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

Global Journal

of Computer Science and Technology: B

Cloud & Distributed

Highlights

Attestation Architecture

Cyber Forensic Investigation

Data Intensive Application

New Efficient Cloud Model

Discovering Thoughts, Inventing Future

VOLUME 15 ISSUE 1 VERSION 1.0

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

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

Volume 15 Issue 1 (Ver. 1.0)

Open Association of Research Society

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

Engage with the contents herein at your own risk.

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

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

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

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

Global Journals Inc.

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

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

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

Packaging & Continental Dispatching

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

Find a correspondence nodal officer near you

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

eContacts

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

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board (Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

President Editor (HON.)

Chief Author (HON.)

Dean & Editor-in-Chief (HON.)

Contents of the Issue

Global Journals Inc.

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Forensic Investigation and Exploration on Cloud Computing Environment

By Dr. S Santhosh Baboo & S. Mani Megalai

SCSVMV University, India

Abstract- Cloud service providers are providing more services on demand. Usage of Cloud in IT Industry, Educational Institution, Social network, Medical Field and other business Industry are tremendously increased. This increases the more criminal activity on cloud. There is a need for forensic capabilities which support investigations of crime in cyber cloud. We need better secured model for cloud deployment and forensic investigation techniques to extract evidence from cloud-based environments in case of any cyber attack. This paper discusses the comprehensive models that provides cyber Forensics capabilities on cloud computing.

Keywords: cloud computing; forensic; cybercrime; forensic investigation.

GJCST-B Classification : C.2.4, C.2.1

Cyber Forensic Investigation and Exploration on Cloud Computing Environment

Dr. S Santhosh Baboo α & S. Mani Megalai σ

Abstract- Cloud service providers are providing more services on demand. Usage of Cloud in IT Industry, Educational Institution, Social network, Medical Field and other business Industry are tremendously increased. This increases the more criminal activity on cloud. There is a need for forensic capabilities which support investigations of crime in cyber cloud. We need better secured model for cloud deployment and forensic investigation techniques to extract evidence from cloud-based environments in case of any cyber attack. This paper discusses the comprehensive models that provides cyber Forensics capabilities on cloud computing.

Keywords: cloud computing; forensic; cybercrime; forensic investigation.

I. Introduction

Cloud Forensic system has the greater demand in this generation. Since the cloud computing has more advantages for the business, most of the companies are deploying their applications on cloud which leads to more cyber attack on cloud. This brings more research for the digital forensics on cloud to identify the criminals in the virtual environment. Since there is constant increase in the cyber attacks across countries in multi-tenant cloud with new trends, the Investigation system is necessary to meet the current challenges in the distributed environment.

Cyber Forensic Investigation and Exploration for cloud computing brings new technical and legal challenges. The forensic investigation on cloud computing is being different by the evidence distributed on virtual environment, less control of physical access, and more secured policies and methods to be followed by the service providers to improvise integrity and authenticity. The difficulty persists in cloud environment in acquisition of remote data, huge data volumes, data ownership and the distributed data across virtual environment.

Generally, if any cyber attack happens on any environment, there should be options to perform their investigations on the server without involving third party service providers. In the Cloud computing environment, service providers have control over the cloud environment. The Investigation process is to be handled by the service providers or the company who deployed the application. [1] To find the victim who had accessed or tampered the secured data, we need to implement digital forensics procedures in clouds [2]. The current forensic investigation practices do not match with the cloud computing characteristics. New methodology is to be implemented for investigating cyber attack on cloud. This paper will confer the forensics aspects of cloud computing by pointing out the forensic investigation issues in cloud computing and recommending new model that provides cyber forensic capabilities in cloud.

II. Related Work

The survey on cyber crime Investigation on cloud discusses various aspects of issues. Ting Shang evaluates the conventional forensic investigations and forensic investigations in cloud and analyses the challenges in cloud Forensic.[3] Shahrzad Zargari, David Benford provides an overview of cloud forensics including the issues and the existing challenges in order to give better future prospects and also offers some steps to be taken to overcome these challenges [4]. Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud and Solahuddin bin Shamsuddin presents the Investigation challenges in cloud environment. They have recommended the solutions like Utilizing TPM in hypervisor, updation of cloud service provider policy to provide the persistent storage devices and multilevel authentication to overcome the challenges in cloud [5].

The cloud computing becomes the most powerful environment for the upcoming companies. In cloud computing the forensic investigation support is not completely given by the cloud providers. There are few challenges in attaining the forensic support. The author highlights the cloud characteristics, models, architecture and the challenges in achieving Forensic support. Some of the challenges are data recovery in finding and retaining forensic evidence from law enforcement perspective. New methods are proposed to bring the evidence of the cyber attack in the cloud environment. Likewise there are challenges in Investigations on virtual machine. Henceforth, the extended Forensic Investigation system is mandatory to meet the Forensic challenges in cloud environment. [6]

a) Threats of Cloud Security Issues

The target of cloud computing is to setup a safe and reliable data storage and network service. The applications are extended over the Internet domain to the CSP, which maintains computer systems in clusters

Author α: Associate Professor, Department of Computer Science and Applications, D. G. Vaishnav College, Chennai.
Author σ: Research Scholar, Ph.D. Research Scholar SCSVMV University, Kancheepuram. e-mail: megalaimini@gmail.com

Apart from all the advantages of the cloud service, cloud data security is the main issue in the quality of service. Since cloud computing is not just a third party data warehouse, the data stored in the cloud may be updated frequently by other users, including insertion, deletion, and modification. Thus, so long as the data is stored in the cloud, there are some unavoidable threats of cloud security issues to the personal users and enterprises. [7]

A. Data Storage Issue

B. Personal Privacy Issue

C. Trust of CSP issue

III. Proposed Work

a) *Proposed Architecture*

Based on the Virtual Machine Introspection method the Forensic Investigation Architecture is built. Cyber forensic Investigation system involve Markov chain algorithm for Investigation.

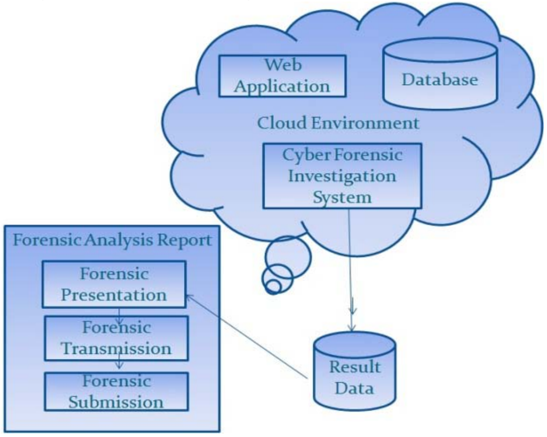


Figure 1 : Cyber Forensic System Architecture

Integrated application setup detects the runtime state of a system-level virtual machine and that information is recorded by the tracker system. Data Acquisition and reporting handled with the acquired knowledge by the Investigation system. Our Investigation system will involve in Identification of Crime, Collection of Evidence, analysis and presentation of the Forensic report.

b) *Framework for Forensic Exploration*

i. *Virtual Machine Introspection*

The framework for investigation of crime on cloud is done with the Virtual Machine Introspection (VMI). This is the technique which keeps tracking the hardware events and the user's behavior. Cyber Forensic system can be integrated in the virtual environment (Hypervisor, Virtual Architecture). For virtual machine introspection, the Investigation system logs the runtime state with the help of the registry, server memory, network etc. Based on this, Forensic Investigation report can be presented.

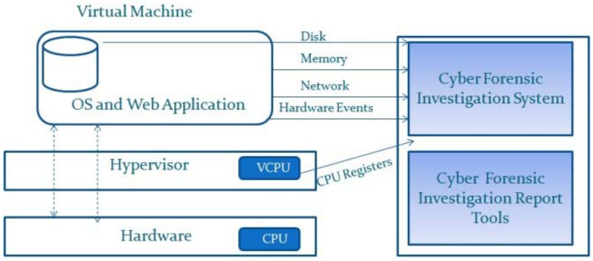


Figure 2 : Virtual Machine Introspection

c) *Cloud Forensic Investigation Model using Markov Chain*

Interaction of each node related with forensic actions on cloud environment and the derivation of data from the login details of the user, timestamps, event access, web page cache and logs. In this section, Cyber Criminal Activity Analysis Models using Markov Chain is proposed.

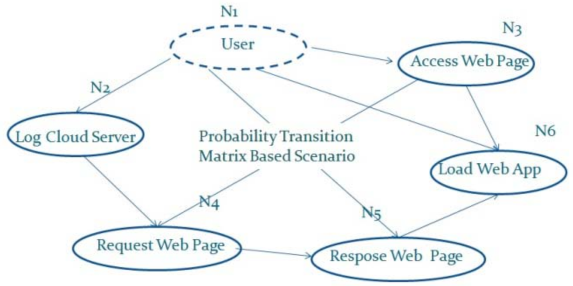


Figure 3 : Interaction of each Node Related Forensic Action on Cloud Environment

For example, the user visits the e-commerce web application deployed in cloud for hacking the user's personal information. The Node N1 and N2 comprise who logged into the server, the N3 and N4 describes when and what web page is being accessed etc. The N5, N6 specify when and which programs are being executed. Based on the six nodes of forensic actions, all of the summarized forensic data are derived and logged in the cloud server with time intervals. Based on the communication of each node, the probability of Forensic action is determined by our Cloud Forensic Investigation Model using Markov Chain.

