead.

i. Existing systems

Existing searchable encryption schemes [6] [15] [38] allow a user to securely search over encrypted data through keywords. These techniques support multi keyword search. The similarity measure “coordinate matching” in MRSE [6] has some drawbacks when used to evaluate the document ranking order. First, it takes no account of term frequency i.e. any keyword appearing in

a document will present in the index vector as binary value 1 for that document, irrespective of the number of its appearance. Obviously, it fails to reflect the importance of a frequently appeared keyword to the document. Second, it takes no account of the term scarcity. Usually a keyword appearing in only one document is more important than a keyword appearing in several ones. In addition, long documents with many terms will be favored by the ranking process because they are likely to contain more terms than short documents. Hence, due to these limitations, the heuristic ranking function, “coordinate matching”, is not able to produce more accurate search results. More advanced similarity measure should be adopted from plaintext information retrieval community. On the other hand, the search complexity of MRSE is linear to the number of documents in the dataset, which becomes undesirable and inefficient when a huge amount of documents are present.

ii. Proposed system

For our system, we choose the B+-tree as indexing data structure to identify the match between search query and data documents. Specially, we use inner data correspondence, i.e., the number of query keywords appearing in document, to evaluate the similarity of that document to the search query. Each document is converted to a balanced B+-tree according to the keywords and encrypted using CRSA. Whenever user wants to search, he/she creates a trapdoor for the keywords. Our aim is to design and analyze the performance of multiple-keyword ranked search scheme using Commutative RSA algorithm and B+ tree data structure for searchable index tree.

We designed a scheme based on secured ranked multiple-keyword search over encrypted cloud data using CRSA. Further, we analyzed its performance over B+ tree based searchable index tree. In [6] [38], authors have studied the performance of RSA algorithm on binary tree. We have used Microsoft's Azure platform to emulate the proposed system and to study its performance.

c) Preliminaries

i. Commutative Encryption (CRSA)

The RSA cryptosystem is one of the optimum public key cryptography approaches. However, its overall robustness gets limited due to one way encryption and majority of existing RSA schemes suffer from reorder issues. Therefore, in order to make this system least complicated and more efficient, an approach called Commutative RSA has been proposed. In this scheme, the order in which encryption has been done would not affect the decryption if it is done in the same order. Encryption is the standard method for making a communication private. With the many cryptographic approaches, our system follows the commutative RSA algorithm. The mathematical scheme

for performing this encryption is described by a pseudo algorithm presented below.

Let us consider two prime numbers $Prime_{p_p}^{CRSA}$ and $Prime_{Q_q}^{CRSA}$ initialized amongst all the group members. Let G_A and G_B represent the group members required to communicate over the documents. To compute the encryption keys and decryption key pairs of the commutative RSA algorithm the parameters $Param_{N_p}^{CRSA}$ and $Param_{\phi_p}^{CRSA}$ are computed using the following

$$Param_{N_p}^{CRSA} = [(Prime_{p_p}^{CRSA}) \times (Prime_{Q_q}^{CRSA})]$$

$$Param_{\phi_p}^{CRSA} = [(Prime_{p_p}^{CRSA} - 1) \times (Prime_{Q_q}^{CRSA} - 1)]$$

From the above equations it is clear that

$$Param_{N_X}^{CRSA} = Param_{N_Y}^{CRSA} \text{ and}$$

$$Param_{\phi_X}^{CRSA} = Param_{\phi_Y}^{CRSA} \text{ for } X \text{ and } Y.$$

The encryption key pair of X and Y are represented as $(Param_{N_X}^{CRSA}, Param_{E_X}^{CRSA})$ and $(Param_{N_Y}^{CRSA}, Param_{E_Y}^{CRSA})$ is to be obtained.

The $Param_{E_p}^{CRSA}$ is obtained by randomly selecting numbers such that it is a co-prime of $Param_{\phi_p}^{CRSA}$ or in other terms

$$\mathcal{F}n_{GCD}(Param_{E_p}^{CRSA}, Param_{\phi_p}^{CRSA}) = 1$$

Where $\mathcal{F}n_{GCD}(u, v)$ represents the greatest common divisor function between two variables u and v .

The decryption key pair of X and Y is represented by $(Param_{N_X}^{CRSA}, Param_{D_X}^{CRSA})$ and $(Param_{N_Y}^{CRSA}, Param_{D_Y}^{CRSA})$ and the parameter $Param_{D_p}^{CRSA}$ is computed based on the following equation

$$Param_{D_p}^{CRSA} = (Param_{E_p}^{CRSA})^{-1} \text{ Mod}(Param_{N_p}^{CRSA})$$

Let Enc_U represent the encrypted data U . The encryption operation is defined as follows

$$Enc_U = U^{Param_{E_p}^{CRSA}} \text{ Mod}(Param_{N_p}^{CRSA})$$

The commutative RSA decryption operation on the encrypted data V is defined

$$Dec_V = V^{Param_{D_p}^{CRSA}} \text{ Mod}(Param_{N_p}^{CRSA})$$

ii. B+ Tree

A B+ tree is a data structure as shown in Figure 2. The tree contains index nodes and leaf nodes. All leaf nodes are at the same level (same depth). Each index nodes contain only keywords. Each node except root node in a B+-tree with order n must contain keys between n to $2n$ keys. Each node also contains (number of keys + 1) pointers to its child nodes. If the root node is an index node then it must have at least 2 children. The insertion, deletion, search operations takes only logarithmic time. Due to high fan-out B+ tree reduces I/O operations time to search an element.

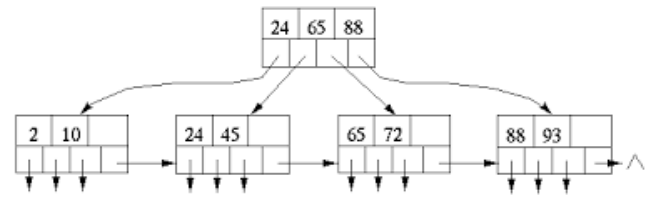


Figure 2 : B+ tree data structure

IV. B+TREE ALGORITHM SEARCH FRAMEWORK USING MICROSOFT WINDOWS AZURE

To enable effective, efficient and secure multi-keyword ranked search over encrypted cloud data under many models, our mechanism is aiming to achieve the following design goals. The proposed framework is mainly on the tree which is index format, hence balanced binary search trees. In this section, we define the framework of multi-keyword ranked search over encrypted cloud data and establish various strict system-wise privacy requirements for such a secure cloud data utilization system.

The Cloud service architecture (CSA) chosen enable us to realize the framework using a modularized approach. The CSA shown in Figure 3 could be considered as a complex system of $p : q$ dependencies, where p represents the services offered and q represents the applications offered by the CSA system. In CSA an application may need multiple service offerings or varied applications need similar services or similar applications may be provided by varied services. The searchable encryption utilizes a similar application of keyword search provided by the n workers hence it could be said that the searchable encryption depends on the availability of the keyword search application offered by the n workers. Multi-keyword search management tends to be cumbersome if it is done manually. In order to automate the multi-keyword search management we need a common syntax and a common searchable encryption to interoperate. The Commutative RSA have standardized the syntax definition through the searchable encryption.

