Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: B

Cloud & Distributed

OTP Generation Process

High Performance Analytics

Highlights

Recursive Quantum Network

Effective Authentication Scheme

Discovering Thoughts, Inventing Future

VOLUME 16 ISSUE 2 VERSION 1.0

Global Journal of Computer Science and Technology: B
Cloud & Distributed

Global Journal of Computer Science and Technology: B
Cloud & Distributed

Volume 16 Issue 2 (Ver. 1.0)

Open Association of Research Society

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
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents of the Issue

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Effective Authentication Scheme for Distributed Mobile Cloud Computing Services using a Single Private Key

By Mrs. Kavitha K K & Avinash B
New Horizon College of Engineering

Abstract- Mobile cloud computing comprises of cloud computing, mobile computing and wireless network. Providing secure and convenience for the mobile users to access multiple cloud computing services is essential. This paper furnish an effective way of providing the authentication for the mobile users to access multiple cloud computing services. The proposed scheme outfit a secure and expediency for mobile users to access several cloud computing services from multiple service providers using a single private key. Our proposed scheme is based on bilinear pairing cryptosystem. In addition, the scheme also supports mutual authentication, key exchange, user anonymity. To overcome the vulnerabilities of traditional methods, from system implementation point of view, the proposed scheme eliminates the usage of verification tables that are required to store the user credentials(user ID and password) which are the part of smart card generator service and cloud computing service provider.

Keywords: smart card generator (SCG), mutual authentication, ID based cryptosystem, bilinear pairing cryptosystem, identity provider (Idp).

GJCST-B Classification : C.1.4 C.2.1 C.2.3

Strictly as per the compliance and regulations of:

An Effective Authentication Scheme for Distributed Mobile Cloud Computing Services using a Single Private Key

Mrs. Kavitha K K [α] & Avinash B [σ]

Abstract- Mobile cloud computing comprises of cloud computing, mobile computing and wireless network. Providing secure and convenience for the mobile users to access multiple cloud computing services is essential. This paper furnish an effective way of providing the authentication for the mobile users to access multiple cloud computing services. The proposed scheme outfit a secure and expediency for mobile users to access several cloud computing services from multiple service providers using a single private key. Our proposed scheme is based on bilinear pairing cryptosystem. In addition, the scheme also supports mutual authentication, key exchange, user anonymity. To overcome the vulnerabilities of traditional methods, from system implementation point of view, the proposed scheme eliminates the usage of verification tables that are required to store the user credentials(user ID and password) which are the part of smart card generator service and cloud computing service provider.

Keywords: smart card generator (SCG), mutual authentication, ID based cryptosystem, bilinear pairing cryptosystem, identity provider (Idp).

I. Introduction

Due to abundant benefits and possibilities that are provided by Cloud computing there is a rapid growth of users in the recent years. As the report from Juniper Research estimates that the number of unique consumers accessing cloud-based services will exceed 3.6bn by 2018, rising from an estimated 2.4bn in 2013 [1]. This expeditious development has been revolutionized in number of areas. In early days of computing, huge scale machine and mainframe computers were used to implement various task and applications. Now a days, we are doing the same tasks, but in flexible, much cheaper, and are in portable manner, either by desktop computers or mobile devices(such as, smart phones, tablets, etc.), with several type of services tied, so called Cloud Computing System(CCS). The user can use services and application on the cloud through internet.

However, In the recent years, there is a rapid growth in the mobile application due to increase in the popularity of smart phones. Mobile devices have started becoming abundant with application in various categories such as entertainment, health, games, business, social networking, travel and news [2]. The reason for this is that mobile computing is able to provide a tool to use the user when and where is needed, irrespective of user movements, hence supporting location independence. So the development mobile cloud computing become an important research in this mobile oriented world. The general purpose[3] of mobile cloud computing is, a public system is built need uses the cloud infrastructure, to contribute in improving mobile device performance efficiency.

In this paper, an effective authentication schema for the distributed mobile cloud computing is proposed. This schema uses a single private key for the authentication of multiple service providers [4]. Earlier, in one mobile user authentication only the target cloud service provider need to interact with the requestor (user). As the mobile user generally access different mobile cloud computing services, it is very tedious for user to register different user accounts on each service provider and to maintain them. The proposed schema is built upon bilinear pairing[5]. And therefore, requires less computation resources on both mobile devices and service provider. Through this, a user can get access to multiple service providers using a single private key, provided both mobile user and service provider should know the identities of each other.

II. Related Work

Today, providing access to right user is the major concern. There should be a right mechanism that prevent the illegal access from unauthorized user. Authorization schema is the security mechanism for the network based services. Traditionally, authorization schema's user traditional public key cryptosystem such as RSA, which requires lengthy key size and utilizes the maximum of computational resources on the mobile devices. Since mobile devices be short of resources, traditional authentication schema are inappropriate to use. Therefore an efficient schema is required, which is beneficial for the mobile device.

Author α: Department of Information science New Horizon College of Engineering Bangalore.
Author σ: Department of Information Science New Horizon College of Engineering Bangalore. e-mail: avinash.kb94@gmail.com

In the recent years, many ID based cryptosystem [6] have been proposed. An ID based cryptosystem is the public key cryptosystem that resolve the issues with the traditional public key cryptosystem. In the proposed system, an ID based cryptosystem is based on bilinear pairing in an elliptic curve.

III. Proposed System

In this paper, an user authentication schema is based on bilinear pairing for distributed mobile cloud computing. The proposed system supports mutual authentication, key exchange, and user untraceability.

The following are the benefits that are preserved by using this authentication scheme.

i. The key size provided by ECC is much smaller compared to the size provided by the traditional public key cryptosystem.
ii. Since the public key is used as a identity of the user, the computational cost to verify other public keys are eliminated and the storing space of other public key is not required.
iii. The user must access multiple service provider, it is important for the user to manage multiple keys provided by each service provider. This problem is resolved by sharing the same private key by all the service provider.

The trusted smart card generator (SCG) is used in the proposed system as the third party, that eliminates the use of identity provider (IdP), which is used by other system for the user authentication. There are three characters in the scheme: mobile user, mobile cloud service provider and trusted SCG service. In our scheme, the user is assigned a smart card, which is being modified by some parameters during the user registration phase. The usage of this smart card makes the system make more protected by avoiding the user from distributing their login credentials. By this the scheme effectively prevents the situation of many logged in users with same login ID. Typically the registered user share his credentials so that other who know the login-ID and password can login successfully. In this scheme, the login request is created by the smart card using its stored secret component without any human intervention. It is extremely difficult to extract the secret component from the smart card, and thus the user cannot share it with others. Even if the legitimate user's password is shared with others, the other person cannot login to the system without the smart card. Once a valid user logs into the remote system, his smart card will be inside the terminal until the user logs out. If the user pulls out the card from the terminal after login the remote system, the login session will be immediately expired. Thus, the scheme can successfully prevent the scenario of many logged in users with the same loginID.

The scheme consist of three phases: set up phase, registration phase, and authentication phase. In the rest of the paper, we give preliminaries of these three phases based on bilinear pairing cryptosystem [7].

Preliminaries

a) Bilinear pairing

Let G_1 the cyclic additive group generated by P, whose order is Q. G_2 be the multiplicative group of same order. A map $e : G_1 \times G_1 \rightarrow G_2$ is called bilinear mapping if it satisfies the following properties.

a) Bilinear: $e(aP, bQ)=e(P,Q)^{ab}$ for all $P,Q \in G_1$ and $a,b \in Zq^*$.
b) Non degenerate: there exist $P,Q \in G_1$ such that $e(P,Q) \neq 1$.
c) Computable: there exist an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

In reality, G_1 is the group of points on an elliptic curve Zq^* and G_2 is the subgroup of multiplicative group of finite field $Z^*_q{}^k$ for some $k \in Z_q^*$.

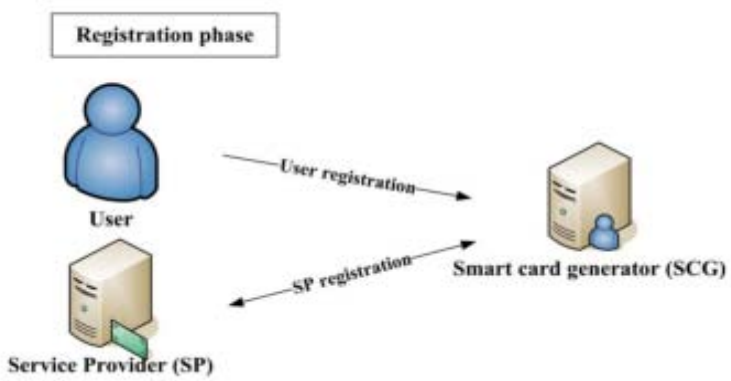
b) Set up Phase

During set up phase, the smart card generator select the random number and computes its master private key (s). With this master private key it also generates public key and public parameters.

Suppose G_1 is an additive group and G_2 is the multiplicative group of order q and suppose P is the generator of G_1, then $e : G_1 \times G_1 \rightarrow G_2$ is called bilinear mapping, $H: \{0,1\}^* \rightarrow G_1$ is the cryptographic hash function. Selects a master private key s and computes public key as $Pub=sP$. Then publishes the public parameters $(G_1, G_2, e, q, P, Pub, H)$ and keeps s secret.

c) Registration Phase

The registration phase is executed between the SCG and the mobile users. The mobile who wishes to join the network and utilize the service can join the network by sending the identities to the SCG. Even the SP's also requested to register with SCG in this phase. With the identities provided, the SCG generates the public key for each mobile user and SP, then dispatches it to corresponding user or SP securely.