When user established the connection to the cloud server then server allow to access the web page and request the web page from user. The cloud server allow and response to authentication users only. If the user authentication verified successfully then load web application to allow access web application and request wed application.

i. *Transitional Probabilities*

As we discussed, we determine w_{ij} *as* the number of forensic actions N_i involved by the user and N_j were number of times accessed the website or web pages. We calculate the probabilities of forensic action w_i as the sum of all the weights of edges pointing to $p_{i.}$

$$W_i = \sum_k \in In(N_i) W_{ki}$$

Using these weights, we can then estimate the prior probabilities of the forensic action, as well as the transition probabilities between two nodes.

ii. *Prior Probabilities*

The forensic probabilities are calculated with the N forensic action and the matrix of the pages visited Q. The probability of the algorithm is calculated based on the type of the forensic action. The first probability (PFA)computes the probability of the page visited by the user between the nodes N1 and N6.The second probability(SUFA) is the calculation of the more common nodes previously visited by many of the users. The third probability is the calculation of the probabilities of the same pattern of access between the nodes. *PFA (Priority of Forensic Action):*

$$O(P_i) = \frac{1}{M} \text{ and } O(P_k, P_i) = \frac{1}{|Out(P_k)|}$$

- ➢ SUFA (Semi-Usage Forensic Action):

$$O(P_i) = \frac{1}{M} \text{ and } O(P_k, P_i) = \left(\sum_{P_j} \in Out(P_k)^{w_{kj}}\right)^{-1}$$

- ➢ UFA (Usage Forensic Action):

$$O(P_i) = \frac{W_i}{\sum_{P_j} \in WS^{W_j}} \text{ and } O(P_k, P_i) = \frac{W_{ki}}{\sum_{P_j} \in Out(P_k)^{W_{kj}}}$$

IV. Results and Discussion

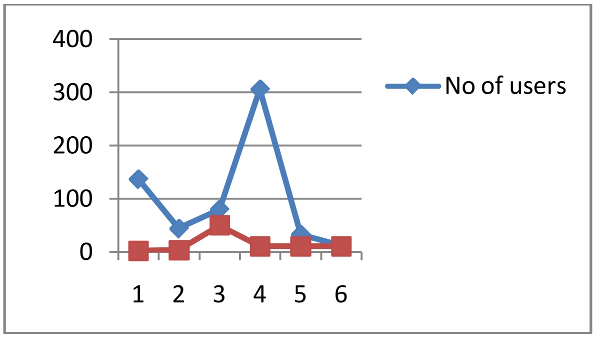
Probabilities of hacking the data or tampering the data are computed by the sum of the weights specified in the algorithm. Every action of the user are monitored and logged by our Investigation system. List of manipulated logged history of the users and the crime probability derived from the user's behavior are shown in tabular column.

Our experiments assume that some of the cloud consumer is the victim of the crime investigation. This situation demands proactive logging of data by the provider which may be of forensic relevance for investigation.

Table 1 : Probability of Forensic Relevance

No of Users	Logged Users	Page Name	Accessed Database	Crime Probability
137	10	Products	137	2
44	44	Personal Information	44	3
80	80	Payment gateway	80	50
306	0	Home page	0	10
33	0	Contact	0	10
12	0	About Us	0	10

Table 2 : Forensic Investigation Probability



V. Conclusion

This paper elaborates the opportunities of applying cyber Forensics in cloud computing. The proposed cloud Forensic model is to be designed with the above mentioned steps and methods. This paper gives a brief introduction to the cloud computing concept and its Cyber Forensics issues and challenges. We outline a new forensic issue for cybercrime in two aspects as collection and preservation. Since cybercrime evidence belongs to electronic evidence, it is easy to be destroyed and tampered with during the forensic procedure. In order to ensure the primitiveness and integrity of the evidence, it should image the relative records and files absolutely. A new cybercrime forensic system is proposed to be set up in cloud computing. An analysis is set up as a special network service in the cloud to communicate with each server. Through the analysis, forensic experts can detect behaviors threatening to servers in the cloud and capture volatile information for late-time analyses by the skilled forensic toolkit. The performance of the forensic system is relative to the scale of the cloud, which should be improved in later research.

References Références Referencias

1. Cunt P. Garrison, "Digital Forensics for Network, Internet and Cloud Computing", Publication Copyright © 2010 Elsevier Inc.
2. Mark C. Chu- Carroll, "code in the Cloud", Copyright © 2011 Pragmatic Programmers, LLC.
3. Ting Shang, "Forensic investigations in Cloud environments, 2012 International Conference on Computer Science and Information Processing (CSIP).
4. Shahrzad Zargari, David Benford, "Cloud Forensics: Concepts, Issues, and Challenges", 2012 Third International Conference on Emerging Intelligent Data and Web Technologies (EIDWT).
5. Mohsen Damshenas, Ali Dehghantanha, Ramlan Mahmoud, Solahuddin bin Shamsuddin, "Forensics investigation challenges in cloud computing environments", 2012 International Conference ON

Cyber Security, Cyber Warfare and Digital Forensic(Cyber Sec).

6. Tony Krone, Concepts and Terms: High-Tech Crime Brief. No. 1 (2005); Kim-Kwang Raymond Choo, Russell Smith and Rob Mc Cusker, 'Future Directions in Technology-Enabled Crime: 2007-09' (Research and public policy series No 78, Australian Institute of Criminology, 2007).
7. Yan, Cheng, "Cybercrime Forensics System in Cloud Computing", 2011 International Conference On Image Analysis and Signal Processing (IASP).

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Portable Tpm Based User Attestation Architecture for Cloud Environments

By Mr. Pramod & Dr. B R Prasad Babu

Abstract- Cloud computing is causing a major shift in the IT industry. Research indicates that the cloud computing industry segment is substantial and growing enormously. New technologies have been developed, and now there are various ways to virtualize IT systems and to access the needed applications on the Internet, through web based applications. Users, now can access their data any time and at any place with the service provided by the cloud storage. With all these benefits, security is always a concern. Even though the cloud provides accessing the data stored in cloud storage in a flexible and scalable manner, the main challenge it faces is with the security issues. Thus user may think it's not secure since the encryption keys are managed by the software, therefore there is no attestation on the client software integrity. The cloud user who has to deploy in the reliable and secure environment should be confirmed from the Infrastructure as a Service (IaaS) that it has not been corrupted by the mischievous acts. Thus, the user identification which consists user ID and password can also be easily compromised. Apart from the traditional network security solutions, trusted computing technology is combined into more and more aspects of cloud computing environment to guarantee the integrity of platform and provide attestation mechanism for trustworthy services. Thus, enhancing the confidence of the IaaS provider.

Keywords: TPM, IaaS, vTPM, cTPM, SMRR, SMM,TCG, TED, DRTM, VLR, DRTM, CA.

GJCST-B Classification : C.2.1, C.5.3

PORTABLETPMBASEDUSERATTESTATIONARCHITECTUREFORCLOUDENVIRONMENTS

Strictly as per the compliance and regulations of:

Open Association of Research Society, USA
Research | Diversity | Ethics

Portable Tpm Based User Attestation Architecture for Cloud Environments

Mr. Pramod [α] & Dr. B R Prasad Babu [σ]

Abstract- Cloud computing is causing a major shift in the IT industry. Research indicates that the cloud computing industry segment is substantial and growing enormously. New technologies have been developed, and now there are various ways to virtualize IT systems and to access the needed applications on the Internet, through web based applications. Users, now can access their data any time and at any place with the service provided by the cloud storage. With all these benefits, security is always a concern. Even though the cloud provides accessing the data stored in cloud storage in a flexible and scalable manner, the main challenge it faces is with the security issues. Thus user may think it's not secure since the encryption keys are managed by the software, therefore there is no attestation on the client software integrity. The cloud user who has to deploy in the reliable and secure environment should be confirmed from the Infrastructure as a Service (IaaS) that it has not been corrupted by the mischievous acts. Thus, the user identification which consists user ID and password can also be easily compromised. Apart from the traditional network security solutions, trusted computing technology is combined into more and more aspects of cloud computing environment to guarantee the integrity of platform and provide attestation mechanism for trustworthy services. Thus, enhancing the confidence of the IaaS provider. A cryptographic protocol adopted by the Trusted Computing Group enables the remote authentication which preserves the privacy of the user based on the trusted platform. Thus we propose a framework which defines Trusted Platform Module (TPM), a trusted computing group which proves the secure data access control in the cloud storage by providing additional security. In this paper, we define the TPM-based key management, remote client attestation and a secure key share protocol across multiple users. Then we consider some of the challenges with the current TPM based attestation techniques. Thus, proposing a potable TPM which is not embedded into the virtual machines so as to provide the efficiency to the cloud users. Using this approach, security of the user is handled in an efficient way. Finally, we demonstrate the effectiveness and efficiency of the proposed schemes through extensive experimental evaluation on the live Microsoft Windows Azure platform.

Keywords: TPM, IaaS, vTPM, cTPM, SMRR, SMM,TCG, TED, DRTM, VLR, DRTM, CA.