Let us consider a set of all multi-keyword search S_K defined as

$$S_K = \{s_{k_1}, s_{k_2}, s_{k_3}, \dots, s_{k_a}\}$$

where s_{k_a} represents the a^{th} search keyword. The s_{k_a} is a keyword derived from both the encrypted tree data $r_{k_a} \in R_K$ from tree search algorithm (TSA) and the encrypted keyword contents $o_{k_a} \in O_K$ from the encrypted tree data R_K of the TSA. In other words

$$s_{k_a} = f_k(r_{k_a}, o_{k_a})$$

where $o_{k_a} = f_0(R_K, r_{k_a})$, f_0 represents the tree builder function.

The tree builder function extracts all the related keywords of r_{k_a} present in the encrypted tree data R_K of the TSA.

The B^+ tree represents a complex CSA hence the encrypted tree data R_K data set is available with

$$R_K = \{r_{k_{11}}, r_{k_{12}}, \dots, r_{k_{1a}}\} \cup \{r_{k_{21}}, r_{k_{22}}, \dots, r_{k_{2a}}\} \cup \dots \dots \{r_{k_{n1}}, r_{k_{n2}}, \dots, r_{k_{na}}\}$$

The encrypted keyword contents extracted from the encrypted tree data could be defined as

$O_K = O_{K1} \cup O_{K2} \cup \dots \cup \dots \dots O_{Kn}$, where O_{Kn} the encrypted set available with n^{th} search service provided by the worker. The locally available encrypted data could be defined as $O_{Kn} \propto R_K$

From the above definition it is clear that encrypted data available with search service n provided by the worker may not contain all the possible keywords as the complete encrypted tree data set R_K is unavailable with the n^{th} search. This is the problem that exists in the current search deployments available [9]. The purpose of the B^+ tree is to overcome the short comings by using efficient searching algorithms and search encryption compositions.

a) Cloud Workers

The workers provide search encryption services which support the multi-keyword search application. The workers are defined as $WR = \{Wr_1, Wr_2, Wr_3, \dots, \dots, Wr_n\}$, where Wr_n is the n^{th} search provided by the worker. The system architecture of the azure cloud search over an encrypted data by the worker is shown in Figure 1. Each search provided by the worker possess the encrypted tree data based documents. The encrypted tree data records could be represented as $R_{KB} = \{rkb_1, rkb_2, rkb_3, rkb_4, \dots, \dots, rkb_r\}$, where rkb_r is the r^{th} encrypted tree data record available with the azure cloud search provided by the worker $Wr_n \in WR$ on the n^{th} search.

The encrypted tree data records are said to consist of triplets. Based on the record, rkb_r could be represented as $rkb_r = \langle trkb_{r_{sub}}, trkb_{r_{prd}}, trkb_{r_{obj}} \rangle$ where $trkb_{r_{sub}}$ is the subject triplet, $trkb_{r_{prd}}$ is the predicate triple and $trkb_{r_{obj}}$ represents the object triplet.

The keywords extracted from the encrypted tree data include some complex relations that cannot be represented in encrypted tree data alone, hence the B^+ tree presented here adopts representation of the encrypted keyword contents through tree structure builder due to its benefits.

The data of the cloud search provided by the worker constitutes of both the encrypted tree data and encrypted keyword contents which are humongous in nature and size. A search executed on huge databases would affect the response times due to numerous disk

n^{th} search service provided by the workers. The encrypted tree data can be defined as

$$R_K = R_{K1} \cup R_{K2} \cup R_{K3} \cup \dots \dots R_{Kn}$$

where $R_{K1} \neq R_{K2} \neq R_{Kn}$

read and disk write operations involved in the search operation. To compress the data and create cache the B^+ tree utilizes a hierarchical data ordering algorithm.

b) Azure Cloud Search Application

The search application is a user interface which accepts user search queries represented by SS_Q . The B^+ tree search algorithm accepts logical, conditional and simple term based search queries. The response of the search is represented as SS_R . The cloud search application provides the search responses SS_R by using cloud search service composition techniques. The search response not only consists of search responses but additionally provides the encrypted relevance score used in ranking the search responses i.e. higher the encrypted relevance score greater is the rank of the search response. The encrypted data are constructed after consuming the search services provided by the n search service. These are provided by the search application from the cloud worker. The encrypted data are constructed by the possible keywords obtained after the cloud search service composition. This enables the B^+ tree search algorithm to provide better search results and overcome the drawback currently discussed in the previous section of this paper.

Let us consider search keyword set S_K and two keywords $s_{k_x} \in S_K$ and $s_{k_y} \in S_K$. There exists 4 possible relations amongst keywords s_{k_x} and s_{k_y} . The possible relations could be defined by using the subsume represented by Sb_{sum} and defined as

$Sb_{sum} : (S_K \times S_K) \mapsto \{T, F\}$, where T represents the conditional true relation and F represents a conditionally false relation. Using the above definition we could define the first possible relation between the keywords s_{k_x} and s_{k_y} as $Sb_{sum}(s_{k_x}, s_{k_y}) = T$ holds if and only if the search keyword s_{k_x} is a generalization of the search keyword s_{k_y} . It could be stated that the search keyword s_{k_y} is a specialization of the search keyword s_{k_x} .

$Sb_{sum}(s_{c_y}, s_{c_x}) = T$ holds if and only if the search keyword s_{k_x} is a generalization of the search keyword s_{k_y} . It could be stated that the search keyword s_{k_y} is a specialization of the search keyword s_{k_x} .

If the search keywords s_{k_x} and s_{k_y} are not related then $Sb_{sum}(s_{k_x}, s_{k_y}) = F$ and $Sb_{sum}(s_{k_y}, s_{k_x}) = F$.

If the search keywords s_{k_x} and s_{k_y} are equal then $Sb_{sum}(s_{k_x}, s_{k_y}) = T$ and $Sb_{sum}(s_{k_y}, s_{k_x}) = T$.

The generalization, specialization and the subsume Sb_{sum} relations are transitive.

Let us consider a parameter p_x of the search service provided by the worker Wr_x and a parameter p_y of the search service provided by the worker Wr_y . If the parameters $p_x = p_y$, then the cloud search service could be called if only $Sb_{sum}(Wr_x, Wr_y) = T$. It could also be stated that the parameter p_x requires less or equal data than the parameter p_y . For the cloud search service composition required, there is no requirement for a demarcation amongst the keywords and the search keywords. Let's define a set of cloud search services available with the search application as follows

$$Sws_{Wr} = \{sws_{Wr_1}, sws_{Wr_2}, \dots, sws_{Wr_n}\}$$

Where sws_{Wr_n} represents the n^{th} cloud search service offered by search service provided by the worker Wr_n .

$$Comp_{Sws}(Sws_{Wr}) \leftrightarrow \forall X \in ss_{Q_{Wr_1}} \exists Y \in SS_{Q_{Wr}} : Sb_{sum}(X, Y) \wedge \forall X \in ss_{Q_{Wr_z}}, z \in \{2, 3, \dots, n\} \\ \exists Y \in SS_{Q_{Wr}} \cup ss_{R_{Wr_{z-1}}} \cup \dots \cup ss_{R_{Wr_1}} : Sb_{sum}(X, Y) \wedge \forall X \in ss_{R_{Wr_1}} \cup \dots \cup ss_{R_{Wr_n}} \cup SS_{Q_{Wr}} : Sb_{sum}(X, Y)$$