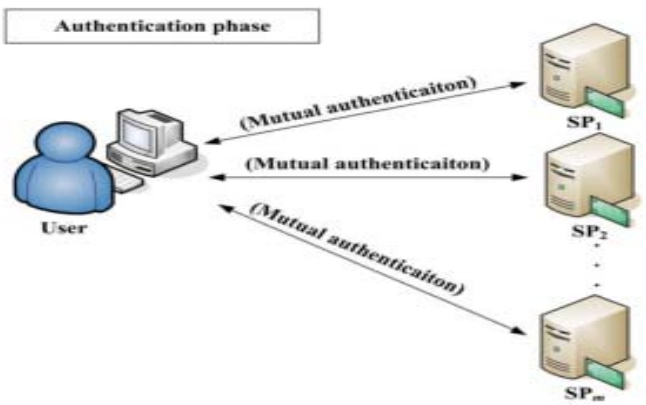


This phase is executed by following steps when user wants to register.

i. Suppose a new user U_i wants to register with SCG.
ii. U_i submits the identity ID_i and password PW_i.
iii. On receiving the request, the SCG computes $Reg_{id} = s.H(ID_i) \mid H(PW_i)$.
iv. The SCG initializes the smart card with the parameter IDi, Regid, H(.) and send the smart card to the U_i over a secure channel.
v. The SCG initializes the smart card with the parameter ID_i, Reg_{id}, $H(.)$ and send the smart card to the U_i over a secure channel.

d) Authentication Phase

This is executed when the user logs into the system. This phase is further divided into login phase and verification phase.



i. *Login Phase*

The user U_i insert the smart card in a terminal and enter ID_i and PW_i. The ID_i is identitical to one that is stored in smart card. If the credentials are same then sends the login request to the corresponding SP.

i. Computes $DID_i = T.Reg_{id}$, where T is the user system's timestamp.
ii. Computes $Vi = T.H(PW_i)$.
iii. Sends the login request $(ID_i, DIDi, V_i, T)$ to the SP over a public channel.

e) verification Phase

The SP receives the login message (ID_i, DID_i, V_i, T) at time $T^* (\geq T)$. Over receiving the login request the SP does the following operations.

i. Computes the time interval between T and T^*. If $(T^* - T) \leq \Delta T$ then SP proceeds to step ii. Otherwise rejects the login request. ΔT is the expected time interval between transmission delay.
ii. Checks whether $e(DID_i - V_i, P) = e(H(ID_i), Pub)$. If it is valid, the SP accept the request , else rejects it.

During this phase, the mobile user and service provider are able to authenticate without the intervention of SCG. And therefore reduces the time required by the trusted third party to verify the user. The session key is also generated during this phase to encrypt/decrypt the messages sent between user and service provider.

f) Password Change Phase

This phase is executed when the user wants to change the password. The proposed scheme allow this step to execute without the intervention of the SCG. The user insert the smart card into the terminal and keys ID_i and PW_i. If ID_i is matching with the value stored in smart card then allows the user to change or it terminates the operation. The phase works like this.

i. U_i enters the new password PW_i.
ii. The smart card calculates $Reg_{id}^{*} = Reg_{id} - H(PW_i) + H(PW_i^{*}) = s.H(ID_i) + H(PW_i^{*})$.
iii. The password has been changed to the new password PW_i^{*} and the smart card restore the value of Reg_{id} with Reg_{id}^{*} value.

IV. Resilience of Proposed System

a) Security

The proposed scheme can resist to the following attacks:

i. *Replay Attack*

Suppose an adversary tap the login request from the valid user, the SP receive the request at time T_{new} . The SP calculates the time interval (T_{new}-T) and compares with expected time interval delay (ΔT) which exceed the value. And therefore the attack fails.

ii. *Forgery Attack*

From the valid login message, an adversary can get only get ID_i, DID_i, V_i and T. from these values an adversary can't find any use full information. Though $DID_i = T. Reg_{id}$, this does not reveal any information needed since the Reg_{id} kept secret.

iii. *Insider Attack*

In password based user request, the trusted third party maintains a separate table called verifier table for storing the user credentials. Since in our proposed scheme, the login request is based on user's password as well as the secret key *s*, and thus it eliminates the usage of verifier table.

V. Conclusion

The scheme prevents the adversary from forgery attacks by employing a dynamic login request in every login session. The use of smart card not only makes the scheme secure but also prevents the users from distribution of their login-IDs, which effectively prohibits the scenario of many logged in users with the same login-ID.

References Références Referencias

1. Steffen Sorrell, "Cloud Computing - Consumer Markets: Strategies & Forecasts 2015-2020", Juniper, Enabling Technologies, 04 November 2015.
2. Ahmed Dheyaa Basha, Irfan Naufal Umar, Merza Abbas, "Mobile Applications as Cloud Computing:Implementation and Challenge", International Journal of Information and Electronics Engineering, Vol. 4, No. 1, January 2014.
3. Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, " Mobile cloud computing: A survey", Elsevier, 22 May 2012.
4. Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication scheme for Distributed Mobile Cloud Computing Services", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015.
5. Al-Sakib Khan Pathan and Choong Seon Hong "Bilinear-Pairing-Based Remote User Authentication Schemes Using Smart Cards" ICUIMC'09, January 2009.
6. T. H. Chen; H. l. Yeh; W. K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing" IEEE Conference Publications, 2011.
7. Manik Lal Das, Ashutosh Saxena, Ved P. Gulati, Deepak B. Phatak, "A novel remote user authentication scheme using bilinear pairings" Elsevier, Computers & Security, 2006.

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cloud Computing Distilled: What the Practitioner Needs to Know

By Harvey Hyman
Library of Congress, United States

Abstract- While cloud computing has moved to the forefront of strategic IT initiatives in recent years, only a few articles have focused on the basic fundamentals, and none have been written with the practitioner in mind. This article presents a basic, yet comprehensive discussion on what cloud computing is, and how it works.

The article identifies and describes the core concepts that an IT manager should know about cloud computing, and provides simple explanations for how the fundamental methods of cloud are used and their impacts upon business processes. This article divides the technology of cloud computing into four distinct categories: service models, delivery architecture models, virtualization and performance.

We describe three service models of SaaS, PaaS and IaaS, three architecture models of public, private and hybrid cloud, explain how virtualization technology works, and discuss the current trends in performance factors of HA, FT, scalability, optimization, control and management.

Keywords: cloud computing, virtualization, hypervisors, provisioning, performance, high availability, fault tolerance.

GJCST-B Classification : C.1.4 C.2.1 C.2.3

Strictly as per the compliance and regulations of:

Cloud Computing Distilled: What the Practitioner Needs to Know

Harvey Hyman

Abstract- While cloud computing has moved to the forefront of strategic IT initiatives in recent years, only a few articles have focused on the basic fundamentals, and none have been written with the practitioner in mind. This article presents a basic, yet comprehensive discussion on what cloud computing is, and how it works.

The article identifies and describes the core concepts that an IT manager should know about cloud computing, and provides simple explanations for how the fundamental methods of cloud are used and their impacts upon business processes. This article divides the technology of cloud computing into four distinct categories: service models, delivery architecture models, virtualization and performance.

We describe three service models of SaaS, PaaS and IaaS, three architecture models of public, private and hybrid cloud, explain how virtualization technology works, and discuss the current trends in performance factors of HA, FT, scalability, optimization, control and management.

Keywords: cloud computing, virtualization, hypervisors, provisioning, performance, high availability, fault tolerance.

I. Introduction: Defining Cloud Computing

What is Cloud Computing? There are three general ways to define it. An operational definition of cloud computing is "utility computing." A descriptive definition for cloud computing is service-based, or resource-based computing. A practical definition is simply "pay as you go" computing [1]. All of these descriptions of cloud are correct, and they reflect the two main impacts of cloud computing upon business: scalability and leverage [2], [3]. We discuss these impacts later in the paper, as well as the business and individual advantages to using cloud computing.

In this article we treat the use of cloud computing in terms of "leveraging third party resources, communicated across a network" to support one's individual or organizational computing needs. The goal here is to divide the use of cloud computing into four simple groupings: service models, delivery architecture models, virtualization, and performance. We describe and explain each grouping in the sections that follow. We begin with the three main models of cloud computing services: SaaS, PaaS, and IaaS [2].

Author: Library of Congress, National Library Service (NLS/BPH).
e-mail: hymanphd@gmail.com

II. Cloud Delivery Models: SAAS, PAAS, IAAS

The general consensus starting point for a framework for discussing concepts in cloud computing is the 2009 article by Armbrust et al., entitled "Above the Clouds" [1], [4]. While there were a few earlier articles [5], [6], theirs marked the first significant attempt to comprehensively define the emerging landscape coined as *cloud computing* by identifying developing categories in the technology, models, and services evolving as the core constructs that make up the "cloud." Over last six years since the release of Armbrust et al., several studies have been working toward a consolidation of the domain constructs into a paradigm to guide academic research and industry practice [4].

The first area of consolidation is in regard to service delivery models. For the past several years there has been an overabundance of descriptive service models. This has not been very helpful. Instead of providing a clear path for guiding researchers and practitioners alike, toward the most productive resources to focus upon, a plethora of service delivery models had led to a murky field of definitions and a glorified "thinking out loud" about the next would-be "potential of the day" in cloud computing services. This overabundance has culminated in the catch-all phrase XaaS or "everything as a service" – not very informative or focused. One might as well use the term AaaS – for "*anything* as a service."

The general consensus, both in academic and practitioner circles is that cloud service delivery models have been consolidated into three distinct categories: SaaS, PaaS, and IaaS.

SaaS, stands for Software as a Service. This delivery model is most commonly associated with the term *thin client* and software accessed via a web browser. Think of this model as *user-facing*. This is the choice of delivery for end-users who wish to access a hosted application such as common business applications. The operative description here is *software applications that are subscription based and internet hosted*.

The main significant factor with SaaS as a service delivery model is the centrality and control in distribution. Instead of deploying multiple copies of a software application, SaaS allows for a single copy to be

accessed by the end-user. The specific advantages here are versioning and policy – both of which can be controlled almost instantly by updating the application host. In technical terms, SaaS supports a *multi-tenant architecture*. This means that all customers of the service use the same single version of the software application with the same single configuration of hardware, OS, and communication network. If we want to support more than one version of an application, another means of SaaS distribution would be the use of individual virtual machines (VMs), each supporting a different configuration or version of the application. This is explained in greater detail later.

PaaS, stands for Platform as a Service. Think of this model as *developer-facing*. In practical terms it is really just a more robust variety of SaaS. This model is most commonly associated with providing development, deployment and maintenance support for a web-based application. You might also think of this model as a lifecycle approach – beginning with developing the application and ending with hosting and maintaining the application. This is the type of solution a business would use to deploy an application to be used as a SaaS by its customers.

Some technical analysts might distinguish SaaS from PaaS in terms of where the user's data lives. For example, SaaS is sometimes viewed as merely providing processing, and the data itself begins and ends on the user's local machine, whereas the "platform" in PaaS is viewed as providing the container for everything, including the residence of the user's data.

This distinction highlights a significant concern when relying on cloud computing for a business solution – when the connection is down, so is the service, there are no local copies as with the traditional client deployment model. There is also the potential for "data lock," not discussed in this article.

IaaS, stands for Infrastructure as a Service. This model is the most aligned with the cloud definition of "utility computing." In this service delivery model, we are no longer focused on the individual end-user. In this model the customer is defined as an organization, and the service is defined as computing resources. Think of this model as the configuration of a computing backbone that supports an entire enterprise. An IaaS provider supplies a pool of resources for the three computing components of CPUs, memory, and storage. The technologies most closely associated with IaaS are virtualization, provisioning, and instances. These are discussed in the sections that follow.