I. Introduction

CLOUD computing is undoubtedly the new era of computing. Industry experts believe that notion of perceiving cloud computing as a new technology trend, is all set to grow. Cost factor is the biggest driver for its expected growth. According to Gartner Inc. Cloud computing is a disruptive phenomenon, with the potential to make IT organizations more responsive than ever. Cloud computing promises economic advantages, speed, agility, flexibility, infinite elasticity and innovation. Cloud computing is an internet-based facility to share technological resources, software and digital information. This technological methodology can save a lot of infrastructure cost and pay-as-you-use model can also be offered through the cloud computing solutions. The above mentioned utilities can help small and mid-sized companies to bring down their operational costs. IDC India lead analyst (software and services research), Kamal Vohra stated, "The most attractive feature of this new technology is the prospect of converting large, upfront capital investments in IT infrastructure into smaller, manageable 'pay-per-use' annuity payments." Recent IDC cloud research shows that spending on public IT cloud services will reach $58.4 billion in 2015 and is expected to be more than $107 billion in 2017. Over the 2013–2017 forecast period, public IT cloud services will have a compound annual growth rate (CAGR) of 23.5%, five times that of the industry overall. Software as a service (SaaS) will remain the largest public IT cloud services category, capturing 59.7% of revenues in 2017. IDC predicts that by 2017, 80%+ of new cloud apps will be hosted on six PaaS platforms. Armonk, N.Y. May 2014 announced businesses across the US have ranked IBM the number 1 cloud computing provider, according to an IDC survey of US market preferences for infrastructure - as - a - service (IaaS). Enterprises ranked Amazon 7th, behind Google (5th) and Microsoft (6th). The rankings are based on responses from more than 400 US-based companies.

Privacy and security is the main concern in the communication over a network. Continuous work to ensure the privacy and confidentiality of the data communication have existed for a long time. Cloud computing is the future but not if security problems persist. The major concern that are being trying to recognize is mainly on the security issues over the cloud computing. However, security and privacy are still cited by many organisations as the top inhibitors of cloud services adoption. FaraziSabhaiet. al. [2] describes the well-known Gartner's seven security issues. The basic security issues such as Data leakage, DoS (Denial of Service) attacks are addressed.

Author α: Research Scholar, VTU, EPCET, Bangalore.
e-mail: pramod741231@gmail.com
Author σ: Head of Department, Computer science and Engineering, SEAIT, Bangalore. e-mail: brprasadbabu@gmail.com

Cloud computing services fall into three major categories- Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software-as-a-Service (SaaS). The software applications which are deployed from the cloud infrastructure provided by the cloud providers are accessed by the Software-as-a-Service (SaaS).The cloud providers manage and control the application so that the user does not need to own the software but rather pay for its use through a web API. Platform as a Service (PaaS) lets the users deploy their applications on the provider's cloud infrastructure using programming languages and tools supported by the provider. Finally, Infrastructure as a Service (IaaS) authorizes the deployment and the execution of an environment fully controlled by the user, typically a Virtual Machine (VM) – on the Cloud resources. Typically, the user should purchase the infrastructure such as software, data resource, server, network accessories in order to operate. But here, the user can directly purchase all these resources as outsourced services from directly from the cloud on "pay-as-you-use" basis. Thus, providing efficiency. Here, we focus on the security aspects of the third category of cloud services, i.e., IaaS platforms and more precisely on confidentiality and integrity issues. The problem arises when the user has to preserve the data confidential on the shared platform. Also, care must be taken that once deployed, the integrity of the environment is not corrupted by the mischievous acts.

A novel approach to protect IaaS platforms that confide on the approach established from the Trusted Computing Group (TCG) whichoffer a secured and reassuring environment with the hardware device called the Trusted Platform Module (TPM). TPM designates both the name of a specification detailing a secure crypto processor as well as the implementation of that specification, often called the TPM chip. TPM asserts the virtue of remote authentication and gets interacted with the symmetric key which can be used for various cryptographic purposes, from the protection of network communications to data encryption. In the IaaS context, it ensures that only the remote resource with which the user is communicating using the TCG protocol can interact with the ciphered data.

Zhidong et. al. [6] address the cloud computing security challenges by proposing a solution called the Trusted Computing Platform (TCP). Trusted cloud computing system is built using TCP as the hardware for cloud computing and it ensures privacy and trust. By design, TPMs offer a hardware root of trust bound to a single, standalone device. TPMs come equipped with encryption keys whose private parts never leave the TPM hardware chip, reducing the possibility those keys may be compromised. Assessing security protocols requires more than showing their robustness against a few use cases. Recent advances in automatic protocol analysis tools [4] allow to scale up the attack complexity against the analyzed protocol and detect design errors.

A TPM is a small tamper proof hardware chip embedded in most recent motherboards. This paper presents TPM with the portability, an extension of the TCG's model which possess an additional secret key to the TPM and shares the secret key with the cloud. Therefore, with this, the cloud can create and share the secret keys of TPM and data over multiple platforms which belongs to a single user.

The research mechanism is organized as follows. Section two discusses the related work. Our proposed work is discussed in section three. The experimental results and comparisons are presented in section four. Section four proves the experimental results of our proposed system. The concluding remarks are discussed in the last section of the paper.

II. Related Work

Much work has been done in concern with security issues in Cloud Computing sector. Let us look into some of the survey which exists. [1] presentsc TPM, an extension of the TPM's design that adds an additional root key to the TPM and shares that root key with the cloud. As a result, the cloud can create and share TPM-protected keys and data across multiple devices owned by one user. Further, the additional key lets the cTPM allocate cloud-backed remote storage so that each TPM can benefit from a trusted real-time clock and high performance, non-volatile storage. This paper shows that cTPM is practical, versatile, and easily applicable to trusted mobile applications. By avoiding a clean-slate redesign, we sidestep the difficult challenge of re-verifying the security properties of a new TPM design. Here it demonstrates cTPM's versatility with two case studies: extending Pasture with additional functionality, and re-implementing TrInc without the need for extra hardware. Re-implementing TrInc without the need for extra hardware again causes with the core security issues.

The paper [3] present a novel secure auditing scheme for cloud computing systems. One major problem with auditing schemes is that they are vulnerable to the transient attack (also known as the timed scrubbing attack). This secure auditing scheme is able to prevent the transient attack via modification of the Linux auditing daemon - audit, which creates attestable logs. This scheme utilizes the System Management Mode (SMM) for integrity checks and the Trusted Platform Module (TPM) chip for attestable security. Specifically, it modifies the auditing daemon protocol such that it records a hash of eachaudit log entry to the TPM's Platform Configuration Register (PCR), which gives an attestable history of every command executed on the cloud server. Different from the existing auditing schemes, this scheme is capable of preventing the transient attack. It has achieved this by modifying the existing Linux auditing daemon as well as making use of existing software and hardware. This scheme can provide clients with greater assurance and trust in cloud computing services. System with Trusted Platform Module (TPM) [14] provides secure boot via the Core Root of Trust for Measurement as well as secure storage for the log file hashes via the Platform Configuration Registers. The CRTM is anextension of the BIOS which will be initialized first, measure parts of the BIOS block, and then pass control back over to the BIOS. Once the BIOS, boot loader, and OS kernel run and pass control to the OS, the expected configuration by examining the TPM's Platform Configuration Register. The main issue here is, any change to the code between CRTM and the OS running will result in anunseen PCR value. The SMRAM is to be properly setup by the BIOS at boot time and to remain tamper-proof from cache poisoning attacks as in [7]. To prevent these attacks, proper hardware configurations, such as System Management Range Register (SMRR) [9], should be used.

A key technology of cloud computing is virtualization, which can lead to reduce the total cost and increase the application flexibility. However along with the se benefits come added security challenges. The extension of Trusted Computing to virtual environments can provide secure storage and ensure system integrity. In [4], it describes and analyse several existing virtualization of TPM (vTPM) designs: software-based vTPM, hardware-based vTPM, para-virtualized TPM and property-based vTPM and analyse each of their limitations. Concerning about security is an important factor that affect the popularity of cloud computing. Incorporation of trusted computing into virtualized systems should significantly enhance cloud computing system security. In this paper, it briefly reviews the concepts virtualization and trusted computing, and proposal the requirements on a virtual TPM facility. It describes and analyse some existing vTPM designs. Finally, it discusses some open issues of the vTPM, using property-based attestation and secure VMvTPM migration protocols are the key research area sofvTPM in the future.

In [5], it proposes DF Cloud, a secure data access control method of cloud storage services to handle these problems found in the typical cloud storage service Drop box. DF Cloud relies on Trusted Platform Module (TPM) [19] to manage all the encryption keys and define a key sharing protocol among legal users. It assumes that each client is mobile device using ARM Trust Zone[13] technology. The DF Cloud server prototype is implemented using ARM Fast model 7.1 and Open Virtualization software stack for ARM Trust Zone. For DF Cloud client, TPM functions are developed in the secure domain of ARM Trust Zone because most ARM-based mobile devices are not equipped with TPM chip. The DF Cloud framework defines TPM-based secure channel setup, TPM-based key management, remote client attestation, and a secure key share protocol across multiple users/devices. There are several security issues in cloud storage services, among these issues we mainly focused on data leakages that can occur in either client side or server-side. DF Cloud exploit client-side encryption technique, remote attestation for client plat form, and hardware based key management to build a secure access environment. DF Cloud also support secure key sharing protocol across the multiple devices or users. It implemented prototype on ARM Fast model to emulate ARM Cortex-A15 core and Open Virtualization's software stack in environment setup. The performance overhead is quiet high, but if it adopts some optimization techniques such as shared memory between two World, then we can reduce overhead introduced in our current implementation.