Let f_{SSWS} represent a service provided by worker on search function based on a keyword S_K which provides all the set of cloud search services available defined as

$$\forall s_{k_a} \in f_{SWr}(S_C) \exists ss_{R_{Wr_a}} \in SS_{R_{Wr}} : Sb_{sum}(S_C, ss_{R_{Wr_a}})$$

The search application is an interface which provides the search criteria to the composed services, the results obtained are then there by provided to the user. On receiving the user's search query SS_Q the application of the B^+ tree search algorithm performs the cloud services search function f_{SSWS} . The cloud service offerings amongst the varied workers are obtained by the process invoked by the f_{SSWS} . Based on the cloud services offered and the user query, appropriate cloud services are selected. The selected cloud service offerings Sws_{Pr} are composed using the cloud search service composition function $Comp_{Sws}(Sws_{Pr})$. On completing the composition, the cloud search services are invoked by parsing the required user parameters SS_Q . The results obtained are aggregated and ranked, based on the encrypted relevance score. Higher is the encrypted relevance score, higher is the rank. The ranking could be easily achieved using any sorting algorithm.

Let the cloud search response set be defined as

$SS_R = \{ss_{R_{Wr_1}}, ss_{R_{Wr_2}}, ss_{R_{Wr_3}}, \dots, ss_{R_{Wr_n}}\}$, where $ss_{R_{Wr_n}}$ represents the search response received from the n^{th} search service by the worker for a given query set SS_Q .

Each cloud search service offered by search worker Wr_n required a set of inputs denoted as $ss_{Q_{Wr_n}}$ and if the set of inputs is provided in an orderly fashion the cloud search service provides a set of output keywords denoted by $ss_{R_{Wr_n}}$ and $ss_{R_{Wr_n}} \in S_K$. The efficient ranked keyword search cloud service composition algorithm discovers the cloud search services available on Sws_{Wr} . On successful execution of the cloud search service execution algorithm, the next cloud search service i.e. sws_{Wr_2} could be processed only if the execution of the previous sws_{Wr_1} (provided with the input parameters $ss_{Q_{Wr_1}}$ and the output keywords $ss_{R_{Wr_1}}$ are obtained in response) is processed successfully. Let the ranked keyword search cloud service composition be represented as $Comp_{Sws}(Sws_{Wr})$ then the cloud search service composition is said to successfully process all the requests if

$$f_{SWr}(S_C) = Sws_{Wr}$$

Also it could be stated that

As stated earlier the search algorithm available at the worker's end, provides the result page information, the encrypted data behind the search and the encrypted relevance score (ranked data). Based on this argument $ss_{R_{Wr_n}}$ could be defined as

$$ss_{R_{Wr_n}} = \{r_1 ss_{R_{Wr_n}}, r_2 ss_{R_{Wr_n}}, r_3 ss_{R_{Wr_n}}, \dots, r_m ss_{R_{Wr_n}}\},$$

where $r_m ss_{R_{Wr_n}}$ represents the m^{th} search result received from the n^{th} search service by the worker for a given query set SS_Q .

The cloud service composition is an important entity of the cloud search application. The next section of this paper discusses the B^+ tree search algorithm utilized in composing the cloud services Sws_{Wr} offered by the n search service provided by the worker.

c) Cloud Service Composition Using B^+ Tree Search Algorithm

The search framework B^+ tree search algorithm introduced in this system utilizes the B^+ tree search algorithm for cloud service composition. The B^+ tree search algorithm is selected for the sole purpose of quicker responses it offers and it is computationally lighter when compared to other cloud service composition algorithms. The cloud service composition function introduced in the earlier section of this paper

$Comp_{Sws} (Sws_{Wr})$ receives the set of cloud services Sws_{Wr} over which the composition has to be performed. The cloud services composition is performed using the B^+ tree search algorithm.

Let us define a function f_{SWS-DS} which performs the B^+ tree search algorithm is defined as

The f_{SWS-DS} is solved by the following algorithm

Step 01: START

Step 02: For Each $Var_1 \in ss_R$

Step 03: For Each $sws_{Wr} \in f_{SWr}(S_K) = Sws_{Wr}$

Step 04: Initialization $ss_{Rtmp} = ss_R$

Step 05: For Each $Var_2 \in ss_{Rtmp}$

Step 06: IF $\exists Var_3 \in ss_{Wr} : Sb_{sum}(Var_2, Var_3)$

Step 07: $ss_{Rtmp} = ss_{Rtmp} / Var_2$

Step 08: End IF

Step 09: End For Each

Step 10: For Each $Var_4 \in ss_{Qtmp}$

Step 11: IF $\exists Var_5 \in ss_{QWr} : Sb_{sum}(Var_4, Var_5)$

Step 12: $ss_{Rtmp} = ss_{Rtmp} \cup Var_4$

Step 13: End If

Step 14: End For Each

Step 15: $sws_{tmp} = sws_{Wr} \oplus Sws_{tmp}$

Step 16: IF $ss_{Rtmp} = \{\}$

Step 17: Return sws_{tmp}

Step 18: End IF

Step 19: ELSE

Step 20: IF $d_c < d_{max}$

Step 21: $ss_{Rtmp} = f_{SWS-DS}(ss_Q, ss_{Rtmp}, sws_{tmp}, d_c + 1)$

Step 22: End IF

Step 23: IF $sws_{tmp} \neq \{\}$

Step 24: Return sws_{tmp}

Step 25: End IF

Step 26: End ELSE

Step 27: End For Each

Step 28: End For Each

Step 29: Return $\{\}$

Step 30: END

Where $Var_1, Var_2, Var_3, Var_4, Var_5$ represent temporary processing variables and d_{max} represents the maximum depth.

Step 01: START

Step 02: Initialization $d_{max} = 2$

Step 03: DO

Step 04: $Sws_{tmp} = f_{SWS-DS}(ss_{QWr_n}, ss_{RWr_n}, \{\}, 1)$

Step 05: $d_{max} = d_{max} + 1$

Step 06: While $Sws_{tmp} \neq \{\}$

Step 07: END

$f_{SWS-DS}(ss_Q, ss_R, Sws_{tmp}, d_c) = sws$, where ss_Q represents the input query set, ss_R is the desired response, Sws_{tmp} represents the current temporary cloud services identified, d_c represents the height and sws represents the resultant cloud service identified.

The cloud service composition function denoted by $Comp_{Sws}(Sws_{Wr})$ is realized using the following algorithm

provided by the worker offering the cloud search services to support the search application.

The CSA architecture considered for the B⁺tree search algorithm is described in this section. The B⁺tree search algorithm is designed to provide appropriate search responses. The B⁺tree search algorithm relies on the encrypted tree data and the encrypted keyword contents housed as the encrypted data component of the cloud service provided by the worker for provisioning of the search responses. The cloud search services offered by the worker are composed using the B⁺tree search algorithm.