In the interest of providing complete information on the subject of service delivery models, we need to acknowledge that over the past several years there have been numerous variations of service oriented computing such as IDaaS (Identification), BaaS (backend), STaaS (storage), EaaS (email), (enterprise), (everything). However, the industry has consolidated service models into the main three described above, with all other variations of service deliveries over the cloud having been merged into the main catch term XaaS – everything as a service, also eponymously written as *aaS or EaaS.

III. How Does Cloud Computing Work? Virtual Machines and Hypervisors

What the IT manager needs to know is that there are three main components to a Cloud Computing solution: Virtual Machines (VMs), Hypervisors (VMM), and Hosts (servers). The remainder of this section will explain what these components are, the purpose they serve, and how they work.

A quick note to the reader here: Virtualization does not make the cloud work, but it allows for the best features of cloud to be provided. Specifically, virtualization allows for scalability, high availability, fault tolerance, optimization, management, and control. These features will be explained later in the article.

Remember, cloud computing is a construct, meaning it is not a technique, in and of, itself. Instead, one should think of cloud computing as a *collection of computing technologies* that support the goal of resource-based, service-based, utility computing.

Remember also that, cloud computing is the ability to access computing services over a network. Cloud computing provides these services by making use of the core technology of virtualization.

The definition of virtualization is "software acting like hardware" or "software taking the place of hardware" or "software emulating hardware" or "software functioning as hardware" [7], [8]. Take your pick, but the concept remains the same. The purpose of virtualization is to increase the capacity of physical hardware by creating multiple virtual environments (VMs) on top of them [8].

The modern virtualization model focuses primarily on the virtual machine (VM) and the hypervisor (VMM), but, like cloud computing, virtualization is more akin to a collection of technologies than a specific technique itself. Meaning, the significance of virtualization is not limited to its application of the VM and the VMM. There are also vLANs to take the place of physical LANs, and vSwitches to take the place of physical switches. Both of which are examples of using software to take the place of hardware with the goal of supporting easier configuration, greater control, scalability, and increased capacity. For an excellent discussion on virtualization techniques applied across the enter enterprise resource pool see reference [9].

Now, for a little history on the origins of the concept of virtualization, early work on virtualization and the use of virtual machines (VMs). The concept of virtualization and the virtual machine dates back to, at

least, the 1950s and the use of mainframes, followed by work in the 1970s on "Grid Computing." [7], [8]. See the referenced Popek and Goldberg article for a good discussion of the 1970s view on virtualization and the VM.

A VM is an "isolated duplicate" [7] of a physical machine. In the practical sense, think of a VM as a separate, isolated container that provides an entire computing environment – this is also known as *provisioning* an *instance*, explained in more detail later.

The hypervisor, which has historically also been called the VMM or virtual machine monitor, [7] also sometimes referred to as the "controller program," [7] is the software application that supports the VM environment. The hypervisor is what allows a single server (also called the host) to support multiple guests (VMs) [7]. The number of VMs is only limited by the total number of physical resources available from the host [8]. So, for example, if there are 20 CPUs available on the host, then up to 20 CPUs can be allocated to the various VMs to be created. An important thing to remember here is that there must always be some reserve for the host itself and for the hypervisor itself, as well as the VMs they are supporting [8].

There are two models for running a hypervisor: Type I and Type II. In a Type I installation, the host is the bare metal server. In this case, the hypervisor "presents" the environment to the VM and serves all resource requests from the OS residing in the VM container [9].

In a Type II installation, the hypervisor sits on top of the existing OS and relates resource requests to the underlying OS, which then fulfills the requests. A common example of this use case is an individual user who downloads an application as an appliance, and runs that appliance in a free virtual machine (typical examples are MS Hyper-V or Oracle Virtual Box) on their laptop or desktop. An application as an appliance is a complete package version of an application that includes everything it needs to run on a bare minimum OS environment – hence why it is a very popular choice for individuals who prefer an application that comes preconfigured for a virtual environment (think a VM wizard). A type II hypervisor model is also handy for presenting a testing environment for a development team that may wish to install specific versions of an OS or a legacy application without impacting the native host or larger resource pool.

IV. Types of Clouds: Public, Private, Hybrid.

Public, private, and hybrid clouds are three leading types of cloud architectures that have emerged as the main conceptual descriptions for the deployment of cloud computing configurations.

In the past several years there have been other variations of cloud architecture offered to explain ad hoc configurations such as *community cloud, distributed cloud, inter-cloud,* and *multi-cloud*. However, for the most part, the industry has consolidated cloud provider models to the main three described here.

The public cloud describes a computing architecture whereby the user's instance is drawn from a shared pool of resources. This is also called multi-tenancy. The main advantage here is for the small business user who wants to "spin up" or "tear down" a web based computing application or service, and does not require specific hardware or software configurations or have particular security concerns. The public cloud is most closely associated with the "pay as you go" business model for cloud computing. The security aspect is particularly important to note here given that the user's instance is based on the shared pool of resources and not dedicated to the user as would be in a single tenant model. This model is associated with managed solutions common supplied by AWS and Azure.

The private cloud describes a computing architecture whereby the hardware, storage and communication network is dedicated to the organization. This is called single tenant. This model is associated with users whom require custom configurations, have specific hardware, software or network requirements, have higher level security concerns such as HIPAA or other compliance issues, and desire greater control and management of their computing resources. This model is not a "pay as you go" model due to the dedicated nature of the hardware and software pool.

The hybrid cloud is more of a scalability solution than an architectural model. Hybrid cloud covers situations whereby an organization requires the flexibility to temporarily expand their computing needs such as increased CPU for processing power, added storage, or additional memory allocation.

In this use case, an organization may have a custom configuration of dedicated hardware, software and network communication, but requires additional resources to temporarily scale up a service or process. The organization can achieve this temporary increase in scale by extending into the public cloud. This allows the organization to take advantage of the "pay as you go" approach for the additional scale up, and release those resources when no longer needed, all the while maintaining their custom configuration to meet their unique business needs.

V. Provisioning and Instances

What is Provisioning? Simply put, provisioning is the allocation of computing resources. The resources are configured as an **instance**, which is the specific operational deployment of computing resources to support a particular business process [10], [11]. A good

use case example is an organization that wants to run a Hadoop application. The cloud provider will "provision" an "instance" of a Hadoop cluster, or "spin up a VM" configured for this purpose. This allows the organization to horizontally scale the Hadoop application, using as much compute, memory and storage as needed.

When we think of provisioning an instance from a pool of resources, we begin to think of this implementation as a computing cluster [12]. A cluster is comprised of nodes. Think of nodes as individually configured CPU, memory and storage elements combined in a manner to support the required business process. This is an example of optimization, whereby a provisioned instance is matched to a specific performance requirement. This is discussed in more detail in a later section.

The cluster approach differs from the Grid model in that each node of a cluster is running its own instance. It is this simple distinction that allows for the support of features known as HA and FT, also associated with functionalities called load balancing and fail over.

VI. High Availability (HA)

High Availability (HA) is a design method for system continuity by switching services over to alternative hosts in the case of server or hardware failure, generating a new VM in the case of software or OS failure, or generating a new node in the case of a node failure [13].

The main thing to understand when discussing HA is that services are restored quickly, but not instantaneously [14]. However, the vast majority of applications and services will appear to be seamless to the end user. HA is often associated with minimizing downtime due to maintenance, upgrades, and software application failures (the most common source of failure). In the use cases of maintenance and upgrades, HA is used to migrate the VM to another available host during the planned down period.

Two additional things to know here. One, in order for HA to work, there needs to be enough resources available to host the VMs needing to migrate. Two, in the case of an application failure, there is a moment of unavailability (however short), until the VM is restarted (this is reboot time).

If services are so critical that the end user cannot accept even a momentary lapse, then FT offers an added level of robustness.

VII. Fault Tolerance (FT)

Fault Tolerance (FT) is a design method intended to achieve no interruption in service [14]. This topic is currently still ripe for continued system testing and bench marking.

The main thing to understand here is the tradeoff between robustness and cost. FT is achieved through redundancy. In the case of HA, as long as resources are available a VM can be restarted (the delay is in the required boot time). FT by comparison not only reserves a redundant amount of resources to absorb the failure, but also sustains a shadow copy of the VM, thereby maintaining a primary and secondary VM [15].

An example of this is the feature known as vLockstep offered by VMware [15]. This feature maintains simultaneous writes to a primary and a secondary VM. When the primary VM fails, the secondary continues on. As far as the customer is concerned, nothing has happened. The main technical difference here is the service continuity occurs without the need for a reboot [14].

The main tradeoff when it comes to HA and FT is the increased cost for the additional resources, just sitting there, waiting to be used. This becomes a significant economic as well as architectural issue that must be considered by the stakeholders of the service in terms of how much risk they are willing to accept, the level of service they are committed to provide, and the cost they are willing to absorb.

VIII. Performance: Scalability, Optimization, Management and Control

Current trends in cloud computing are exploring performance factors in scalability, optimization, management, and control. These factors are used to assist organizations when choosing the type of cloud service model (SaaS, PaaS, IaaS), architecture model (Public, Private, Hybrid), and continuity model (HA, FT) best suited for their business processes.

When we discuss scalability in the cloud, we are referring to the ability to scale up as well as scale down dynamically and elastically [16]. Scaling up refers to the ability to add resources to handle additional workloads without reducing performance. Scaling down refers to the ability to release or eliminate resources when workloads are reduced.

Under the physical model for computing, increased scalability is achieved through the time consuming acquisition, installation and configuration of hard assets. When workloads are reduced, idle computing assets sit unused, waiting to be tasked – costing money.

The cloud model (applying virtualization) allows for dynamic scaling of resources. The advantage here is the ability to instantly respond to increased workload demands and yet, only pay for what is needed, when it is needed. Unused assets are released. In this use case, "elasticity rules" are applied to establish the optimal use of computing resources for an organization's needs [17].

The practical definition of optimization is the ability to match resources to workload needs as closely as possible. In the realm of cloud computing this refers to the dynamic adjustment of provisioned resources to meet the exact needs of the business process at any given moment. Optimization is a constant exercise in the avoidance of two problems: overprovisioning and underprovisioning [18].

Overprovisioning refers to the problem of having more computing resources than needed, resulting in idle assets.

Underprovisioning refers to the problem of having too few computing resources available for the current workload, and may result in reduced performance below service level agreements (SLAs), outages, or even complete system failures due to lack of compute, memory or storage.

Cloud Management refers to the "fundamental support of users of cloud services" [19]. From the practical IT management point of view, this issue refers to how much direct control the organization wants to exert on its cloud solution. This is a strategic IT decision that will impact the organization's choice of service model (SaaS, PaaS, IaaS) and delivery architecture (Public, Private, Hybrid).

The degree of control to which the organization wishes to maintain over its computing resources is largely a factor of balancing the preference of having portions of computing resources, or even the entire computing infrastructure, managed by a provider versus maintaining those resources by internal personnel.