TPM is able to provide strong secure storage for sensitive data such as passwords. Although several commercial password managers have used TPM to cache passwords, they are not capable of protecting passwords during verification. This [8] proposes a new TPM-based password caching and verification method called Pwd CaVe. In addition to using TPM in password caching, Pwd CaVe also uses TPM during password verification. In Pwd CaVe, all password-related computations are performed in the TPM. Pwd CaVe guarantees that once a password is cached in the TPM, it will be protected by the TPM through the rest of its lifetime, thus eliminating the possibility that passwords might be attacked in memory. Pwd CaVe eliminates the time that passwords stay in the memory during verification, and therefore keep passwords from attacks in memory. Once a password is cached in the TPM, it will never be released out of the TPM, even in later password verification. Again which proves, the user himself cannot be able to change the password even in emergency situations, in which the password is compromised. Thus, not efficient.

In this [10], it address the issues by incorporating a hardware-based Trusted Platform Module (TPM) mechanism called the Trusted Extension Device (TED) together with the security model and protocol to allow stronger privacy of data compared to software-based security protocols. It demonstrates the concept of using TED for stronger protection and management of cryptographic keys and how the secure data sharing protocol will allow a data owner (e.g., author) to securely store data via untrusted Cloud services. Here, it prevents keys to be stolen by outsiders and dishonest authorised consumers. As part of our future work, this work has to improve the performance of this protocol to the extent that it will be feasible in the real-world scenario. It should also aim to incorporate larger data sizes. Furthermore, it must extend the current work to incorporate further data sharing control.

In addition to security, most of the hardware that is being shipped today is equipped with the TPM which can be used for realization of trusted platforms. Recently several TPM attestation techniques such as binary attestation and property based attestation techniques have been proposed but there are some fundamental issues that need to be addressed for using these techniques in practice. In [11], it considers an architecture where different services are hosted on the cloud infrastructure by multiple cloud customers (tenants). Then it considers an attacker model that is specific to the cloud and some of the challenges with the current TPM based attestation techniques. In this model, the cloud service provider is used as the Certification Authority (CA) for the tenant virtual machines. The CA only certifies the basic security properties which are the assurance on the traffic originating from the tenant virtual machine and validation of the tenant virtual machine transactions. The components of the CA monitor the interactions of the tenant virtual machine for the certified properties. Since the tenant virtual machines are running on the cloud service provider infrastructure, it is aware of the dynamic changes to the tenant virtual machine. The CA can terminate the ongoing transactions and/or dynamically isolate the tenant virtual machine if there is a variation in the behaviour of the tenant virtual machine from the certified properties. Hence this model is used to address the challenges with the current TPM based attestation techniques and efficiently deal with the attacks in the cloud. This model still need to get extended with the functionality of the CA to certify the behaviour of the tenant virtual machines. Since the Node Controller is aware of the dynamic changes to the tenant virtual machine, it has to ensure that the certified properties are satisfied by the tenant virtual machines.

Group signatures have recently become important for enabling privacy-preserving attestation in projects such as Microsoft's NGSCB effort (formerly Palladium). Revocation is critical to the security of such systems. [15] construct a short group signature scheme that supports Verifier Local Revocation (VLR). In this model, revocation messages are only sent to signature verifiers (as opposed to both signers and verifiers). Consequently there is no need to contact individual signers when some user is revoked. This model is appealing for systems providing attestation capabilities. The signatures are as short as standard RSA signatures with comparable security. Security of our group signature (in the random oracle model) is based on the Strong Diffie Hellman assumption and the Decision Linear assumption in bilinear groups. Here, a precise model for VLR group signatures and discussed its implications. It has described a short group signature scheme where user revocation only requires sending revocation information to signature verifiers, a setup we call verifier-local revocation. Here, the signatures are short: only 141 bytes for a standard security level. They are shorter than group signatures built from the Strong-RSA assumption and are shorter even than BBS short group signatures [8], which do not support verifier-local revocation. There are still a number of open problems related to VLR signatures. Most importantly, is there an efficient VLR group signature scheme where signature verification time is sub-linear in the number of revoked users, without compromising user privacy.

Employs a TPM based method to providea minimum Trusted Code Base (TCB) in [12], which can be used to detect the modification of the kernel. It requires advanced hardware features such as Dynamic Root of Trust Measurement (DRTM) and late launch. The scheme is also directly vulnerable to the scrubbing attack because the measurement target is responsible for invoking the integrity measurement.

To overcome all these issues, we have proposed a portable hardware based security preserving model. Our scheme is different from theirs in that, our scheme offers more revocation capabilities than other schemes, and our scheme is built from the strong public key cryptographic assumptions whereas their scheme is constructed using bilinear maps. Thus, a high performance security model is proposed.

III. Proposed System

Let us consider a case where a cloud provider, cloud users, a blacklisting controller and the cloud verifiers are concerned. The membership certificates for the cloud users are issued by the cloud provider. Membership certificates are blacklisted by the blacklisting controller. The cloud users in the system may vary and also users may access their data according to their need. Let us consider a hardware based authentication key in an ideal system. The operation carried out by the authentication keyKare initialize, register, membership approval and blacklisting.

In initialize phase, every entity is controlled by the controller which is indicated by the authentication key. Users are need to be registered. A user requests the authenticator with K and the authenticator asks the cloud provider whether the user can get registered. If the cloud provider agrees, the authenticator notifies the user that he can become a member.

In the membership approval phase, the authenticator sends a request that he wants to contact the verifier. With $\mathbb{K}$, it informs the verifier that user wants to perform the membership approval without revealing to the verifier who the authenticator is. The verifier chooses a message$s$ andsends s to the authenticator. If the authenticator is not a member,$\mathbb{K}$ aborts. Otherwise,

$\mathbb{K}$ tellsthe authenticator whether he has been blacklisted and asks him whether to proceed. If the authenticator does not abort, $\mathbb{K}$ lets the verifier know that a blacklisted user has signed the message s.Otherwise, $\mathbb{K}$ informs the verifier that s has been signed by a legitimate member. Blacklist revokes the membership authentication. The blacklisting controller tells the authenticator to blacklist a user. If the user is not a group member, $\mathbb{K}$ denies the request. Otherwise, $\mathbb{K}$ marks the user as blacklisted.

A user who is not a member or is a member but has been blacklisted cannot succeed in membership approvaltoany verifiers. The verifier cannot identify who is the authenticator in a membership approval operation, thus proving anonymity. Blacklist causes verifiers to reject message assigned by a blacklisted user in an ideal system. In our protocol, if a user's private key is exposed and the cloud user is blacklisted, the signatures from this blacklisted cloud user become link able to an honest verifier. As a result, corrupted users who reveal their private keys and are blacklisted deliberately lose their privacy. Thus, an authenticator can check whether the user has been blacklisted from on the blacklist, before the user signs asignature and sends it to the verifier. If the authenticator finds out that the user has been blacklisted, he can choose to not proceed.

The security of our scheme relies on the public key cryptographic protocol and the Diffie-Hellman assumption. The public key cryptographic protocol is established as follows.

It is computationally infeasible, on input of a random modulus M and a random element $a \in \mathbb{A}_l^*$ compute values $i > 1$ and q such that $q^i \equiv a (mod\, M)$. In other words, for every probabilistic polynomial-time algorithm R,

$$\begin{aligned}\mathcal{B}[M \leftarrow \mathcal{K}(1^p), a \in \mathbb{A}_l^*, (q,i) \leftarrow R(M,a) :\ q^i \\ \equiv a(mod\, M) \wedge 1 < i < M] \\ = \phi(p)\end{aligned} \quad (1)$$

where$\mathcal{K}(1^p)$ is an algorithm that generates a public keymodulusand$\phi(p)$ is a negligible function.

Let u be an l_u-bit prime and v is anl_v-bit prime such that$v|u-1$. Let $s \in \mathbb{A}_u^*$ be arandom element of order v. Then, for sufficiently large values of $l_u$and l_v, the distribution $\{(s^x, s^y, s^z)\}$ is computationally indistinguishable from the distribution $\{(s^x, s^y, s^{xy})\}$ where x, y and $z$are random elements from$\mathbb{A}_u$. It can beformally stated as, for every probabilistic polynomial-time algorithm R, the Diffie-Hellman assumption is given by:

$$\begin{aligned}|\mathrm{B}[R(u, v, s, s^x, s^y, s^{xy}) = 1] \\ - \mathrm{B}[R(u, v, s, s^x, s^y, s^z) \\ = 1]| = \phi(p)\end{aligned} \quad (2)$$

Where $\phi(p)$ a negligible function and the probabilities is are taken over the choice of u, v, s according to some generation function $\mathcal{K}(1^p)$ and the random choice of x, y, zin $\mathbb{A}_u$.