The encrypted keyword contents of r encrypted tree data records is defined as

$$O_{KB} = \{okb_1, okb_2, okb_3, okb_4, \dots \dots \dots okb_r\}$$

Let the cache of a keyword s_{k_a} which represents the a^{th} search keyword be represented as $Cache_{s_{k_a}} = \langle s_{k_a}, r_{k_a}, e_{k_a} \rangle$, where r_{k_a} is the number of relations of the keyword and e_{k_a} represents the number of edge keywords.

It is evident that greater the number of keywords and greater the relations that exist, larger is the data size and increasing the number of disk operation for the search operation. The number of occurrences of a keyword in an encrypted data is directly proportional or equivalent to the number of relations r_{k_a} of a keyword. Also it can be stated that for a constant m is equivalent to a function of the number of relations (f_{num_r}) r_{k_a} of a keyword s_{k_a} and a function of the tree depth (f_{edg_dpth}) of a keyword s_{k_a} .

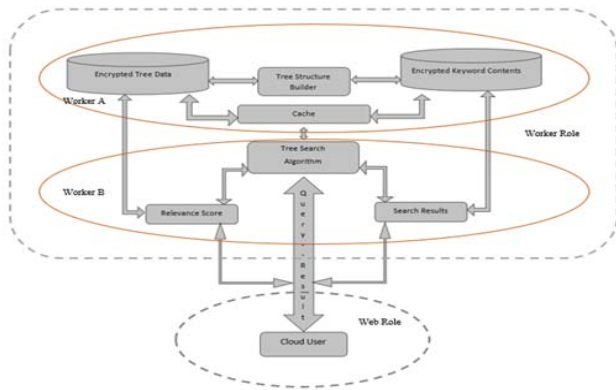


Figure 3 : System Architecture of Azure Cloud search over encrypted data

$$ACost_{Cache} = \sum_{\{r_{k_a} : f_{num_r}(r_{k_a}) \leq t\}} f_{num_r}(r_{k_a}) \approx \int_{S_{Util}/t}^{S_{Util}} \frac{S_{Util}}{f_{edg_dpth}} df_{edg_dpth} = S_{Util} \ln t$$

where $f_{num_r}(r_{k_a}) \leq t \leftrightarrow f_{edg_dpth}(r_{k_a}) \geq S_{Util}/t$

The probability of $AProb$ finding the keyword s_{k_a} in the encrypted data is defined as

$$f_{num_r}(r_{k_a}) \times f_{edg_dpth}(r_{k_a}) \approx m$$

Also

$$r_{k_a} \approx \sum_{x=1}^{x=m} m/x \approx m \int_{x=1}^{x=m} 1/x dx = m \ln m$$

From the above equation it is clear that even if the number of relations r_{k_a} of a keyword s_{k_a} increases, the cache size does not increase by a great extent. Generally the keywords require $2S_{Unit}$ cloud storage space per keyword (s_{k_a}). The space utilized in storing the cache defined above is given by

$$\sum_{r_{k_a}} (2 + f_{num_r}(r_{k_a})) \approx S_{Util} (2 + \ln S_{Util})$$

where S_{Util} is the cloud space required to store the same keyword s_{k_a} .

It is considered that only one entry of a s_{k_a} keyword is allowed in the cache. In order to compare the normal caching strategy with the caching strategy used in B⁺ tree search, the comparison ratio is defined as

$$\frac{2S_{Util} (1 + \ln S_{Util} / 2)}{2S_{Util} \ln S_{Util}} = 1/\ln S_{Util} + 1/2$$

Hence the proposed caching strategy improves the cloud storage space utilization by approximately 50%.

The azure cloud access cost for the caching strategy is defined as

The access time of the cache to search for a keyword s_{k_a} within the encrypted data with a probability $AProb_{Cache}$ is defined as

$$AProb_{Cache} = \ln t / \ln S_{Util}$$

$$ATime_{Cache} = AProb_{Cache} \log_b ACost_{Cache} + (1 - AProb_{Cache})(\log_b ACost_{Cache} + 1) = \log_b ACost_{Cache} + (1 - AProb_{Cache})$$

where b represents the branching factor of the encrypted tree.

The cache created based on the encrypted tree data and encrypted keyword content is encoded in a binary format for faster access.

The encrypted relevance score is a ratio between the query keyword and the response keyword based on the encryptions constructed. The encrypted relevance score is used by the Search Application in ranking the search responses received by the n search service provided by workers considered in the B^+ tree search.

The search query SS_Q could be defined as a set of keywords and relational operators. The search encrypted service offered supports queries containing Boolean operators like *AND, OR, NOT, +, -, ""* commonly available with the major search operation provided by the worker.

$$ss_Q = \langle s_{k_{ss_Q}}, R_{K_{ss_Q}} \rangle$$

The search query ss_Q could be represented as a $p \times q$ matrix where p represents the number of keywords queried for and q represents the number of relations, logical operators and special characters defined for querying amongst the p keywords.

The search response ss_R is a set of responses and the corresponding relevance score defined as

$$ss_R = \langle s_{R_{ss_R}}, ORS_{R_{ss_R}} \rangle$$

The search response ss_R could also be represented as a $r \times r$ matrix where r the number of responses obtained for the search query in ss_Q . The encrypted relevance score is defined as

$$ors_{R_{ss_R}}(ss_Q, ss_R) = \frac{\sum_r s_{r_{ss_R}}, ss_Q}{\|ss_Q\| \|s_r\|}$$

To represent the encrypted relevance score to a scale of 0 to 1, Normalization is considered in the B^+ tree search hence the encrypted relevance score could be defined as

$$ors_{R_{ss_R}}(ss_Q, ss_R) = s_{r_{ss_R}}', ss_Q, \text{ where } s_{r_{ss_R}}' = \frac{s_{r_{ss_R}}}{s_r}$$

The Azure cloud search provided by worker could be considered as the core of the B^+ tree search architecture. The worker discussed in this section not only rely on the encrypted tree data to provide effective search queries but also rely heavily on the encrypted keyword contents to provide effective and accurate search responses. The cloud search worker not only incorporates effective hierarchical caching strategies enhancing query response time but also provide relevant query responses. In addition to the query

responses, the search worker also provide encrypted relevance scores associated with each query responses enabling effective ranking when multiple cloud search response are composed.

V. PERFORMANCE ANALYSIS

The security of the designed system is provided by using CRSA. As long as private key (encrypted) is kept secret the cloud provider cannot deduce index tree or documents set. Since trapdoor is also encrypted using CRSA, the provider cannot make out the keywords inside the trapdoor maintaining the confidentiality at index and query level. The documents in cloud storage are also protected, since documents are encrypted using CRSA. Without having the decryption key it is highly hard to decrypt the documents thus provides security at storage level.

To be useful and usable, databases must support operations, such as search, deletion and insertion of data. For large organizations the databases are huge in size and cannot be maintained entirely in memory. By using balanced B+ trees to construct the index for the data we can improve the search efficiency. B+ tree minimizes the disk I/O (disk read and disk write) by copying a block of data (page) containing many records at a time into memory. This in turn improves the search efficiency. Asymptotically, Searching an unsorted database without indexing will have a worst case running time of $O(n)$, where n represents the number of keywords. If the same data is indexed with a B+ Tree, the same search operation will run in logarithmic time i.e $O(\log n)$.