Issues effecting this strategic calculation normally include: the level of expertise on hand, whether the organization's IT solution is starting from scratch or is migrating an existing solution, ability to control policy and protocols, specific regulatory requirements, unique security concerns, and the organization's culture and comfort with risk and third party provided services.

IX. Conclusion

This article set out to present a discussion on the underlying concepts of cloud computing, and point out the most common factors and issues that an IT manager will be confronted with, based on current trends.

The author wishes to thank Henry Chao, Thomas Hull and the IT support staff at Florida Polytechnic University for their support and contributions that made this article possible.

References Références Referencias

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M., (2009), "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, http://radlab.cs.berkeley.edu.
2. Malathi, M., (2011), "Cloud Computing Concepts," 3rd International Conference on Electronics Computer Technology (ICECT).
3. Jadeja, Y., Modi, K., (2012), "Cloud Computing - Concepts, Architecture and Challenges," International Conference on Computing, Electronics and Electrical Technologies (ICCEET).
4. Nuseibeh, H., Alhayyan, K., (2014), "Trends in the Study of Cloud Computing: Observations and Research Gaps," Proceedings of the 5th International Multi-Conference on Complexity, Informatics, and Cybernetics, (IMCIC/ICSIT, 2014), pages 38 – 43.
5. Vaquero, L. M., Rodero-Merino, L., Caceres, J., Lindner, M. (2008) "A break in the clouds: towards a cloud definition." ACM SIGCOMM Computer Communication Review, 39(1), 50-55.
6. Reed, D.A., (2008) "Clouds, clusters and ManyCore: The revolution ahead," Conference on Cluster Computing, IEEE International.
7. Popek, G. J., Goldberg, R. P., (1974), "Formal Requirements Virtualizable Third Generation Architectures," Communications of the ACM, Volume 17, Number 4.
8. Delgado, J., Salah-Eddin, A., Adjouadi, M., Masoud-Sadjadi, S., "Paravirtualization for Scientific Computing: Performance Analysis and Prediction," (2011), IEEE International Conference on High Performance Computing and Communications.
9. Vandenbeld, M., McDonald, J., (2014), "VCA-DCV Official Cert Guide." VMware Certified Associate Data Center Virtualization, VMware Press.
10. Hossny, E., Salem, S., Khattab, S. M., (2012), "Towards automated user-centric cloud provisioning: Job provisioning and scheduling on heterogeneous virtual machines," 8th International Conference Informatics and Systems (INFOS).
11. Chieu, T. C., Mohindra, A., Karve, A. A., Segal, A., (2010), "A Cloud Provisioning System for Deploying Complex Application Services," 7th International Conference on e-Business Engineering (ICEBE).
12. [Awad, O.M.O., Artoli, A.M.A., Ahmed, A.H.A., (2014), "Cloud computing versus in-house clusters: a comparative study," World Congress on Computer Applications and Information Systems (WCCAIS).
13. Singh, D., Singh, J., Chhabra, A., (2012) "High Availability of Clouds: Failover Strategies for Cloud Computing using Integrated Checkpointing
14. Algorithms," International Conference on Communication Systems and Network Technologies.
15. IBM Knowledge Center. Cited as: http://www-01.ibm.com/support/knowledgecenter

/SSPHQG_6.1.0/com.ibm.hacmp.concepts/ha_concepts_fault.htm
16. VMware's vSphere Availability Guide. Cited as: http://pubs.vmware.com/vsphere51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-availability-guide.pdf
17. Vaquero, L. M., Rodero-Merino, L., & Buyya, R. (2011) "Dynamically scaling applications in the cloud," ACM SIGCOMM Computer Communication Review, 41(1), 45-52.
18. Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I. M., Galan, F. (2009). "The reservoir model and architecture for open federated cloud computing," IBM Journal of Research and Development, 53(4), 4-1.
19. Chaisiri, S., Lee, B. S., & Niyato, D. (2012). "Optimization of resource provisioning cost in cloud computing," Services Computing,IEEE Transactions on, 5(2), 164-177.
20. Lonea, A.M., Popescu, D.E., Prostean, O., (2012) "A survey of management interfaces for eucalyptus cloud," IEEE 7th International Symposium on Applied Computational Intelligence and Informatics (SACI),

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Big Data using Cloud Technologies

By Sushma Talluri
Jawaharlal Nehru Technological University

Abstract- Cloud technology is playing a vital role in presentera to store and process massive amount of data, which leads to the convergence of cloud and big data. Cloud computing holds a tremendous promise of unlimited, on demand, elastic, computing and data storage resources. It has the potential to enhance business agility and productivity while enabling greater efficiencies and reducing costs. Big data environments require clusters of servers to support the tools that process the large volumes, high velocity, and varied formats of big data. It offers the promise of providing valuable insights that can create competitive advantage and also to explode new innovations. In this paper, I discussed how cloud and big data technologies are converged to improve quantitative decision making with minimal risk and to offer cost-effective delivery model for cloud-based big data analytics.

Keywords: *cloud, big data, technology, analytics.*

GJCST-B Classification : *H.2.8 C.2.1 C.2.3*

Strictly as per the compliance and regulations of:

Big Data using Cloud Technologies

Sushma Talluri

Abstract- Cloud technology is playing a vital role in presentera to store and process massive amount of data, which leads to the convergence of cloud and big data. Cloud computing holds a tremendous promise of unlimited, on demand, elastic, computing and data storage resources. It has the potential to enhance business agility and productivity while enabling greater efficiencies and reducing costs. Big data environments require clusters of servers to support the tools that process the large volumes, high velocity, and varied formats of big data. It offers the promise of providing valuable insights that can create competitive advantage and also to explode new innovations. In this paper, I discussed how cloud and big data technologies are converged to improve quantitative decision making with minimal risk and to offer cost-effective delivery model for cloud-based big data analytics.

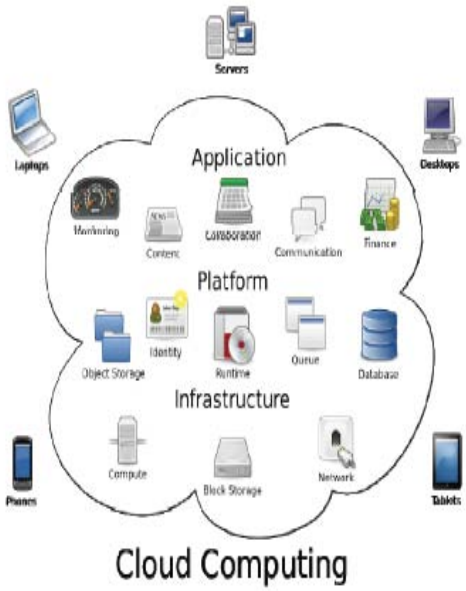
Keywords: cloud, big data, technology, analytics.

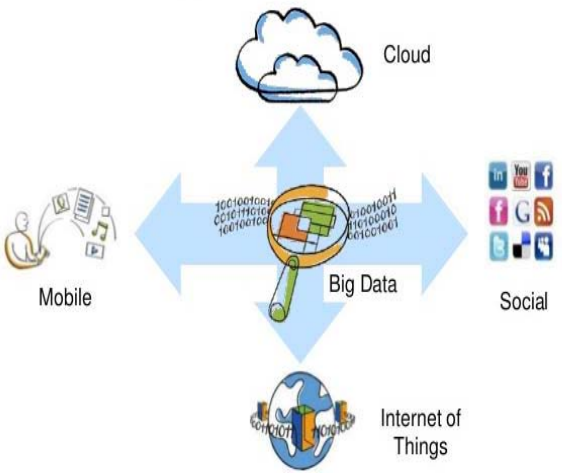
I. Introduction

a) Cloud Computing

Cloud Computing technology depends on sharing of resources than having local servers or personal devices to handle the applications. In Cloud Computing, the word "Cloud" means "The Internet", so cloud computing means which performs operations or services through the Internet.

The main objective of Cloud Computing is to make use of increasing computing power to execute millions of instructions per second. [1] It uses large group of servers with specialized connections to allocate data processing among the servers. By using this technology just there is a need to install single software in each computer that allows users to log into a Web-based service and which also hosts all the programs required by the user. In this system there will be a considerable workload shift and therefore, local computers no longer have to take the entire burden in running applications. Thus minimize the usage cost of computing resources [4]. The only thing that must be done at the user's part is to connect to the cloud. Cloud Computing consists of a front end and back end. The frontend includes the user's computer and software required to access the cloud network. Back end consists of various computers, servers and database systems that create the cloud. The user can access applications in the cloud network from anywhere by connecting to the cloud using the Internet. Some of the real time applications which use Cloud Computing are Gmail, Google Calendar, Google Docs, etc.





Author: Software Engineer Tata Consultancy Services Synergy park, Gachibowli Hyderabad. e-mail: Sushma.1249@gmail.com

a) Big Data

The term "Big Data" is used to describe massive volumes of structured and unstructured data that are difficult to process using traditional databases and software technologies.

The following are the properties of Big data:

a) *Volume:* Various aspects contribute towards increasing quantity flow of data.
b) *Variety:* In the present days data come up in all types of formats emails, video, audio, transactions etc.
c) *Velocity:* This means how fast the data is being produced and how fast the data needs to be processedto meet the demand.[5].
d) *Variability:* Along with the Velocity, the data flows can be highly incoherent with regular peaks.
e) *Complexity:* Complexity of the data also needs to be considered when the data is coming from multiple sources. The data must be linked, matched, cleansed and transformed into required formats before actual processing.

II. Converging Technologies of Cloud and Big Data

Data is becoming more valuable. Now-a-days the discussion is shifting from "What data should we store?" to "What can we do with the data?" to boost the competitiveness companies must find new approaches to processing, managing, and analyzing their data whether its structured data or more varied, unstructured formats.