Remote authentication of the hardware based authentication key is enabled in the cryptographic protocols. Here, it preserves the privacy of the cloud user which contains the key $\mathbb{K}$. This protocol consists of the cloud provider, authenticator who provides access issued by the cloud provider and the verifier who verifies with the authenticator. The authenticator consists of the portable key $\mathbb{K}$ which preserves the privacy for the cloud user. The protocol is constructed by the Camenisch-Lysyanskaya signature scheme, where it has two secret messages m_0 and m_1 , and attains the CLsignature (membership of the user)on m_0 and $m_1$from the cloud provider through a secure protocol, and thus the user is verified by the verifier. Here, the authenticator chooses two random l_m-bit secret messages m_0 and m_1, then interacts with the cloud provider, and inthe end obtains (R, i, q) from the protocol such that $R^i G_0^{m_0} G_1^{m_1} Q^q \equiv A(mod\, M)$. The authenticator will check with verifier that the user is verified and possess the CL-signature on the values of m_0 and m_1. This can be done by values (m_0, m_1, R, i, q) such that $R^i G_0^{m_0} G_1^{m_1} Q^q \equiv A(mod\, M)$ .Let $m = m_0 + m_1 2^{l_m}$ the authenticator also computes $P := \mathcal{D}^m\ mod\, u$where$\mathcal{D}$ is a generator of an algebra group wherecomputing discrete logarithms is infeasible, and proves to the verifier that the exponent m is related tom_0 and m_1. In this protocol, it can choose$\mathcal{D}$: the value of $\mathcal{D}$ can be chosenrandomly by the authenticator, or can be derived from theverifier's name by using an appropriate hash function. If authentication key$\mathbb{K}$ was found comprised and its private key R, i, m_0, m_1, q was exposed, the values m_0 and m_1 are extracted and put on a blacklist. The verifier can then check the public key P in thesignature against this blacklist by comparing it with $\mathcal{D}^{m_0 + m_1 2^{l_m}}$ for all pairsm_0 and m_1 on the black list. In our scheme, there are several types of entities: a cloud provider, cloud users, a blacklisting controller and verifiers. The cloud provider and blacklisting controller could be the same entity or separate entities.

Our scheme builds in concern with the cryptographic protocol scheme and uses the Camenisch-Lysyanskaya signature scheme as underlying building block. To simplify our presentation, we modified the cryptographic protocol scheme in the following ways: 1) each user chooses a single secret m instead of two secrets, and 2) the signature operation is performed solely by the user (along with authentication key $\mathbb{K}$), instead of split by two separate entities (authentication key $\mathbb{K}$ and host in the cryptographic protocol scheme).

In the register phase, a cloud user chooses a secret message m and sends the cloud providera commit mentto m, i.e., $C := G^m Q^{q'}$ whereq' is a value chosen randomly by the user to blind the m. Also, the usercomputes $P := \mathcal{D}_I^m \ mod\ u$, where $\mathcal{D}_I$ is a number derivedfrom the cloud provider's basename. The user sends (P,C) to the cloud provider. The provider then issues a membership for the user based on C. The cloud provider chooses a random integer q'' and a random prime i, then computes R such that $R^i C Q^{q''} \equiv A(mod\ M)$, and sends the user (R,i,q''). The cloud provider also proves to the user that he computed R correctly.The CL signature on m is then $R,i,q := q' + q''$. The user'sprivate key is set to be (R,i,m,q).A user can now prove that he is a valid memberby proving that he has a CL signature on the value m.This can be done by values of $m,R,i$and q such that $R^i G^m Q^q \equiv A\ (mod\ M)$. Also, theuser computes $P := \mathcal{D}^m \ mod\ u$ where $\mathcal{D}$ is a random basepicked up by the user, reveals $\mathcal{D}$and P, and proves that $\log_{\mathcal{D}} P$is the same as the one in his private key. The value$P$ serves the purpose of blacklist. Same as in the cryptographic scheme, if a user's private key(R,i,m,q) is compromisedand gets exposed to the public, m is put in the blacklist. The verifier can then check P in the signature against the blacklist by comparing it with $\mathcal{D}^{\widehat{m}}$for all$\widehat{m}$ in the blacklist. We refer this type of blacklist as private key-based blacklist and useV_{priv} to denote the blacklist of this type.

This scheme supports two additional blacklist methods, one is signature-based blacklist and the other is cloud provider-based blacklist. In signature-based blacklist, suppose a verifier received a signature from an authenticator and then decided that the authenticator was compromised. The verifier reports the signature to the blacklisting controller who later places$(\mathcal{D},P)$ of the signatureto the signature-based blacklist, where $\log_{\mathcal{D}} P$ is thesecret of the compromised authenticator. To prove membership, auser with private key (R,i,m,q) now needs not only toprove the (R,i,m,q) such that$R^i C Q^{q''} \equiv A(mod\ M)$ but also to prove that m in his private key isdifferent from$\log_{\mathcal{D}} \hat{P}$ for each$(\widehat{\mathcal{D}},\hat{P})$ pair in the signature-based blacklist. We useV_{sign} to denote the blacklist of this type. In the cloud provider-based blacklist, the provider obtained$(P,C)$from a user when the user registers and laterdecided to revoke this user from some reason. The cloud provider sends(P,H) to the blacklisting controller who places P to the cloud provider-based blacklist, where $\log_{\mathcal{D}_I} P$ is the secret of the blacklisted user. To prove the membership of the user, a user needs to prove that m in his private keyis different from $\log_{\mathcal{D}_I} \hat{P}$ for each$\hat{P}$ in the cloud provider-based blacklist. We use cloud provider V_{cp} to denote the blacklist of this type.

a) Security

Let us consider the security parameters $r_M r_m r_i r_{i'} r_q r_\theta r_\psi r_\mu r_u$ and r_v where$r_M(2048)$is the size of the public-key modulus, $r_v(208)$ isthe size of the m's (user's secret, part of membership privatekey), $r_i(576)$ is the size of i's (exponent, part of membership private key), $r_{i'}(128)$ is the size of the interval the i''s are chosen from, $r_q(2720)$ is the size of the q's (random value, part of membership private key), $r_\theta(80)$ is the security parameter controlling the statistical property, $r_\psi(256)$ is the output length of the hash function used for Fiat-Shamir heuristic, $r_\mu(80)$ is the security parameter needed for the reduction in the proof of security, $r_u(1632)$ is the size of the modulus u, and $r_v(208)$ is the size of the order$v$ of the subgroup of$\mathbb{A}_u^*$ that is used for blacklist checking. We require that

$$\begin{aligned} r_\theta + r_\psi + 2 + max\{r_m, r_{i'}\} \\ &< r_i r_M + r_\theta r_\psi \\ &+ max\{r_m + r_\mu + 3, r_\theta \\ &+ 2\} < r_q, \qquad r_m = r_q \end{aligned} \tag{3}$$

The parameters r_u and r_v should be chosen such that the discrete logarithm problem in the sub group of$\mathbb{A}_u^*$of order v with u and v being primes such that $u \in [2^{r_u - 1}, 2^{r_u} - 1]$ and $v \in [2^{r_v - 1}, 2^{r_v} - 1]$, has about the same difficulty as factoringr_M-bit public-key modulus.

b) Generating authentication keys

The key generation program also produces a non-interactive proof that the public key was formed correctly. Here we describe how the cloud provider chooses the public key and the user issuing private key. The later will guarantee the security properties, i.e., that privacy and anonymity of signatures will hold. The cloud provider chooses a public-key cryptographic modulus $M = u_M v_M$ with $u_M = 2u'_M + 1, v_M = 2v'_M + 1$ such that u_M, u'_M, v_M, v'_M are all primes,u_M and v_M have the same length, and$m$ has r_M bits.Furthermore, the cloud provider chooses a random generator$s'$of ZG_M, the group of quadratic residues modulo M. Next, it chooses random integers $e_s, e_t, e_q, e_b, e_g \in [1, u'_M v'_M]$ and computes

$$\begin{aligned} s &:= s'^{e_s}\ mod\ M; \qquad & t &:= s'^{e_t}\ mod\ M; \\ G &:= t^{e_s}\ mod\ M; \\ Q &:= t^{e_q}\ mod\ M; \qquad & A &:= t^{e_b}\ mod\ M. \end{aligned} \tag{4}$$

It produces a non-interactive proof thats,t,G,Q and A are computed correctly, i.e., $s,t \in \langle s' \rangle$ and $Q,A,G \in \langle t \rangle$. This can be proved using the standard cut-and-choose technique. The cloud provider generates a group of prime order as follows:it chooses random primes u and v such that $u = \mu v + 1$ for some μ with $v |\ \mu, u \in [2^{r_u - 1}, 2^{r_u} - 1]$, and $v \in [2^{r_v - 1}, 2^{r_v} - 1]$. It then chooses a random $a' \leftarrow \mathbb{A}_u^*$ suchthat $a'^{(u-1)/v} \not\equiv 1(mod\ u)$ and sets $a := a'^{(u-1)/v}\ mod\ u$. Finally, the cloud provider publishes the public key $(M, s', s, t, G, Q, A, u, v, a)$ and the proof, and stores(u'_M, v'_M) as the user issuing private key.