VI. RESULT ANALYSIS

The privacy preserved multi-keyword search based on the encrypted cloud data is been implemented. The system model presented has been developed on Visual Studio 2010 framework 4.0 with C#. The overall system has been developed and implemented with Microsoft Azure platform.

Different parameters like computation overhead, computation time, and bytes overhead have been considered to study and compare the performance of our proposed scheme with existing scheme.

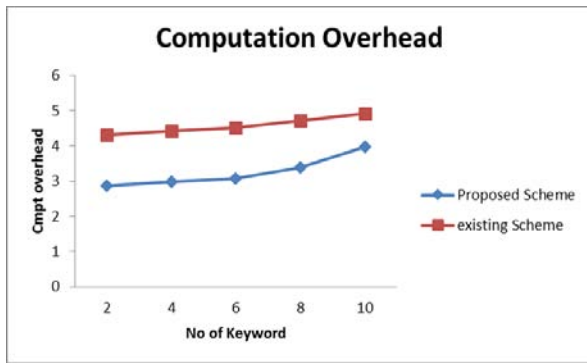


Figure 4 : Computation Overhead

Figure 4 depicts the computation overhead in seconds based on the number of keywords. In this study, we compared the performance of our proposed system with the existing system proposed in [15]. Results clearly show that even for 10 keywords, the overhead computation using CRSA is low as compared to the existing system [15]. For example, existing system takes approximately 4.5 seconds for searching 2 keywords, whereas our proposed CRSA based scheme takes only 3 seconds. The computation cost for search increases linearly in both schemes. But from Figure 4 it is evident that our proposed CRSA based scheme performs better even under increased number of keywords.

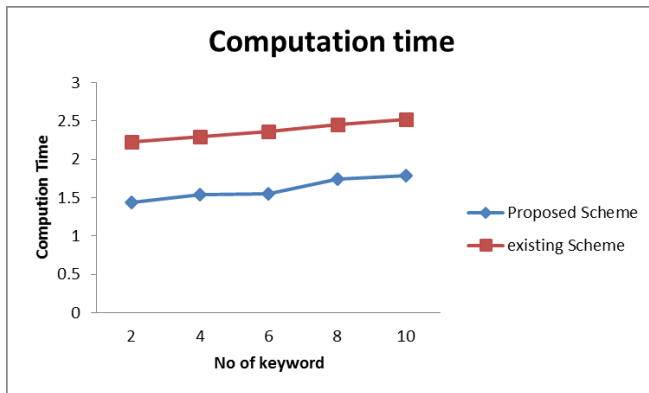


Figure 5 : Time Computation

The graph in Figure 5 plotted above makes the comparison of the search computation time in seconds of our proposed system against the existing system. For two keywords search, the time taken by the existing [15] scheme is approximately 2.5 seconds, whereas our proposed system takes approximately 1 seconds less. As the number of keywords increased for search, the computation time for search also increases linearly in both schemes. But CRSA based scheme is found to perform better. Thus it is evident that encryption algorithm CRSA with B+ tree as index tree performs better than RSA and B tree combination.

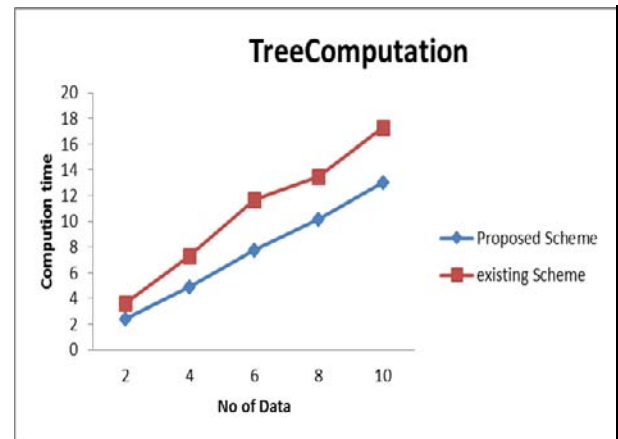


Figure 6 : Computation of Tree Structure

The graph in Figure 5 plotted above makes the comparison of the search computation time in seconds of our proposed system against the existing system [15]. For two files search, the time taken by the existing scheme is approximately 2.5 seconds, whereas our proposed system takes approximately 0.5 seconds less. As the number of data files increases, the computation time for search also increases linearly in both schemes. But B+ tree index based scheme is found to perform better. Thus it is evident that encryption algorithm CRSA with B+ tree as index tree performs better than RSA and B tree combination.

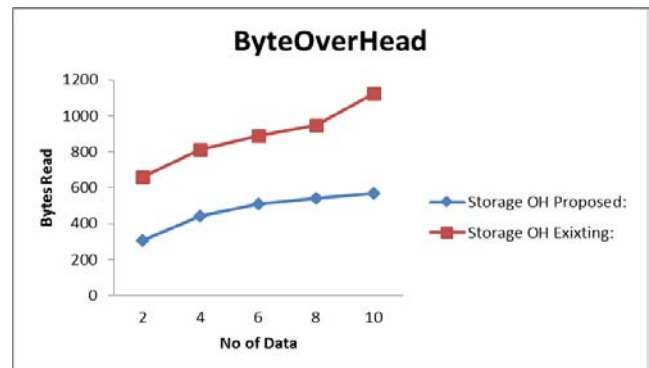


Figure 7 : Computation of Byte Overhead

The graph in Figure 7 portrays the overhead computation in bytes. For two data files the number of bytes read is around 200 bytes compared 600 bytes from existing system. As the number of data files increases the bytes read for search also increases linearly in both schemes. But CRSA/B+ tree based scheme is found to perform better.

Therefore from these results, we have established that the proposed model can be an effective, robust and optimum adaptable approach for privacy preserving multi-keyword search of encrypted data in cloud environment.

VII. CONCLUSION AND FUTURE WORK

The insights of privacy-assured searchable cloud data storage services are discussed. Despite the popularity of cloud services and their wide adoption by enterprises and governments, cloud providers still lack services that guarantee both data privacy and privacy preserving search operation on encrypted. Here we tried to address the security issues considering a large set of cloud data and users based on preserving the privacy of multi keyword search over an encrypted data. We have designed a cryptographic scheme using C-RSA and B+ tree. The B⁺tree search algorithm is adopted for the ranked search technique to fetch the relevance score so as to retrieve the similarity between the query keyword search performed by the cloud user and the documents which are outsourced on cloud. Detailed analysis which examines the privacy and search efficiency of our proposed model is given. The experimental results proves our proposed model induces low overhead on the overall system. Using the C-RSA, the computation overhead is much reduced which means, if any changes have to be made to the already encrypted documents, it can be easily done with the C-RSA technique which allows dual encryption hence proves it is dynamic, thus reducing the computation overhead compared to other cryptographic methods. Therefore, specifying the computation overheads and comparatively proving efficiency. Finally, we conduct comprehensive performance analysis, which shows that our scheme is more secure, efficient and practical than existing schemes.