Cloud computing is becoming a reality for many businesses. Among different types of deployment models private cloud deployment model often leading the way in business.[2] Cloud technology is maturing and addressing barriers to adoption with improvements in security and data integration, while IT organizations are evolving to support cloud services delivery. As a result, businesses are demonstrating growing trust in cloud delivery models. Organizations continue to store more and more data in cloud environments, which represent an immense, valuable source of information to extract by offering business users scalable resources on demand.

a) Scope of big data analytics

In the beginning day's interest in big data analytics focused first and foremost on business and social data sources, such as e-mail, videos, tweets, Facebook posts, reviews, and Web behavior. [3] But now the scope of big data analytics is growing to include data from intelligent systems, smart devices and device sensors at the boundary of networks because everywhere connectivity and the growth of sensors and intelligent systems have opened up a whole new storehouse of valuable information. By applying big data analytics to these increases richer insight to enhance machine-based decision making more cost effectively than in the past and to personalize customer experiences.

b) Cloud and big data

Cloud delivery models offer incomparable flexibility, enabling IT to evaluate the best approach to each business user's request. For example, if organizations that already support an internal private cloud environment can add big data analytics to their in-house using a cloud services provider or by building a hybrid cloud to protect certain sensitive data in a private cloud. Private clouds can offer a more efficient, cost-effective model to implement analysis of big data in-house, while enhancing internal resources with public cloud services. This hybrid cloud option enables companies to use on-demand storage space and computing power via public cloud services for certain analytics initiatives like short-term projects and provide added capacity and scale as needed. While enterprises often keep their most sensitive data in-house, huge volumes of big data owned by the organization or generated by third party and public providers may be located externally some of it already in a cloud environment. Moving relevant data sources behind the firewall can be a significant commitment of resources. Analyzing the data where it resides either in internal or public cloud data centers or in edge systems and client devices often makes more sense. Thus, cloud and big data technologies are converging to offer a cost-effective delivery model for cloud-based big data analytics.

III. Conclusion

Cloud and big data technologies continue to evolve. Big data provided through Cloud is an absolutely necessary trait for today's businesses to make proactive, knowledge driven decisions, as it helps them have future trends and behaviors predicted. As data is growing every day, the ability of integrating big data in cloud has potential for elasticity, scalability, deployment time, and reliability by offering a cost-effective delivery model.

References Références Referencias

1. Hao, Chen, and Ying Qiao. "Research of Cloud Computing based on the Hadoop platform." Chengdu, China: 2011, pp. 181 – 184, 21-23.
2. Y, Amanatullah, Ipung H.P., Juliandri A, and Lim C. "Toward cloud computing reference architecture: Cloud service management perspective.". Jakarta: 2013, pp. 1-4, 13-14 Jun. 2013.
3. A, Katal, Wazid M, and Goudar R.H. "Big data: Issues, challenges, tools and Good practices.". Noida: 2013, pp. 404 – 409, 8-10 Aug. 2013.

4. Groenfeldt, Tom. "Big Data—Big Money Says It Is a Paradigm Buster." Forbes (January 6, 2012).
5. Peer Research: Big Data Analytics: Intel's IT Manager Survey on How Organizations Are Using Big Data. Intel IT Center (August.

This page is intentionally left blank

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

To Enhance the OTP Generation Process for Cloud data Security using Diffie-Hellman and HMAC

By Gagandeep Kaur Sandhu & Er. Gurjit Singh
Punjabi University

Abstract- Cloud computing is an innovation or distributed network where user can move their data and any application programming on it. In any case, there is a few issues in cloud computing, the main one is security on the grounds that each user store their helpful data on the network so they need their data ought to be protected from any unapproved access, any progressions that is not done for user's benefit. There are diverse encryption methods utilized for security reason like FDE and FHE. To tackle the issue of Key management, Key Sharing different plans have been proposed. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To tackle this issue, we will chip away at to design new modular for key sharing and key management in completely Homomorphic Encryption plan. In this paper, we have utilized the symmetric key understanding algorithm named Diffie Hellman, it is key trade algorithm with make session key between two gatherings who need to speak with each other and HMAC for the data integrity OTP(One Time Password) is made which gives more security. Because of this the issue of managing the key is expelled and data is more secured.

Keywords: *OTP, HMAC, diffie-hellman, cloud security, FHE, FDE.*

GJCST-B Classification : *H.2.7 C.2.1 C.2.3*

Strictly as per the compliance and regulations of:

To Enhance the OTP Generation Process for Cloud data Security using Diffie-Hellman and HMAC

Gagandeep Kaur Sandhu[α] & Er. Gurjit Singh[σ]

Abstract- Cloud computing is an innovation or distributed network where user can move their data and any application programming on it. In any case, there is a few issues in cloud computing, the main one is security on the grounds that each user store their helpful data on the network so they need their data ought to be protected from any unapproved access, any progressions that is not done for user's benefit. There are diverse encryption methods utilized for security reason like FDE and FHE. To tackle the issue of Key management, Key Sharing different plans have been proposed. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To tackle this issue, we will chip away at to design new modular for key sharing and key management in completely Homomorphic Encryption plan. In this paper, we have utilized the symmetric key understanding algorithm named Diffie Hellman, it is key trade algorithm with make session key between two gatherings who need to speak with each other and HMAC for the data integrity OTP(One Time Password) is made which gives more security. Because of this the issue of managing the key is expelled and data is more secured.

Keywords: OTP, HMAC, diffie-hellman, cloud security, FHE, FDE.

I. Introduction

Cloud computing is the earth which gives on-demand and helpful access of the network to a computing resources like storage, servers, applications, networks and the other services which can be discharged minimum effectiveness way. The five key characteristics made by cloud design. Cloud design likewise advances the accessibility [5]. User retrieved data and changed data which is stored by client or an association in centralized data called cloud. Cloud is a design, where cloud service provider gives services to user on demand and it is otherwise called CSP stands for "Cloud Service Provider" [3]. It implies that the user or the client who is using the service needs to pay for whatever he/she is using or being utilized and served. There are three deployment models and three services models defined by NIST, theses are:

Author α σ : Bhathal Student, Assistant Professor, Department of Computer Science, Punjabi University, Patiala, Punjab. e-mail: sandhugagandeep200@gmail.com

a) Service Models: There are three service models of cloud-

i. *Software as a Service (SaaS)*

This is the ability of using applications which are running on cloud infrastructure. The users access these applications through internet associations. These kinds of clouds offer the usage of some particular business strings that gives particular cloud abilities. For E.g. GMAIL, Facebook [2].

ii. *Platform as a Service (PaaS)*

It gives the computational resources on which services and applications can be host and create. For E.g. Online Photo Editing, Google Docs, YouTube [12]

iii. *Infrastructure as a Service (Iaa* S)

This is the ability of doing processing, storing and run software which is given to the buyer. It's additionally alluded as the "Resource Code" which gives resources as the services to a user. This work is finished by the service provider. For E.g. Host Firewalls [6].

b) Deployment Models

Cloud services are mainly available in the three types of cloud. These clouds are as follows-

i. *Public Cloud*

In this cloud, resources dispensed are publically. Applications in this cloud are on pay-per-use premise. Public clouds can be managed by government organizations or business. For E. g. Sky Drive and Google Drive [2].

ii. *Private Cloud*

In this cloud, resources are constrained and used within an association. It is more secure as representatives in an association can access the specific data as it were. For E. g. Banks [12].

iii. *Hybrid Cloud*

In this cloud, there is a combination of both Public and Private cloud. The services within the association are control by the client and resources which should be conveyed remotely are controlled by the service provider [12].

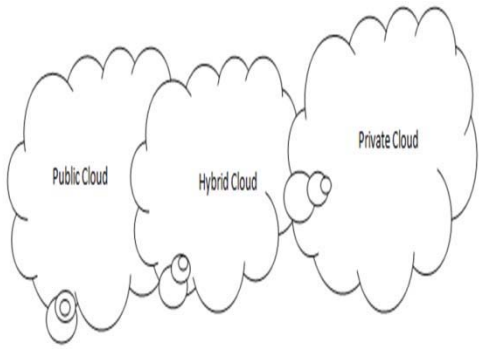


Fig. 1.1 : Deployment model of Cloud

c) Cloud Computing Security

Network security, information security and many other security sorts like the PC security together make the expression "Cloud Security" because it comprise the greater part of the security system as given above. It gives the expansive set of innovations, policies and controls that are used to secure the data and applications exist with the cloud computing environment [8]. It is not the result of PC security like hostile to viruses and against spam's. Security is the most concerning point to any service. Outer security or internal security required to every field. Just security guarantees the privacy and integrity the cloud data. There are many security loopholes exist in the service. There are many sorts of security issues exist like DDOS, Man in the middle and so on. Some security sorts include:

i. *Outages*

This term alludes to the issue of the user where he/she is not ready to access services because of the provider being down. Assume there is some imperative business meeting and user require a document for the presentation and provider's site is down. This may happen part of times [8].

ii. *Data Loss*

Due to lack of security data may be lost during uploading on cloud because of nearness of malicious hub [11].

iii. *Phishing*

It is an email misrepresentation trick which is directed with the assistance of network investigation stream tool to concentrate information from the server.

II. Review of Literature

In this paper [1] they proposed distinctive systems and their benefits and bad marks like Message Authentication Code (MAC) which protect the data from integrity. The proprietor of any information checked the data integrity by recalculating the message authentication code of data got by others however recalculation is conceivable if the measure of data is huge. A hash tree is used for extensive files. Outsider auditor is used to alleviate the substantial data into little parts of maintenance and security. The proposed algorithm depicts data integrity and dynamic data operations. They use encryption to ensuring the data integrity. Public key is likewise defined which is based on homomorphic authenticator. A hash function is used for evidence of retriveability. The proposed algorithm has a main drawback that it require usage of the higher resources cost. In this paper [2] Dynamic versatile token application is introduced. This is the application in cellular telephones which is used to produce a code with the assistance of OTP (One Time Password). This OTP code is used just for one an opportunity to login session. In this paper, they depict one of the techniques for OTP. There are two phases in it Registration phase and Login phase. User first enlists itself by fill credentials in the structure and then enters to the Login phase. In login phase, OTP will produce for the login session. OTP is produced by three parameters: The present time, 4-digiti PIN code and Init-mystery. This code is legitimate for three minutes as it were. This guarantees protection against eavsdroppers attack and man-in-middle attack. Henceforth, they demonstrate OTP is extremely secure. In this paper [3] a design and engineering is recommended that can scramble and unscramble the file at the user side which gives data security in both cases while user is very still or is transferring data. In this paper they used the Rijndael Encryption Algorithm alongside EAP-CHAP. This algorithm has five stages which should be take after for the data security. The users are dependably worry about the privacy protection and security issues before storing their data on cloud. So in this the attention is on client side security in which just the approved user can access the data. Regardless of the possibility that some intruder (Unauthorized user) gets access of the data then the data won't be unscramble. Encryption must be finished by the user to give better security Algorithm. For this, Rijndael Encryption algorithm is used. In this paper [4], two strategies are talked about: Virtualization and Multi-tenancy which gives security about cloud computing. Data is sorted out by outsider organizations that offer Saas and PaaS which is critical for the security. In this way, Virtualization and Multi-tenancy strategies are used for the security purposes. Virtualization is a method for making a physical PC function as though it were two or more PCs where each non-physical or virtualized. There are two sorts of virtualization: Full virtualization and Para virtualization and two designs of virtualization: Hosted and Hypervisor engineering. Multi-tenancy is the capacity to give computing services to different clients by using a typical infrastructure and code base. Multi-tenancy can be connected to various levels i.e. application level, middleware level, operating system, equipment level. Then security of virtualization and multi-tenancy has been talked about. In this paper [5] they talked about various issues identified with cloud

computing security. To protect cloud computing system and to counteract different attacks many security instruments have been created. To enhance the security of cloud computing new innovations has been created by the analysts. Distinctive sorts of attacks like SYN flood, malware injection, account hijacking are examined in this paper. The main center of this paper is on detecting and preventing SYN flood in cloud computing. The creator created two algorithm one detecting algorithm and one preventing algorithm. They will actualize and test these algorithms on cloud computing.