In addition to generating the user public key and user issuing private key, the cloud provider generates also a long term public private key pair (P_I, P_I^{-1}). The cloud provider publishes the public key P. This key is used for authentication between the cloud provider and any user who wants to become a registered member. Analogously, the blacklisting controller has long term public/private key pair(P_M, P_M^{-1}). The blacklisting controller uses its key to sign the blacklist.

c) Verification of the Cloud Provider's Public Key

The user's public key is $(M, s', s, t, G, Q, A, u, v, a)$ and the proof thats, t, Q, A, G are formed properly. Any user inthe system can verify the correctness of the group public key are as follows. Firstly, it verify the proof that$Q, A, G \in \langle t \rangle$and $s, t \in \langle s' \rangle$. Then check whether u and v are primes,$v | (u-1), v \nmid \frac{u-1}{v}$and $a^v \equiv 1 (mod\, u)$. Later check whether all public key parameters have the required length.

If s, t, Q, A, G are not formed correctly, it couldpotentially mean that the security properties for the usersdo not hold. However, it is sufficient if the users verify theproof thats, t, Q, A, G are computed correctly only once. Also, if a does not generate a subgroup of$\mathbb{A}_u^*$, the cloud provider could potentially use this to link different signatures. As argued in, it is not necessary to prove that M is a productof two safe primes for the anonymity of the users. In fact, itwould be very expensive for the cloud provider to prove that M is a safe-prime product.

d) Registration

This is a protocol which runs between the cloud provider and auser. The public input to this protocol is the user public key $(M, s', s, t, G, Q, A, u, v, a)$ and the cloud provider's long-termpublic keyP_I and the cloud provider's basename$name_I$. The privateinput of the cloud provider is the user issuing private key. We assume that the user and the cloud provider have established an authentic channel, i.e., the user needs to make sure that he talks to the right cloud provider and the cloud provider needs to be sure that the user is allowed to register for the membership. Note that we do not require secrecy of the communication channel. Let $\psi(\cdot)$ and $\psi_u(\cdot)$ be two collision-resistant hash functions: $\psi(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^{r_\psi}$ and $\psi_u : \{0,1\}^* \rightarrow \{0,1\}^{r_u + r_\theta}$. In the register protocol, the user verifies that the user public key $(M, s', s, t, G, Q, A, u, v, a)$is signed by P_I. Then both the user and cloud provider computes $\mathcal{D}_I := \psi_u(name_I)^{(u-1)/v}\, mod\, u$ .The user chooses at random $m \leftarrow \mathbb{A}_v^*$; $q' \leftarrow \{0,1\}^{r_M + r_\theta}$ then computes $P := \mathcal{D}_I^m\, mod\, u$ and $C := G^m Q^{q'}\, mod\, M$. The user sends (P, C) to the cloud provider. Therefore, the user proves to the cloud provider the knowledge of m andq'. He runs as the authenticator of the protocol with the cloud provider as the verifier.

$$\mathbb{a} = \Big((m, q') : C := G^m Q^{q'}\, mod\, u \wedge P : \\ = \mathcal{D}_I^m\, mod\, u \wedge m \\ \in \{0,1\}^{r_m + r_\theta + r_\psi + 1} \wedge q' \\ \in \{0,1\}^{r_M + r_\theta + r_\psi + 1}\Big)$$

Thus,

$$QUP\{\mathbb{a}\}(l_I) \tag{5}$$

The cloud provider chooses a random $q'' \leftarrow [2^{r_q - 1}, 2^{r_q} - 1]$ and a random prime$i \leftarrow [2^{r_i}, 2^{r_i} + 2^{r_i'}]$ and computes

$$R := \left(\frac{A}{CQ^{q''}}\right)^{1/i} mod\ M \tag{6}$$

To convince the user that R was correctly computed,the cloud provider as authenticator runs the protocol

$$QUP\left\{(f) : R \equiv \left(\frac{A}{CQ^{q''}}\right)^f mod\ M\right\}(m_C) \tag{7}$$

with the host so that,

a. The user chooses a random integer $m_C \leftarrow \{0,1\}^{r_\psi}$ and sends m_c to the cloud provider.

b. The cloud provider randomly chooses $\mu_i \leftarrow [0, u'_M v'_M]$ and computes

$$\tilde{R} := \left(\frac{A}{CQ^{q''}}\right)^{\mu_i} mod\ M \tag{8}$$

$$z' := \psi(M \parallel A \parallel Q \parallel C \parallel q'' \parallel A \parallel \tilde{A} \parallel m_C) \tag{9}$$

$$b_i := \mu_i + {}^{z'}/_{i}\, mod\, u'_M v'_M \tag{10}$$

and sends z', b_i and (R, i, q'') to the user.

c. The user verifies whether i is a prime and lies in$[2^{r_i}, 2^{r_i} + 2^{r_i'}]$, computes

$$\hat{R} := R^{-z'} \left(\frac{A}{CQ^{q''}}\right)^{b_i} mod\ M \tag{11}$$

and checks whether $z' = \psi(M \parallel A \parallel Q \parallel C \parallel q'' \parallel A \parallel \tilde{A} \parallel m_C)$.

The user sets$q := q'' + q'$ and stores(R, i, m, q) as itsmembership private key.

Same as in the cryptographic protocol scheme, the cloud provider proves to the user that R was formed correctly, i.e., R lies in $\langle t \rangle$. In above procedure, the cloud provider proves that $R \equiv (AC^{-1}Q^{-q''})^f (mod\, M)$ for some value f .Inthesetupprogram, the cloud provider proves that $QGA \in \langle t \rangle$ .Since $C := G^m Q^{q'}\, mod\, M$, the user can conclude that $R \in \langle t \rangle$. Thereason for requiring $R \in \langle t \rangle$ is to assure that later, in the membership approval protocol, R can be statistically hiddenin$\langle t \rangle$. Otherwise, an adversarial cloud provider could link signatures generated by users whose R does not lie in $\langle t \rangle$. Notethat schemes such as have prevented this byensuring that M is a safe-prime product and then made surethat all elements are members of ZG_M. However, provingthat a modulus is a safe-prime product is rather inefficientand hence the setup of these schemes is not practical asour scheme.

e) Membership Approval Protocol

The membership approval protocol is a protocol run by an authenticator and a verifier. It consists of login and verify. In the login step, the authenticator initializes the interaction with the verifier by sending a request to the verifier. There are three types of blacklist: private-key-based blacklist, signature-based blacklist, and cloud provider-based blacklist. Therefore, the blacklist V contains three sublists, i.e.,$V = \{V_{priv}, V_{sign}, V_{cp}\}$ LetV_{priv} be the blacklist for private-key-based blacklist, in which each element is a value in $\langle a \rangle$. Let V_{sign} be the blacklistforsignature-based blacklist, in which each element is a pairof values in$\langle a \rangle$. Let cloud provider V_{cp} be the blacklist for cloud provider-based blacklist, in which each element is a value in$\langle a \rangle$. The blacklisting controller maintains the blacklist and regularly publishes the newest blacklisttoeveryone in the system, signed using his private key. Thatis, the blacklisting controller publishes $\{V_{priv}\}_{P_G^{-1}}$, $\{V_{sign}\}_{P_G^{-1}}$ and $\{V_{cp}\}_{P_G^{-1}}$.

The verifier first chooses a message$s$ and a nonce $l_q \leftarrow \{0,1\}^{r_\psi}$. The verifier then sends to the authenticator s, l_q, $\{V_{sign}\}_{P_G^{-1}}$ and $\{V_{cp}\}_{P_G^{-1}}$ as the challenge. After the authenticator receives the challenges from the verifier, the authenticator verifies the content of $\{V_{sign}\}_{P_G^{-1}}$ and $\{V_{cp}\}_{P_G^{-1}}$using the blacklisting controller's public key P_G. Let (R, i, m, q) be the authenticator's private key. For each element $(\mathcal{D}_\alpha, P_\alpha)$in $\{V_{sign}\}$, the authenticator checks whether $\mathcal{D}_\alpha^m \not\equiv P_\alpha (mod\, u)$. If there exists some α such that$\mathcal{D}_\alpha^m \not\equiv P_\alpha (mod\, u)$, it means that the authenticator has been blacklisted, the authenticator aborts the membership protocol. Analogously, for each item P_α in V_{cp}, the authenticator checks whether $\mathcal{D}_\alpha^m \not\equiv P_\alpha (mod\, u)$ where $\mathcal{D}_I$ is the base derived from the cloud provider's basename $name_I$. The authenticator quits the membership protocol if the check fails. Note that the authenticator can directly obtain V from the blacklisting controller and checks whether he has been blacklisted. However, it is not required for the authenticator to conduct such operation. Also note that it is the verifier's responsibility to obtain the latest blacklist from the blacklisting controller. IfV_{sign} and V_{cp} in the verifier's challenge are not the latest ones, then there is a chance that some blacklisted users may successfully perform membership proof to the verifier without being detected.

i. *Login*

This step is run by the authenticator. The input to this program is the group public key,$(M, s', s, t, G, Q, A, u, v, a)$ the authenticator's private key (R, i, m, q), the verifier's message s and noncel_q, the signature-based blacklist V_{sign} and the blacklist-based blacklist V_{cp}. The output to this program is a signature $\mathbb{S}$ produced by the authenticator. Firstly, the authenticator picks a random $\mathcal{D} \leftarrow \langle a \rangle$ and two integers $\mathbb{O}, \mu \leftarrow \{0,1\}^{r_M + r_\theta}$ and computes $\mathbb{P}_1 := Rt^{\mathbb{O}}\, mod\, M$, $\mathbb{P}_2 := s^{\mathbb{O}} t^i (s')^\mu\, mod\, M$, $P := \mathcal{D}^m mod\, u$