The C-RSA cryptographic technique induces low computation overhead with the asymmetric key. This can further be improved with the use of ECC technique which proves much reduced computation overhead with the symmetric keys without compromising security.

REFERENCES RÉFÉRENCES REFERENCIAS

1. M. Armbrust et al., 'Above the Clouds: A Berkeley View of Cloud Computing,' Feb 2009.
2. S. Kamara and K. Lauter, 'Cryptographic cloud storage,' in RLCPS, January 2010, LNCS. Springer, Heidelberg.
3. A. Singhal, 'Modern information retrieval: A brief overview,' IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.
4. Cloud Security Alliance, 'Security Guidance for Critical Areas of Focus in Cloud Computing,' <http://www.cloudsecurityalliance.org>, 2009.
5. R. Brinkman, 'Searching in encrypted data,' in University of Twente, PhD thesis, 2007.
6. Ning Cao; Cong Wang; Ming Li; Kui Ren; Wenjing Lou, 'Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,' Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.1, pp.222,233, Jan. 2014.
7. Dawn Xiaoding Song; Wagner, D.; Perrig, A., 'Practical techniques for searches on encrypted data,' Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, doi: 10.1109/SECPRI.2000.848445 vol., no., pp.44,55, 2000.
8. J. Li et al., 'Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,' Proc. IEEE INFOCOM '10 Mini-Conf., San Diego, CA, Mar. 2010.
9. M. Li et al., 'Authorized Private Keyword Search over Encrypted Data in Cloud Computing,' 31st Int'l. Conf. Distributed Computing Systems, 2011, pp. 383–92.
10. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, 'Public key encryption with keyword search,' in Proc. of EUROCRYPT, 2004.
11. C. Wang et al., 'Secure Ranked Keyword Search Over Encrypted Cloud Data,' Proc. ICDCS '10, 2010
12. Wenjun Lu; Varna, A.L.; Min Wu, 'Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance-Preserving Randomization,' Access, IEEE , vol.2, no., pp.125,141, 2014.
13. W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, 'Secure knn computation on encrypted databases,' in Proc. of SIGMOD, 2009.
14. K. Ren, C. Wang, and Q. Wang, 'Security Challenges for the Public Cloud,' IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.
15. Zhangjie Fu et al, 'Multikeyword Ranked Search Supporting Synonym Query over Encrypted Data in Cloud Computing', IEEE Conference, 2013.
16. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, 'Searchable symmetric encryption: improved definitions and efficient constructions,' in ACM CCS, 2006.
17. P. Naresh, K. Pavan kumar, and D. K. Shareef, 'Implementation of Secure Ranked Keyword Search by Using RSSE,' International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 3, March – 2013.
18. S. Buyrukilen and S. Bairas, 'Privacy preserving ranked search on public key encrypted data,' in Proc. IEEE International Conference on High Performance Computing and Communications (HPCC), November 2013.
19. B. H. Bloom, 'Space/time trade-offs in hash coding with allowable errors,' Communications of the ACM, vol. 13, no. 7, 1970, pp. 422–426.
20. C. Gentry and Z. Ramzan, 'Single-database private information retrieval with constant communication rate,' in ICALP, pp. 803–815.2005.
21. Y. T. Hou, H. Li, W. Lou, and W. Sun. 'Privacy-preserving keyword search over encrypted data in cloud computing, Insecure Cloud computing,' edited by S. Jajodia et al., Springer, 2014.

22. Sun, W., Wang, B., Cao, N., Li, M., Lou, W., Hou, Y.T., Li, H., 'Privacy-preserving multikeyword text search in the cloud supporting similarity-based ranking,' Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ACM, pp. 71–82.2013.
23. Prasanna B.T, C.B. Akki, 'A Survey on Homomorphic and Searchable Encryption Security Algorithms for Cloud Computing,' Communicated to International Journal of Information Technology and Computer Science, November, 2014.
24. Prasanna B.T, C.B. Akki, 'A Comparative Study of Homomorphic and Searchable Encryption Schemes for Cloud Computing,' Communicated to International Journal of Communication Networks and Distributed Systems, November, 2014.
25. Prasanna B.T, C.B. Akki, 'A Survey on Challenges and Security Issues in Cloud,' Presented in conference presented in Conference on Evolutionary Trends in Information Technology, May 20-22 2011, at Visvesvaraya Technological University, Belgaum, Karnataka.





GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY: E
NETWORK, WEB & SECURITY

Volume 15 Issue 1 Version 1.0 Year 2015

Type: Double Blind Peer Reviewed International Research Journal

Publisher: Global Journals Inc. (USA)

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

Energy Utilization of TCP in Ad Hoc Networks

By JVN. Ramesh & K. Bhavana

KLEF University, India

Abstract- In this paper we have a tendency to study the energy value (protocol process and communication cost) and good output of different various of TCP (Transmission management Protocol) in unintended networks. We enforced a tested and measured the particular energy cost furthermore as good output of running communications protocol urban center, Newreno, SACK (Selective Acknowledgement). we see energy savings between 20% and 500% depending on the network conditions action.

Keywords: *protocol, mobile, TCP, energy.*

GJCST-E Classification : C.2.2



Strictly as per the compliance and regulations of:



Energy Utilization of TCP in Ad Hoc Networks

JVN. Ramesh^α & K. Bhavana^σ

Abstract- In this paper we have a tendency to study the energy value (protocol process and communication cost) and good output of different various of TCP (Transmission management Protocol) in unintended networks. We enforced a tested and measured the particular energy cost furthermore as good output of running communications protocol urban center, Newreno, SACK (Selective Acknowledgement). we see energy savings between 20% and 500% depending on the network conditions action.

Keywords: protocol, mobile, TCP, energy.

I. INTRODUCTION

Communication plays a major role in the ad-hoc networks and is used many applications. It account for a large proportion of energy usage. Energy is an important factor in the ad-hoc networks. It is very essential to lower the energy consumption in the adhoc networks. There are many techniques for reducing energy consumption and energy cost in ad-hoc networks. MAC protocols and routing protocols use energy based metrics. This approach reduces the energy cost. Additionally the energy of the TCP also can be reduced as well. There are four variants in saving the energy. The four variants in saving the TCP energy are : Reno, New Reno, SACK, and TCP-ECN-ELFN. SACK means selective acknowledgement. TCP- ECN-ELFN is a combination of ECN AND ELFN. ECN means Explicit Congestion Notification. ELFN is Explicit Link Failure Notification. ECN is a mechanism that enables the senders to respond quickly to the beginning congestion in the network. When the energy cost is measured there is a good throughput for this mechanism. There is a good total energy and idealized energy for this mechanism. The idealized energy is defined as the energy consumed by the sender for transmitting or sending or receiving. The other variant TCP- ECN-ELFN mechanism results in the lower energy consumption when compared to the SACK. The other variants of TCP that is Reno and New Reno also had a good throughput. In this paper we discuss about the energy model and summary of the various TCP variant mechanisms.