III. Diffie-Hellman and OTP

Diffie Hellman was the primary public key algorithm or we can say that it is symmetric key agreement ever invented, in 1976. Diffie Hellman key agreement protocol is [6]:

1. It allows exchanging a secret key between two parties.
2. Exponential key agreement
3. Requires no prior secrets

a) Definition of Diffie Hellman

Before establishing a symmetric key, the both the two parties need to pick two numbers n and p. Give n a chance to be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the issue of computing the estimation of p^{ab}(mod n) from the known estimations of p^a (mod n) and p^b (mod n).The setup of Diffie Hellman algorithm

Assume that we have two parties Alice (Master) and Bob (Slave), they need to convey to each other.

They don't need the eavesdropper to know their message.

Alice and Bob concur upon and make public two numbers n and p, where n is a prime number and p is a primitive root mod n. Anybody has admittance to these numbers.

Table 1 : Private computations

Alice	Bob
Choose a secret number a. Compute M≡ p^a (mod n)	Choose a secret number b Compute S≡ p^b(mod n).

Generated public values are exchanged.

- Alice sends M to Bob ==M
- S= Bob sends S to Alice
- Alice calculate the number K≡ S^a ≡(P^a)^b (modn).
- Bob calculate the number K≡M^b≡(p^b)^a (mod n).

Here Alice and Bob have the same key that is K=p^{ab} (mod n).

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to trade data, both concur on a symmetric key. For encryption or decryption of the messages symmetric key is used. We realizes that Diffie Hellman algorithm is used for just key agreement or key trade, however it doesn't used for encryption or decryption. Before starting the correspondence, secure channel is set up between both the parties [5]. Both parties select their own particular random number. On the premise of the chose random numbers, secure channel and shared key is built up.

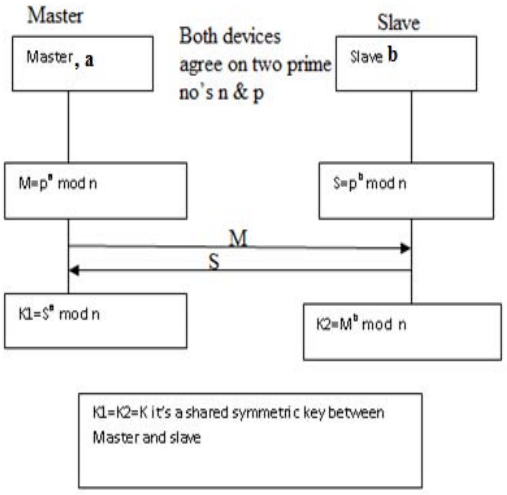


Fig.1.2 : Diffie-Hellman Key exchange

Figure1.2 demonstrates that Master and Slave needs to speak with each other. To begin correspondence both parties need to build up secure channel. To set up secure channel, two random prime number p and n are chosen, both gadgets are concurred on these two numbers. Chosen p and n are the public numbers. Both parties, say gadget 1 get to be master and gadget 2 get to be slave; both master and slave select their private numbers "an" and "b" individually. Master and slave use their public and private number and computed their private keys [15].

Master computes:

M= p^a mod n

Slave computes:

S= p^b mod n

Now both master and slave exchange their private keys such as 'M' and 'S'. After getting 'M' and 'S', master and slave calculates the secret keys such as K1, K2.

From S, master computes:

K1= S^a mod n

From M, slave computes:

K2= M^b mod n

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of K1 and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (K) of both parties. For decryption of

messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used [16].

a) One Time Password

Password is used for authentication by all the business and association. In addition Static passwords have many impediments. Password can be get hacked. Lackadaisical representative may note down passwords some place, system with spared passwords might be used by different users or a malicious user may reset all passwords just to make destruction. So it is exceptionally useful to use dynamic password i.e. one time password [10]. Dynamic passwords are more secure when contrasted with static. There is no compelling reason to record these passwords and recollect these passwords. For each login session every time another password is produced. One time passwords are more reliable and user friendly also for authentication. OTP generation should be possible by different OTP generation algorithms for generating strings of passwords. OTP guarantees security. This prompts authenticating them again and again over the period of time for each login session. To maintain a strategic distance from the overhead we can use OTP for multi cloud environment.

IV. Proposed Methodology

There are many encryption algorithms to give security to the cloud. "Fully Homomorphic" is more reliable. It gives more privacy and security as contrast with plan of "Full Disk Encryption". The main issue which is there in Fully Homomorphic Encryption is a key storage, key management, Access control and Data Aggregation list maintaining. To tackle issue of Key management, Key Sharing different plans have been proposed in a years ago. The different security attacks are conceivable in these plans. The outsider auditor is the plan for key management and key sharing. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To take care of this issue, In this thesis we will take a shot at to design new model for key sharing and key management in fully Homomorphic Encryption plan. In this work, we find that fully homomorphic encryption system is more effective than full disk encryption. Yet, the main issue exists in fully homomorphic encryption is of key management and key sharing which decreases the reliability of the plan. For key management and key sharing, improvement has been proposed in the encryption plan and upgrade is based on Diffie-hellman algorithm and HMAC and OTP is created on the premise of mystery key produced from Diffie-hellman algorithm. This algorithm makes session key amongst user and cloud. Every time new key is produced between two preceding correspondence selected node suppose user1

1. Login
2. Key generation
   2.1 Enter prime numbers
   2.2 Enter random numbers by client and cloud service provider
   2.3Secret key generation and secure channel establishment
3. OTP (One Time Password) generation
   3.1 cloud server will set count1=0, count2=0...count5=0 for respective user at its side.
   3.2 Cloud Server will request for the OTP from user 1
   3.3 user1 enter (secret key+count) as OTP
   3.3 server match it because server knows both secret key and count of each user.
   3.3.1: count1++; // so for user 1 it will be count1=1; for remainig user their count will be still 0;
   3.3.2 if (secret_key+count(x) == secret_key+count(y))
   { Access granted;
   display message by server : print ("please enter the operation");}
   else{ display message by server: print(" wrong password, your login number is count1);}
4.4 clinet will enter the operation using HMAC digest
   4.4.1 : hmac(already generated secret key || v, file1,ver1 || sha1)
   { if(ope==v)
   { server will check the file name and version;
   if (file1,ver1== file1,ver1)
   {
   printf("file is valid"); }
   else {
   print (file is invalid, please replace the file)
   }}
if(ope==I) { insert new file file2 }
5. encryption/decryiton
6.data operation
7.logout;

note: // 1.at client side, user will enter prime number, random number for generating secret keys, once generating secret key user will enter otp , after inserting otp, user will enter operation(Insertion) with corresponding file name(file1 or file2).

V. Exprimental Results

The whole scenario has been implemented on MATLAB tool.

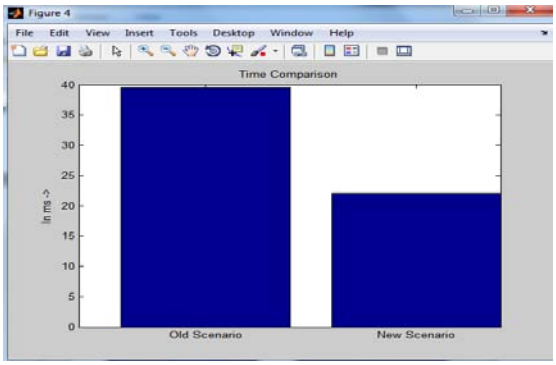


Fig. 1.3 : Comparison Graph

As appeared in figure 1.3, the comparison amongst previous and proposed methodology is appeared as far as delay. The delay in previous system is increasing, when numbers of trade messages are increased. In the proposed approach the delay is less because of increasing the number of message.

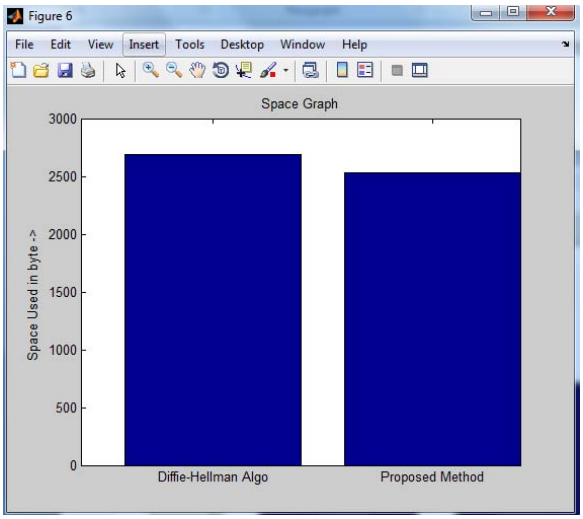


Fig.1.4 : Comparison with Diffie Hellman in terms of used bytes

As appeared in figure 1.4, the comparison amongst previous and proposed methodology is appeared as far as used bytes. The used byte in previous method is increasing, when numbers of trade messages are increased. In the proposed approach the data utilization is less when contrasted with existing strategy.

VI. Conclusion

Cloud computing is the environment which gives on-demand and helpful access of the network to a computing resources like storage, servers, applications, networks and the other services which can be discharged minimum productivity way. In this user can store their data and use diverse services and pay according to those services. The main component is security that how we can store our data while storing into the cloud. In this thesis, we audited two most prevalent procedures for cloud data encryption. These systems are full disk encryption and fully homomorphic encryption. In this work, we find that fully homomorphic encryption method is more proficient than full disk encryption. Yet, the main issue exists in fully homomorphic encryption is of key management and key sharing which lessens the reliability of the plan. For key management and key sharing, improvement has been proposed in the encryption plan and upgrade is based on Diffie-hellman algorithm and HMAC and OTP is produced on the premise of secret key created from diffie-hellman algorithm. This algorithm makes session key amongst user and cloud. Every time new key is produced between two preceding correspondence. This decreases the time happens in management and sharing of keys and secure channel is set up between both i.e. user and the cloud service provider. The simulation demonstrates that proposed improvement is more proficient and reliable than the existing one.

References Références Referencias

1. Bhavna Makhija, VinitKumar Gupta, 2013 "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345.
2. Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4.
3. Sanjoli Singla, Jasmeet Singh, 2013 "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235.
4. Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 "Cloud Computing Security" International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39
5. Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946.
6. Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II.
7. Craig Gentry, 2009,"full homomorphic encryption scheme" .
8. Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45.