Then, the authenticator produces a signature of knowledge that $\mathbb{P}_1$ and $\mathbb{P}_2$ are commitments to the authenticator's private key and P was computed using the authenticator's secret m. That is, the authenticator computes the signature of knowledge

$$\begin{aligned} &QUP\{m, q, i, \mathbb{O}, \mu, i\mathbb{O}, ii, i\mu : A \\ &\equiv \mathbb{P}_1{}^i G^m Q^q t^{-i\mathbb{O}} (mod\, M) \wedge \mathbb{P}_2 \\ &\equiv s^{\mathbb{O}} t^i (s')^\mu (mod\, M) \wedge 1 \\ &\equiv \mathbb{P}_2{}^{-i} s^{i\mathbb{O}} t^{ii} (s')^{i\mu} (mod\, M) \wedge P \\ &\equiv \mathcal{D}^m (mod\, u) \wedge m \\ &\in (0,1)^{r_M + r_\theta + r_\psi + 1} \wedge (i - 2^{r_i}) \\ &\in \{0,1\}^{r_i' + r_\theta + r_\psi + 1}\}(l_q \parallel s) \end{aligned} \qquad (12)$$

with the following steps:

a. The authenticator picks random integers $\mu_q \leftarrow \{0,1\}^{r_q + r_\theta + r_\psi}$, $\mu_m \leftarrow \{0,1\}^{r_m + r_\theta + r_\psi}$ $\mu_i \leftarrow \{0,1\}^{r_i' + r_\theta + r_\psi}$, $\mu_{ii} \leftarrow \{0,1\}^{r_i + r_\theta + r_\psi + 1}$ $\mu_{\mathbb{O}}, \mu_\mu \leftarrow \{0,1\}^{r_M + 2r_\theta + r_\psi}$, $\mu_{i\mathbb{O}}, \mu_{i\mu} \leftarrow \{0,1\}2^{r_i + r_M + 2r_\theta + r_\psi + 1}$

b. The authenticator computes $\widetilde{\mathbb{P}_1} := \mathbb{P}_1{}^{\mu_i} G^{\mu_m} Q^{\mu_q} t^{-\mu_{i\mathbb{O}}} (mod\, M)$ $\widetilde{\mathbb{P}_2} := s^{\mu_{\mathbb{O}}} t^{\mu_i} (s')^{\mu_\mu} (mod\, M)$ $\widetilde{\mathbb{P}_3} := \mathbb{P}_2{}^{-\mu_i} s^{\mu_{i\mathbb{O}}} t^{\mu_{ii}} (s')^{\mu_{ii}} (mod\, M)$ $\tilde{P} := \mathcal{D}^{\mu_m}\, mod\, u$

c. The authenticator computes

$$z_1 := \psi(M \parallel s' \parallel s \parallel t \parallel G \parallel Q \parallel A \parallel u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \mathbb{P}_1 \parallel \mathbb{P}_2 \parallel \widetilde{\mathbb{P}_1} \parallel \widetilde{\mathbb{P}_2} \parallel \widetilde{\mathbb{P}_3} \parallel \tilde{P} \parallel s \parallel l_q)$$

d. The authenticator computes(over the integers) $b_q := \mu_q + z_1 \cdot q$, $b_m := \mu_m + z_1 \cdot m$, $b_i := \mu_i + z_1 \cdot (i - 2^{r_i})$, $b_\mu := \mu_\mu + z_1 \cdot \mu$, $b_{\mathbb{O}} := \mu_{\mathbb{O}} + z_1 \cdot \mathbb{O}$, $b_{i\mathbb{O}} := \mu_{i\mathbb{O}} + z_1 \cdot \mathbb{O} \cdot i$, $b_{ii} := \mu_{ii} + z_1 \cdot i^2$, $b_{i\mu} := \mu_{i\mu} + z_1 \cdot i \cdot \mu$

e. The authenticator sets

$$\mathbb{S}_1 := (\mathcal{D}, P, \mathbb{P}_1, \mathbb{P}_2, z_1, b_q, b_m, b_i, b_\mu, b_{\mathbb{O}}, b_{i\mathbb{O}}, b_{ii}, b_{i\mu})$$

The authenticator produces a signature of knowledge that his private key has not been blacklisted in V_{sign} . Let $V_{sign} = \{(\mathcal{D}_1, P_1), \dots (\mathcal{D}_{m_2}, P_{m_2})\}$. The authenticator computes the signature of knowledge

$$QUP\{(m) : P \equiv \mathcal{D}^m (mod\, u) \wedge P_1 \not\equiv \mathcal{D}_1^m (mod\, u) \wedge \dots \wedge P_{m2} \not\equiv \mathcal{D}_{m2}^m (mod\, u)\}(l_q \parallel s)$$

with the following steps:

a. The authenticator chooses a random$\mu \longleftarrow \mathbb{A}_v$ and computes $\tilde{P} := \mathcal{D}^\mu \ mod\, u$.

b. For $\alpha = 1, \dots m_2$, the authenticator does the following:

i. The authenticator chooses a random$e_\alpha \longleftarrow \mathbb{A}_v$.

ii. The authenticator computes

$$C_\alpha := \mathcal{D}_\alpha^{e_\alpha} mod\, u \qquad E_\alpha := P_\alpha^{e_\alpha} mod\, u$$
$$F_\alpha := C_\alpha^{e_\alpha} mod\, u$$

iii. The authenticator chooses a random integer $\mu_\alpha \longleftarrow \mathbb{A}_v$

iv. The authenticator computes

$$\tilde{C}_\alpha := \mathcal{D}_\alpha^{\mu_\alpha} mod\, u\, \tilde{E}_\alpha := P_\alpha^{\mu_\alpha} mod\, u\ \tilde{F}_\alpha := C_\alpha^{\mu_\alpha} mod\, u$$

c. The authenticator computes

$$z_2 := \psi(u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \tilde{P} \parallel C_1 \parallel E_1 \parallel F_1 \parallel \tilde{C}_1 \parallel \tilde{E}_1 \parallel \tilde{F}_1 \parallel \cdots \parallel C_{m_2} \parallel E_{m_2} \parallel F_{m_2} \parallel \tilde{C}_{m_2} \parallel \tilde{E}_{m_2} \parallel \tilde{F}_{m_2} \parallel s \parallel V_{sign} \parallel l_q)$$

d. For $\alpha = 1, \dots m_2$, the authenticator computes $b_\alpha := \alpha_\alpha + z_2 \cdot e_\alpha \ mod\, v$

e. The authenticator computes $b := \alpha + z_2 \cdot m \ mod\, v$.

f. The authenticator sets

$$\mathbb{S}_2 := (\mathcal{D}, P, z_2, b, C_1, E_1, F_1, b_1, \dots C_{m_2}, E_{m_2}, F_{m_2}, b_{m_2})$$

The authenticator produces a signature of knowledge that his private key has not been blacklisted in cloud provider V_{cp} . Let cloud provider $V_{cp} = \{\mathcal{D}_1, P_1, \dots P_{m_3}\}$. The authenticator computes the signature of knowledge

$$QUP\{(m) : P \equiv \mathcal{D}^m (mod\, u) \wedge P_1 \not\equiv \mathcal{D}_1^m (mod\, u) \wedge \dots \wedge P_{m3} \not\equiv \mathcal{D}_l^m (mod\, u)\}(l_q \parallel s)$$

The authenticator outputs the signature $\mathbb{S} := (\mathbb{S}_1, \mathbb{S}_2, \mathbb{S}_3)$ and sends $\mathbb{S}$ to the verifier.