II. RELATED WORK

The link is an approach it includes the effect of ARQ AND FEC and the combination of the two in the ad-hoc networks. There are some link layer schemas to improve the energy behavior. The key idea is to discard the packet transmission when channel conditions are

worsen. When the channel conditions is good then the packet transmission is resumed. The three implementations of TCP the no, Reno, New Reno. This mainly focuses on the wired and the wireless environment.

III. TCP-ECN-ELFN

Table 1 summarizes the changes made to the operation of TCP to include ECN and ELFN. We note that our implementation goes beyond simply adding ELFN and ECN to TCP - we no longer treat timeouts and triple duplicate ACKs as indications of congestion. Rather, we rely exclusively on ECN to a network congestion. The table also describes the intuition behind these changes.[7] describes the interplay between routing failure (due to link outage or propagation of stale routes) and TCP throughput, in detail. Briefly, successive route failures (due to link failure) lead to timeouts hence resulting in a small congestion window.. Hence, the throughput of the connection is small. The proposed in [7] and used by us is as follows. A route failure message is propagated back to the TCP sender from the intermediate node that detects the route failure. This message has the effect of freezing TCP's state and initiating the transmission of probe packets. When there is a response to the probe packet (i.e., the route is up), TCP's state is unfrozen and transmission resumes. This solution ensures that there are no timeouts(and hence no unnecessary retransmissions), and that the TCP sender begins sending packets soon after the route is up. Mobility of nodes can cause packets belonging to the same connection to be routed along different routes. This can result in the receiver getting out-of-order packets which causes duplicate ACKs to arrive at the sender. Likewise, packet loss due to link- layer errors can result in triple duplicate ACKs or timeouts. On receiving three duplicate ACKs, the sender reduces its congestion window by a half and retransmits. the out of sequence packet while in the case of timeouts, the window is reduced to one or two segments. This congestion avoidance behavior has the net effect of reducing the throughput of the connection (due to the smaller congestion window) and thus increasing overall energy consumption. We believe that the appropriate _x for this problem is for the TCP sender to retransmit the of ending packet but not adjust its congestion window. We made this medication.

Author α σ : Dept. of Electronics and Computer Engineering K L E F University. e-mails: jvnramesh@gmail.com, bhavanakarumanchi@gmail.com

Event	TCP's Behavior	TCP-ECN-ELFN
Routing Failure	Timeout, $CWND \leftarrow 1$ Retransmissions Exponential backoff timer	Freeze state Probe network Unfreeze when route restored
Triple Duplicate (TD) ACKs	Retransmit packet $CWND \leftarrow CWND/2 + 3$	Retransmit packet
Timeout	$CWND \leftarrow 1$ Retransmit Exponential backoff timer	Retransmit packet
Explicit Congestion Notification	No action	$CWND \leftarrow CWND/2$

Figure 1

IV. OVER VIEW OF TCP VARIANTS

At present all the TCP implementations depends on Tahoe. Various algorithms are incorporated on TCP for slow start, fast avoidance and fast retransmit and modifications in the formulas for estimation the RTT. RTT means round trip time. The TCP RENO is very much similar to the Tahoe but there is a slight difference that is the fast retransmit algorithm this fast retransmit algorithm includes the fast recovery. When a sender receives three duplicate acknowledgment signals then it reduces by half. But as not like a Tahoe it becomes the slow start. Thus the RENO increases the congestion rapidly by setting it to the minimum. Here the retransmit timer will turn off and this leads to the congestion and the low throughput.

TCP New Reno overcome the disadvantages of the RENO. A partial acknowledgment infers that there are some unacked packets in the senders window. In RENO a partial acknowledgment gives the sender the fast recovery in a view of the multiple packet losses. Whenever the receiver gets a data is out of sequence then that unsequences data creates a hole in the buffer that is present at the receivers end. This is the reason why the receiver generates a duplicate acknowledgment. The receiver includes the starting and ending sequence addresses that is the sequence numbers. These sequence numbers are present in the SACK. The first block in the SACK represents the recently transmitted segment to the receiver. The remaining SACK block represents the recently reported blocks. This algorithm is helpful for TCP to recover from multiple segment losses of data within one round trip time. When the sender comes to know that there is a loss of the packet then it retransmits and reduces the congestion to half and does fast recovery in RENO and New RENO. SACK has a variable named pipe it gives the number of packets in the flight. This pipe variable is increased by one that is incremented for the transmission and it is decreased by one that is decremented when it receives a duplicate acknowledgment. The sender maintains a list of packets that are missed those packets zed energy cost is high for SACK.

V. RESULTS

The greater part of the examination in impromptu systems administration utilizes the ns2 test system and to a lesser degree different test systems like glomosim to run tests. The benefit of this approach is that scientists can expand upon the work of others and utilize a standard stage to check contending thoughts

Ntutk condition	Lower E_1	Higher Goodput
<i>Mobile ad hoc networks</i>		
Route failure	ECN-ELFN	ECN-ELFN
Pkt reordering	ECN-ELFN	ECN-ELFN
<i>Static ad hoc networks</i>		
Packet Loss	Newreno	ECN-ELFN
Bursty loss	ECN-ELFN	ECN-ELFN
Congestion	ECN-ELFN	ECN-ELFN

Figure 2

retransmitted. Even if the partial acknowledgements are received the pipe value is decremented by the sender. SACK has a good throughput in the many of the network conditions. SACK would consume low total energy but the sender that is using has to execute lot of code and maintain big data structures. While ns2 is a decent instrument for measuring customary system measurements, for example, throughput, misfortune, and deferral, it is ill suited to measure vitality utilization of a convention like TCP. This is on the grounds that the vitality devoured incorporates not just the radio costs (which are demonstrated to some degree in ns2) yet the hub level convention handling and information duplicate expenses. An alternative thought would be to utilize a hub level vitality simulator/emulator that gives genuinely precise vitality readings for preparing code. The issue, notwithstanding, is that these devices don't reenact the specially appointed system environment. Therefore, an romanticized test system would be one which joined a point by point hub level emulator and ns2. Nonetheless, we are not mindful of any such test system that we could have utilized. Given the above obligations, we chose to utilize a half breed methodology to measure the hub level TCP vitality. Specifically, we utilized a 4-hub system (see Figure 3) in which we measured the vitality of the sender hub straightforwardly utilizing two Agilent 34401a multi metres (determination of 1msec) one measured the aggregate framework vitality while the second measured the radio level vitality alone (Figure 2 demonstrates an example information follow) Toshiba smart phone that has a Lucent 802.11 Silver (11 Mbps) Wavelan DSSS PC card. Further, the two moderate hubs

are situated up to go about as switches. To reproduce multi-bounce specially appointed system conduct, we ran Dummynet at hub C. Dummynet is an unreservedly accessible portion level fix that permits us to control a wide-mixed bag of system practices, for example, been advanced as an issue Standard for utilization over the Web.