9. Deyan Chen, Hong Zhao, 2012" Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, pp 647-651.
10. Deepanchakaravarthi Purushothaman[1] and Dr.Sunitha Abburu[2] ,2012" An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1.
11. Dian-Yuan Han, Feng-qing Zhang, 2012 "Applying Agents to the Data Security in Cloud Computing" International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128.
12. Dr Nashaat el-Khameesy, Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3.

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Review on Integration of Quantum Processor Services with Recursive Quantum Network in Cloud System

By M. M. Fazle Rabbi, Md. Masudul Islam & Mijanur Rahaman
Bangladesh University of Business and Technology

Abstract- Cloud computing system is based on a vast network. They provide different services, transmit valuable data and store them in remote storage. Making the network security system stronger and faster is one of the greatest challenges to secure the cloud. Since recent trends are going on quantum technological research, there is a way to secure cloud system using quantum internet. However, recently developed recursive quantum repeater networkfor large-scale internetwith cloud system could bring revolutionary change in cloud computing services. Our paper's main view is to show recent progress of quantum internet and recursive quantum network. In addition, we will review a simple model to integrate quantum processor services in cloud with recursive quantum network architecture for reliable, secure and faster cloud computing services.

Keywords: quantum chip, recursive network, quantum repeater, cloud, network layer, entanglement, QCaaS, QRNA.

GJCST-B Classification : C.2.1 C.2.3

Strictly as per the compliance and regulations of:

A Review on Integration of Quantum processor Services with Recursive Quantum Network in Cloud System

M.M. Fazle Rabbi [α], Md. Masudul Islam [σ] & Mijanur Rahaman [ρ]

Abstract- Cloud computing system is based on a vast network. They provide different services, transmit valuable data and store them in remote storage. Making thenetwork security system stronger and faster is one of the greatest challenges to secure the cloud. Since recent trends are going on quantum technological research, there is a way to secure cloud system using quantum internet.However, recently developed recursive quantum repeater networkfor large-scale internetwith cloud system could bring revolutionary change in cloud computing services. Our paper's main view is to show recent progress of quantum internet and recursive quantum network. In addition, we will review a simple model to integrate quantum processorservices in cloud with recursive quantum network architecture for reliable, secure and faster cloud computing services.

Keywords: quantum chip, recursive network, quantum repeater, cloud, network layer, entanglement, QCaaS, QRNA.

I. Introduction

Cloud computing is globalization for internet computing. It is a revolutionary system but still faces some vulnerability in many cases. Many threats such as, data loss, privacy issue, data theft, vendor security, data locality etc. has shown up. Using most powerful encryption system or secured medium to transfer data over cloud is not properly safe yet.

Because intruders have a chance to eavesdrop client's information at any time in this classical system. Cloud computing is 50 year old business model, which still needs to expand and overcome limitations that prevent the full use of its potential.[1]Clouds must be able to define computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs.[2]

Author α: Lecturer, Dept. of CSE, Bangladesh University of Businessand Technology, Mirpur-2, Dhaka-1216.
e-mail: rabbi102@gmail.com
Author σ: Lecturer, Dept. of CSE, Bangladesh University of Businessand Technology, Mirpur-2, Dhaka-1216.
e-mail: masudulislam11@gmail.com
Author ρ: Asst. Professor, Dept. of CSE, Bangladesh University of Businessand Technology, Mirpur-2, Dhaka-1216.
e-mail: riponcse.it@bubt.edu.bd

Secure cloud computing concerns some issues like secure cryptographic key distributions, strong network system, fast processing etc.

All these system are based on classical method, they are electronically and virtually safe. However, they are not safe enough to rely because advancement of technology and method is a hint of upcoming problem. However, new concept of quantum physics for information technology is making a way to make safe and faster cloud system. All we need to integrate the quantum network system with cloud system. In order to established Quantum internet networks using classical optical technology it needs storage to store quantum information and quantum repeater as amplifier for long distribution of entanglement.

As we know, there is a possibility of QCaaS (Quantum Computing as a Service) in cloud system.[17]In here our paper is reviewing the model of integration cloud with recursive quantum internet for further more secured and faster cloud computing.

At first, we will know about some facts aboutcloud, classical networks and quantum networks, entanglements as well as recursive quantum repeater network for our further review on integrating quantum internet with cloud.

a) Cloud System

Understanding basic system of how cloud-computing works in network is important. It consist two layers; user interface layer and backend layer consist of hardware and software services. This cloud uses a network layer to connect users' endpoint devices. Present network architecture of cloud system consist router, firewall, Ethernet switch, fiber channel switch, Server Load balancing etc. Fig. 1[3] shows present architecture of cloud computing network. However, these architecture cloud change based on different service module. This complex structure is costly and has different vulnerabilities. As we see, each part is connected to the internet at a time so making the network system more secure and faster is one of the challenges. This why we will review a new model of cloud system integrated with recursive quantum internet.

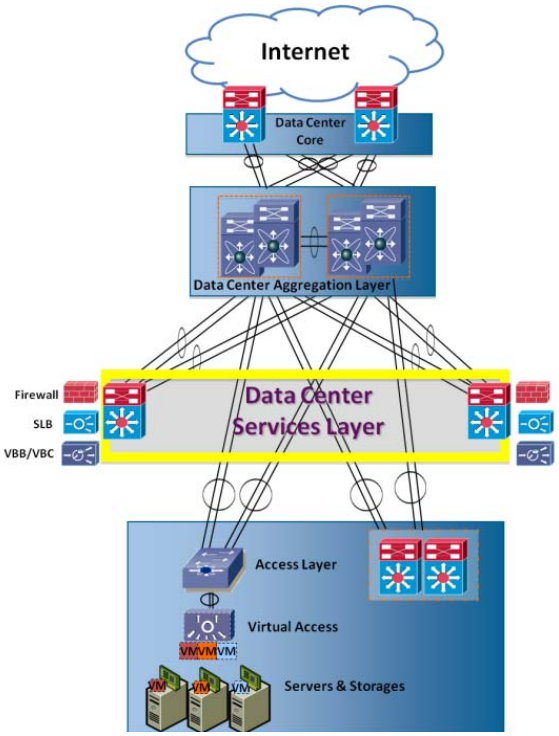


Fig. 1: Cloud Network Architecture

b) Superposition & Entanglement

Superposition and Entanglement are two vital point for our quantum network system to secured QKD and faster information travel. If a Qubit is $|0\rangle \pm |1\rangle$then the equal superposition state of the Qubit is $(|0\rangle \pm |1\rangle)/\sqrt{2}$ which represent 45° linear polarization. This means there are immense possibilities of information bits within a single photon. This single Qubit representation is simpler to see but in the case of two Qubit, they show a new behavior called entanglement. Entanglement happens when a pair of particles interacts physically. Entangled photon particles spin vice-versa even if we observe it from a far distance. Fig. 2 shows a simple view of entanglement for a pair of photon particle. It shows if we observe one of the photon from the pair then we can assume easily the other one's spin status not matter how far they are. This is a key technique for instant data teleportation in Quantum networks system.

c) Recursive Networking

In classical network system can be used or add all over the network topology so that the complex subnet structure stay hidden and it can reuse single protocol for different layers in a protocol stack. In Fig 3. A simple recursive network is presenting where each node in the fig can actually represents a complete network itself. Here the black dot represents simple repeater, red dot represents router and blue dot represents nodes in request states.[4]

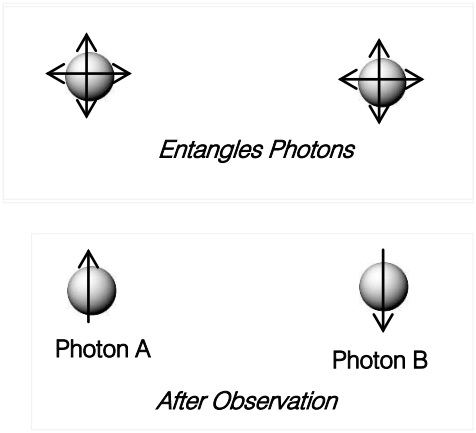


Fig. 2 : Entangled Photons

A recursive network architecture reuses single flexible protocol for the different layer of protocol stack to avoid recapitulation of implementation and dynamic composition of services.[5] Before we introduce recursive quantum network with cloud system it's essential to know why new network architecture like RNA is needed. Current classical internet architecture has been remodeled by adding different extension layer, protocol and facilities such as, SHIM6, HIP, SCTP, TLS, BEEP etc.[6]But in many cases these extensions affects the nature of conventional protocol stack and sometimes it repeats services which are available at existing layer. That is why recursive network model unifies basic properties of protocols and reuses components services to avoid these shortcomings. Another similar classical network recursion is shown in Fig. 4, a simple recursive classical network where the embedded subnet works as router at the higher level, this embedding could happen in many times, on top of its existing embedding and that's how it works like a recursive network.[7]

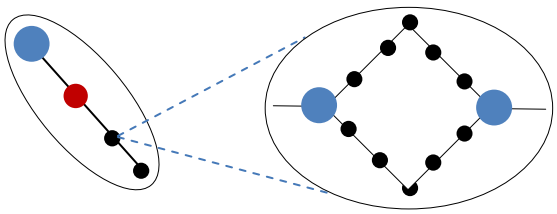


Fig. 3 : A simple view of classical recursive network system

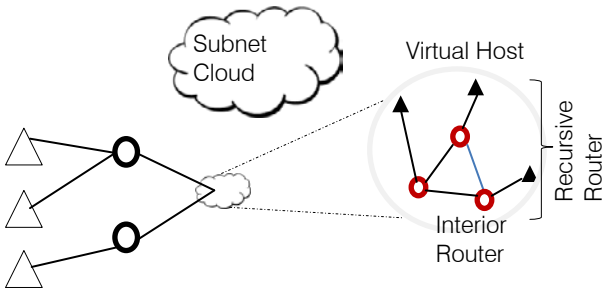


Fig. 4 : Classical recursive networking

II. Quantum Internet & Quantum Repeater

The Quantum Internet is a concept of information travels to the end users in a quantum state through an optical fiber link using entanglement. The main thing to create a quantum internet is the capability to encrypt information on single photons of light that can be produced on demand. There is no quantum communication scheme so that is why we use a classical communication scheme to transmit quantum information using infrared photon through optical fiber. However, photons decay exponentially as they propagate so a quantum repeater is used to amplify the transmission as long as possible. Simple quantum network structure using entanglement is shown in Fig. 5. Just like in classical perspective amplifiers is used to extend the data communication we use here quantum repeater to pass data through one fiber links to another fiber links. Our main concern for Quantum repeater is to ensure that the whole system is compatible with standard fiber optical communication system for long distance transmission.

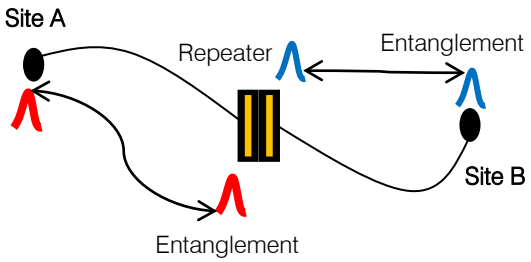


Fig. 5 : Quantum repeater internet using photon entanglement

III. Recursive Quantum Repeater Network

In 2011, a team of Van Meter, Joe Touch and Clare Horseman presented a better quantum internet system by adopting classical recursive network. As we know classical network forward the data packet on towards its destinations but quantum internet does not sends the data rather than it recreate quantum states by requesting for the execution of operation. In the(QRNA) Quantum Recursive Network Architecture system the developer team contributes a solution for 4 major scaling problem such as: ensuring interoperability among technologies that are heterogeneous (at both the physical and logical levels), reconciling the competing needs and policies of independent organizations (including the desire to keep information about the network internals private), choosing a technical approach for the routing, naming, and resource discovery problems that is robust in the face of this heterogeneity and federated operation and managing communication requests using incomplete, out-of-date information about the dynamic state of the network, including availability of resources and topological change occurring as nodes join and leave, and network links go up and down.[8]This model gives quantum internetwork system a possibility in large-scale deployment which is essential for world-wide cloud computing services.

IV. Recursive Quantum Repeater Network and Quantum Processor Services in Cloud

In 2015, the Cloud Security Alliance formed a new working group called the Quantum-Safe Security Working Group (QSSWG).[9] So secured cloud computing is a provocative question at present. Judging this facts unify present fiber network technology with Quantum physics features we could build a strong repetitive and large network system, so that cloud data passing and storing will more secured and reliable. Our approach is to unify different progress in Quantum internetwork system in recent years and propose a minimum view of model to integrate cloud with Quantum internet.

One of the greatest challenges for implementing a globally distributed quantum computer or a quantum internet is entangling nodes across the network.[10]

Building peer-to-peer small quantum network system is not so hard. However, in the case of large quantum network there are difficulties to deal with de-coherence and photon decay. Therefore, there is a method to build large quantum network using photon entanglement by distributing quantum state. In this system, the network nodes are Quantum repeaters, which are equivalent to classical internet routers. In entanglement, behavior pair of entangled particle is called Bell pair. This entanglement increases the photon transmission distance through networks. Research on the physical mechanisms for transmitting quantum states typically assumes transmission through a fiber, but free-space optical links and even satellite links can also be used, with repeater nodes at each end of the link.[11]Since our present technology is not fully quantum specialized and the quantum computer still not available so we have to take help from classical network control system to design a unified Quantum Repeater. A unified architecture proposed by Van Meter, Joe and Horsman team to build classical recursive network concepts to extend data distribution. This system claimed to be very useful to build arbitrary distributed states such as Bell pairs and GHZ, W and Cluster state.[12]In order to safely long-distance Distribute Quantum Key through a large network system there must be an error proof request-response protocol. The request naturally produced in the nodes and processed through a set of protocol

software modules.[13]In their proposed system, the building block for distributed algorithm is a core group of entangled states, which supports direct distributed execution of any quantum algorithm. In quantum repeater, network recursion is natural model because of purification, entanglement, swapping and Calderbank-Shor-Steane (CSS)[14]

Fig.6shows a simple structure of Quantum repeater network, which can distribute QKD over approximately 50km to 3000km where each Quantum Repeater node contains Error correction purification, Entanglement distribution, initialization and measurements.

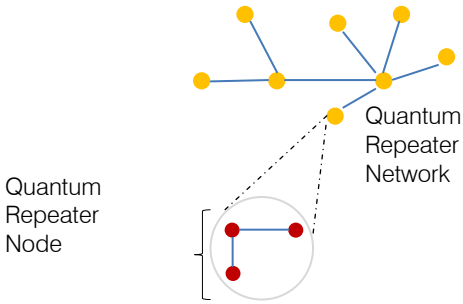


Fig. 6 : Simple structure of Quantum repeater network & nodes

Another progress in Quantum internet system is to add a quantum SIM chip in cloud architecture so that anyone can process any quantum algorithm application in web browser using internet. A group of scientist in University of Bristol, UK has already done this part experimentally. According to their claim a small quantum chip connected to the internet will works by guiding two photons through a series of optical channels. As the photons pass through the 2-Qubit chip, they become entangled, meaning that a measurement on one influences the outcome when measuring the other. Programming the computer involves tweaking the extent of this entanglement to produce different computations.[15]However, this is a limited version of Quantum processor service; we need to implement it in large scale for public. And that's why we propose to unite recursive quantum repeater network system for large-scale communication with the quantum cloud chip services.

Because of QKD is vulnerable to distance and loss factor so we could use recursive quantum repeater network model with an extra layer of Quantum chip service so that anyone can process Quantum algorithm over the internet using existing fiber optical technology.

In our proposed approach, we could add the Quantum chip service in our physical layer of present network architecture thatprovides users a secured and faster quantum processing over internet. The quantum SIM chip we are using is actually open web interface simulator. This high-level application interface helps us to do experiments on various quantum application theory. This API could integrate in Application layer of QRNA.We merge the recursive quantum repeater system in physical layer so that processed Quantum encrypted key could travel through internet to the end user in cloud system in large-scale. This integrated approach will increase the performance the Quantum internet over cloud system.Fig. 7 is a simple structure for our proposed model how the end user cloud use Quantum processor which is interconnected with recursive Quantuminternet system over cloud.

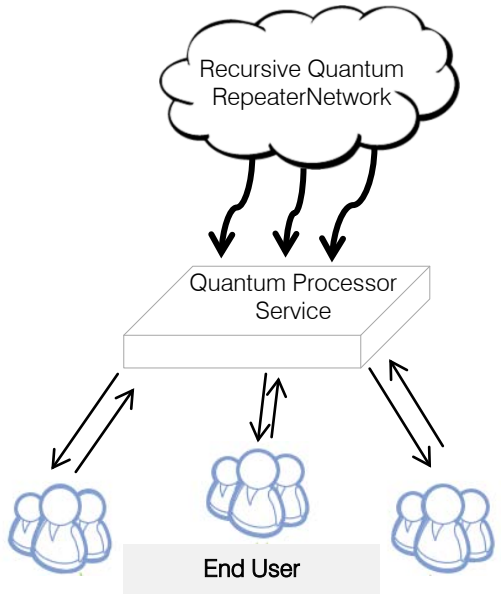


Fig. 7 : Tentative model view of integration recursive quantum network with Quantum Processor service

V. Conclusion

A cloud system is all over the world is truly a large-scale system. In classical networking approaches data moves through network using source applications, but in normal quantum networking system it creates distributed entangled quantum states as well as transport the data one to another places. In advance, Quantum recursive Network system it asks a node or network to contribute vigorously in the view of large state network. Therefore, the major issue of large-scale distributed computing could be solved using QRNA. We hope within next few years, hybrid technology of quantum internet will deploy. So that Quantum processor with quantum storage system in cloud system will add with microwave–optical transducers for long-distance optical communication.[16]In our paper we have showed a simple view and recent progress of integrated quantum network system with quantum processor chip in cloud, but there could be more of it. Not only a single quantum chip but also all the major cloud application could be attached with recursive quantum network so

that distributed quantum computing gets availability all over the internetwork system. We hope QCaaS (Quantum Computing as a Service) would be more efficient with the integration with recursive quantum repeater networks.

References Références Referencias

1. F. Durao, J. F. S. Carvalho, A. Fonseka and V. C. Garcia, "A Systematic Review on Cloud Computing", The Journal of Supercomputing, Vol. 68, Issue 3, pp. 1321-1346, 2014.
2. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th Utility", Future Generation Computer Systems, Elsevier, Vol. 25, pp. 599-616, 2009.
3. International Journal of Networks and Communications 2012, 2(5): 105-111
4. Rodney VAN METER, Joe TOUCH and Clare HORSMAN, Recursive Quantum Repeater Networks, No. 8, pp.65-79, (2011)
5. Joseph D. Touch, Yu-Shun Wang, Venkata Pingali, "A Recursive Network Architecture", Oct, 2006.
6. Joseph D. Touch, Yu-Shun Wang, Venkata Pingali, "A Recursive Network Architecture", Oct, 2006
7. Rodney VAN METER, Joe TOUCH and Clare HORSMAN, "Recursive Quantum Repeater Networks", No. 8, pp.65-79, (2011)
8. Rodney VAN METER, Joe TOUCH and Clare HORSMAN, "Recursive Quantum Repeater Networks", No. 8, pp.65-79, (2011)
9. Cloud Security Alliance(2009), Quantum-safe Security Working Group. Retrieve from:https://cloudsecurityalliance.org/group/quantum-safe-security/
10. H. J. Kimble, "Review Article The quantum internet", Nature 453, 1023-1030, dx.doi.org/10.1038/nature07127
11. P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between Space and Earth". New Journal of Physics, 10:033038, 2008.
12. Rodney VAN METER1, Joe TOUCH2 and Clare HORSMAN3, "Progress in Informatics", No. 8, pp.65-79, (2011)
13. Rodney VAN METER1, Joe TOUCH2 and Clare HORSMAN3, "Progress in Informatics", No. 8, pp.65-79, (2011)
14. R. Calderbank and Peter W. Shor. "Good quantum error-correcting codes exist", Physical Review A, 54:1098–1105, 1996.
15. New Scientist (2013), Quantum chip connected to internet is yours to command. Retrieve from: https://www.newscientist.com/article/dn24159-quantum-chip-connected-to-internet-is-yours-to-command/
16. H. J. Kimble, "Review Article The quantum internet", Nature 453, 1023-1030, dx.doi.org/ 10.1038/ nature 07127
17. Mijanur Rahaman, Md. Masudul Islam. "An Overview on Quantum Computing as a Service (QCaaS): Probability or Possibility", doi:10. 5815 /ijmsc. 2016.01.02, 2016, 1, 16-22

Global Journals Inc. (US) Guidelines Handbook 2016

www.GlobalJournals.org

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 repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan 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.

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 briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

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 though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

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

Final Points:

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

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

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

General style:

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

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

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

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

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

Abstract:

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

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

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

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

Approach:

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

Introduction:

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

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

Approach:

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

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

Procedures (Methods and Materials):

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

Materials:

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

Methods:

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

Approach:

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

What to keep away from

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

Results:

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

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

Content

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

What to stay away from

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

Approach

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

Figures and tables

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

Discussion:

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

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

Approach:

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

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

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