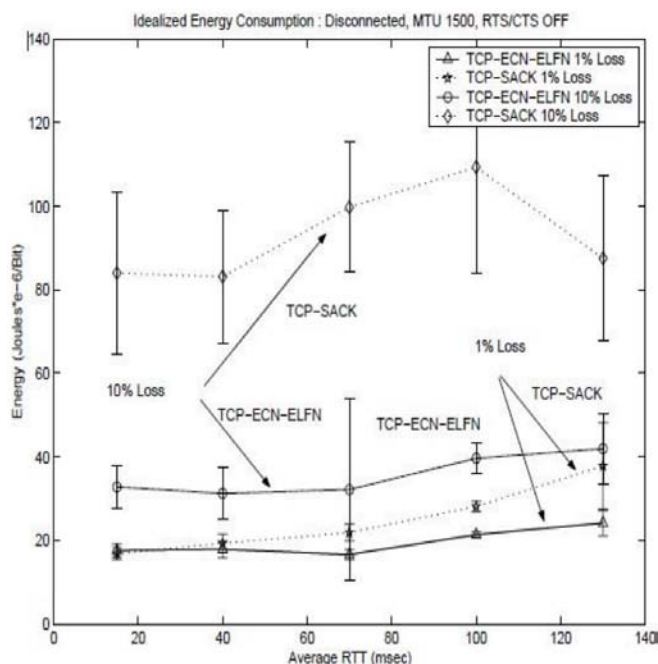


Figure 3

VI. CONCLUSION

In this paper we have characterized the energy cost of TCP Reno, Newreno, SACK and a modified version of TCP(ECN-ELFN) that appears to be better suited for operation in ad hoc networks. The TCP-ECN-ELFN protocol relies on explicit routing failure notifications to freeze TCP state allowing faster recovery when the route is back up. In addition, it uses ECN to respond to network congestion. We showed that the TCP-ECN-ELFN protocol uses less energy and delivers a higher good put as compared with the other three TCP variants in all cases but one where Newreno performs better (see Table 2). One of the areas of concern in using the TCP-ECN-ELFN protocol, however, is the issue of fairness. That is, will this protocol share bandwidth fairly between multiple connections. This question is fairly complex and is presently being studied in a ns2 simulation.

VII. ACKNOWLEDGMENT

We would like to thank Jim Binkley for his technical support in implementing our testbed, L. Rizzo for technical support on Dummy net, and the FreeBSD community for technical support during our implementation of SACK in FreeBSD4.3.

REFERENCES RÉFÉRENCES REFERENCIAS

1. Ashish Ahuja, Sulabh Agarwal, Jatinder Pal Singh, and Rajeev Shorey. Performance of tcp over direct routing protocols in mobile ad-hoc networks. In IEEE Vehicular Technology Conference (VTC 2000), Tokyo, Japan, May 2000.
2. Thomas D. Dyer and Rajendra V. Boppana. A comparison of tcp performance over three routing protocols for mobile ad hoc networks. In ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), October 2001.
3. Sorav Bansal et.al. Energy efficiency and throughput for tcp traffic in multi-hop wireless networks. In Proceedings INFOCOM 2002, New York, NY, 2002.
4. K. Fall and S. Floyd. Simulation-based comparison of tahoe, reno, and sack tcp. ACM Computer Communications Review, 26(3):5 { 21, July 1996.
5. S. Floyd TCP and explicit congestion notification. ACM Computer Communication Review, 24(5):10{23, 1994.
6. M. Gerla, K. Tang, and R. Bagrodia. Tcp performance in wireless multi-hop networks. 26-29 1998. In IEEE WMCSA'99, (New Orleans, LA), Feb. 1999.
7. Gavin Holland and Nitin H. Vaidya. Analysis of TCP performance over mobile ad hoc networks. In ACM Mobile Computing and Networking (MOBICOM'99), pages 219{230, 1999.
8. M. Srivastava P. Lettieri, C. Schurgers. Adaptive link layer strategies for energy efficient wireless networking. In Wireless Networks, volume 5, pages 339 {355, 1999.
9. L. Rizzo. Issues in the implementation of selective acknowledgements for tcp, 1996.
10. L. Rizzo. Dummynet: a simple approach to the evaluation of network protocols. ACM Computer Communication Review, 27(1), January 1997.
11. W. Richard Stevens. TCP/IP Illustrated, Volume I: The Protocols. Addison Wesley, 1994.
12. V. Tsaoussidis, H. Badr, X. Ge, and K. Pentikousis. Energy/throughput tradeoffs of tcp error control strategies. In In Proceedings of the 5th IEEE Symposium on Computers and Communications, France, July 2000.
13. Xiang Zeng, Rajive Bagrodia, and Mario Gerla. Glomosim: a library for parallel simulation of large-scale wireless networks. In Proceedings of the 12th Workshop on Parallel and Distributed Simulations { PADS '98, May

GLOBAL JOURNALS INC. (US) GUIDELINES HANDBOOK 2015

WWW.GLOBALJOURNALS.ORG

FELLOWS

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards “FARSC” title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.



- The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:



FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA). The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.



You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

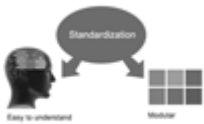
We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.





The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.



The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website <https://associationofresearch.org> which will be helpful to upgrade the dignity.



The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.





The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.



MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.

The "MARSC" is a dignified ornament which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.



MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and reputé to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefits can be availed by you only for next three years from the date of certification.



MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.





We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.



Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.



AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as “Institutional Fellow of Open Association of Research Society” (IFOARS).

The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.



The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as “Institutional Board of Open Association of Research Society”-(IBOARS).

The Institute will be entitled to following benefits:



The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.



The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of “Open Association of Research Society, U.S.A (OARS)” so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.



Journals Research
inducing researches

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.



After nomination of your institution as “Institutional Fellow” and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.

The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.



Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.



We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth \$ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.



- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10% discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in-depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

//

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of “Difference of Opinion [if any]” among the Board members, our decision will be final and binding to everyone.

//

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.



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 brevity.

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 $1.4 \times 10^{-3} \text{ m}^3$, or 4 mm somewhat than $4 \times 10^{-3} \text{ m}$. 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.

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.



Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.



12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.



27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium through which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

INFORMAL GUIDELINES OF RESEARCH PAPER WRITING

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.



Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

- Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

- Use standard writing style including articles ("a", "the," etc.)
- Keep on paying attention on the research topic of the paper
- Use paragraphs to split each significant point (excluding for the abstract)
- Align the primary line of each section
- Present your points in sound order
- Use present tense to report well accepted
- Use past tense to describe specific results
- Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives
- Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.



Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript-- must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.



- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently. You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.



Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.



THE ADMINISTRATION RULES

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.



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

C

Cotopic · 9
Cryptography · 17

D

Daewook · 10, 16

E

Encryption · 17, 19, 21, 23, 24, 25, 36

G

Guobing · 8, 16

H

Heuristic · 7, 21
Homomorphic · 17, 19
Huiyuan · 13

O

Ontologies · 10
Ourania · 9, 16

P

Pareto · 7
Petrinet · 12

T

Tuples · 11

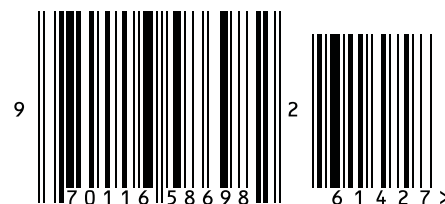


save our planet



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