Observe that in the sign process, the authenticator proves the knowledge of m such that $\mathcal{D}^m \equiv K\ (mod\, u)$ three times, one in each signature of knowledge. We could merge all three signatures of knowledge together such that the authenticator only needs to prove the knowledge of m once, thus couldimprove the performance of membership approvalslightly. When we present the above sign process, we choose to have three separate proof of knowledge protocols to make our protocol easier to read.

ii. Verify

The group public key is $(M, s', s, t, G, Q, A, a, u, v,)$, the message s, the nonce l_q, the corresponding signature$\mathbb{S} := (\mathbb{S}_1, \mathbb{S}_2, \mathbb{S}_3)$, and the blacklist $V = \{V_{priv}, V_{sign}, V_{cp}\}$. The verifier verifies the signature asfollows:

1. The verifier verifies that s and l_q are the message and the nonce he sent to the authenticator in the challenge step. The verifier also verifies $(\mathcal{D}, P)$in $\mathbb{S}_1$, $\mathbb{S}_2$ and $\mathbb{S}_3$all matches.
2. The verifier verifies the correctness of $\mathbb{S}_1 = (\mathcal{D}, P, \mathbb{P}_1, \mathbb{P}_2, z_1, b_q, b_m, b_i, b_\mu, b_{\mathbb{O}}, b_{i\mathbb{O}}, b_{ii}, b_{i\mu})$ as follows:

i. The verifier computes $b_i' := b_i + z_1 \cdot 2^{r_i}$ and computes

$$\widehat{\mathbb{P}}_1 := A^{-z_1}\ \mathbb{P}_1{}^{b'{}_i} G^{b_m} Q^{b_q} t^{-b_{i\mathbb{O}}} (mod\, M)$$
$$\widehat{\mathbb{P}}_2 := \mathbb{P}_2{}^{-z_i} s^{b_{\mathbb{O}}} t^{b_i} (s')^{b_\mu} (mod\, M)$$
$$\widehat{\mathbb{P}}_3 := \mathbb{P}_2{}^{-b_i} s^{b_{i\mathbb{O}}} t^{b_{ii}} (s')^{b_{i\mu}} (mod\, M) \qquad \tilde{P} := P^{-z_1} \mathcal{D}^{b_m}\ mod\, u$$

ii. The verifier verifies that

$\mathcal{D}, P \in \langle a \rangle$, $\quad b_m \in \{0,1\}^{r_m + r_\theta + r_\psi + 1}$, $\quad b_i \in \{0,1\}^{r_i' + r_\theta + r_\psi + 1}$

iii. The verifier verifies that

$$z_1 := \psi(M \parallel s' \parallel s \parallel t \parallel G \parallel Q \parallel A \parallel u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \mathbb{P}_1 \parallel \mathbb{P}_2 \parallel \widetilde{\mathbb{P}_1} \parallel \widetilde{\mathbb{P}_2} \parallel \widetilde{\mathbb{P}_3} \parallel \tilde{P} \parallel s \parallel l_q)$$

3. The verifier verifies that the authenticator's private key has not been black listed in V_{priv} , where $V_{priv} = \{m_1, \dots m_{m_1}\}$. . For $\alpha = 1, \dots m_2$, the verifier verifies that$P \not\equiv \mathcal{D}^{m_\alpha} (mod\, u)$
4. The verifier verifies the correctness of $\mathbb{S}_2 := (\mathcal{D}, P, z_2, b, C_1, E_1, F_1, b_1, \dots C_{m_2}, E_{m_2}, F_{m_2}, b_{m_2})$ based on $V_{sign} = \{(\mathcal{D}_1, P_1), \dots (\mathcal{D}_{m_2}, P_{m_2})\}$. It takes the following steps:

a. The verifier computes $\hat{P} \equiv P^{-z_2} \mathcal{D}^b (mod\, u)$

b. For $\alpha = 1, \dots m_2$, the verifier does the following:

i. The verifier verifies that

$C_\alpha E_\alpha F_\alpha \in \langle a \rangle$, $\quad b_\alpha \in \mathbb{A}_v$, $\qquad E_\alpha \neq F_\alpha$

ii. The verifier computes

$$\hat{C}_\alpha := C_\alpha{}^{-z_1} \mathcal{D}^{b_\alpha}\ mod\, u, \quad \hat{E}_\alpha := E_\alpha{}^{-z_1} P^{b_\alpha}\ mod\, u \quad , \quad \hat{F}_\alpha := F_\alpha{}^{-z_1} C^{b_\alpha}\ mod\, u$$

c. The verifier verifies that

$$z_2 := \psi(u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \tilde{P} \parallel C_1 \parallel E_1 \parallel F_1 \parallel \tilde{C}_1 \parallel \tilde{E}_1 \parallel \tilde{F}_1 \parallel \cdots \parallel C_{m_2} \parallel E_{m_2} \parallel F_{m_2} \parallel \tilde{C}_{m_2} \parallel \tilde{E}_{m_2} \parallel \tilde{F}_{m_2} \parallel s \parallel V_{sign} \parallel l_q)$$

5. The verifier verifies the correctness of $\mathbb{S}_3 := (\mathcal{D}, P, z_3, b_e, b_m, C_1, E_1 \dots C_{m_2}, E_{m_3}, F)$ based on $V_{cp} = \{\mathcal{D}_1, P_1, \dots P_{m_3}\}$. It takes the following steps:

i. The verifier verifies that

$C, E \in \langle a \rangle$, $\qquad b_e, b_m \in \mathbb{A}_v$

ii. The verifier computes $\hat{P} := P^{-z_3}\mathcal{D}^{b_m} \ mod\ u \qquad \hat{C} := C^{-z_3}\mathcal{D}^{b_\alpha} \ mod\ u, \qquad \hat{F} := F^{-z_3}C^{b_\alpha} \ mod\ u$

6. If all the verifications succeed, the verifier outputs succeed, otherwise outputs fail.

iii. Blacklist

There are three sub lists in the blacklist:V_{priv} , V_{sign} , andV_{cp} . Initially, V_{priv} and V_{sign} are set to beempty, and V_{cp} is set to be $\{\mathcal{D}_I\}$, where $\mathcal{D}_I \equiv T_u(name_I)^{u-1/v} \ mod\ u$ and $name$ is the cloud provider's basename.There are three ways to blacklist a cloud user. Firstly, when a user is compromised and his private key(R, i, m, q) has been exposed (e.g., on the Internet orembedded into some software), the blacklisting controller verifies the correctness of this exposed key by checking $R^i G^m Q^q \equiv A \ (mod\ M)$, then adds $m$to V_{priv} .

Secondly, when a verifier interacts with some compromised authenticator and finds the authenticator suspicious, the verifier reports the authenticator's signature$\mathbb{S} := (\mathbb{S}_1, \mathbb{S}_2, \mathbb{S}_3)$ alongwith some other physical evidences to the blacklisting controller. After the blacklisting controllerverifies the evidences and correctness of $\mathbb{S}_1$, he adds(P, U) in $\mathbb{S}_1$ to V_{sign} . Then finally, when the cloud provider wants to blacklist a cloud user (e.g., because that user leaves the group), the cloud provider sends (P, C, Θ) to the blacklisting controller, where the (P, C, Θ) tuple was obtained from the to-be- blacklisted user during the register protocol. The blacklisting controller verifies that correctness of $\Theta$and then adds P to cloud provider blacklist V_{cp} .

When the blacklisting controller renounces a user based on the signature of the user, it needs to make sure that the signature is valid. That is, the signature was signed by a group member. This is to prevent a malicious verifier fromadding arbitrary$(\mathcal{D}, P)$ pair toV_{sign} . Similarly, when the blacklisting controller revokes a user based on (P, C, Θ) fromthe cloud provider, he needs to make sure that Θ is a correct signature of knowledge. This is to prevent the (malicious) cloud provider from adding arbitrary P toV_{cp} . Observe that, the cloud provider can always add new members, create new signatures, and later revoke the members that he created by herself. However, even though the malicious cloud provider can choose P of his choice, he has to know $\log_{\mathcal{D}} P$ in order to create a valid signature $\mathbb{S}$ or know $\log_{\mathcal{D}_I} P$ to create a valid Θ.This is a requirement in our security proof. After the blacklisting controller publishes the blacklist $V$and signs using his private keyP_G^{-1} , everyone can verifythe authenticity of this blacklist using the blacklisting controller's public key P_G . In practice, we may assume that the blacklisting controller is trusted. Then, the verifiers trust the blacklisting controller to construct the blacklist in a correct manner. In the model where the blacklisting controller is not completely trusted, the blacklisting controller also needs to publish a compromised private key for each item in V_{priv} , a signature for each item in V_{sign} , and a (P, C, Θ) tuple for each element in V_{cp} . The verifiers have to verify the correctness of each element in the blacklist in the same way as the blacklisting controller does. We show that that even if the blacklisting controller or the cloud provider has been corrupted by the adversary, the anonymity of the honest users is still guaranteed.

The initialize and register have the same performance as in the cryptographic protocol scheme. The cost of membership approval protocol has four parts: proof of knowledge of a membership private key, verification that the private key is not in V_{priv} , proof that the private key does not appear in V_{sign} ,and proof that the private key does not appear inV_{cp} . The first part of the membership approval protocol is the same as the cryptographic protocol scheme and takes constant time for both the authenticator and verifier. The second part is also the same as the cryptographic protocol scheme and takes m_1 modular exponentiations for the verifier, where m_1 is the size of V_{priv} . The third andfourth parts together take about $6m_2 + 2m_3 + z$ modul are xponentiations for both the authenticator and verifier, where m_2 and m_3 are the lengths of V_{sign} and V_{cp} , respectively, and z is a small constant.Observe that the cost of membership approval is linear to the size of the blacklist and could be quite expensive if the blacklist becomes large. There are two possible ways to control the size of the blacklist. First, divide into smaller groups. If the group size is too big, the blacklist may become large as well. One way is to control the size of the blacklist is to have multiple smaller groups. If a group size was 10,000, and at most two percent of the users would get blacklisted, then the blacklist would have at most 200 items. The drawback of this method is that the verifier needs to know which group the authenticator is in, thus, learns more information about the authenticator. It is a trade-off between privacy and performance.

Second, issue a new group if the blacklist grows too big. If the size of the blacklist is above certain threshold (e.g., two percent of the group size), then the cloud provider can do a rekey process as follows: The cloud provider first creates a new group. Then, each user in the old group proves to the cloud provider that he is a legitimate member of the old group and has not been blacklisted, then obtains a new membership private key for the new group.

f) *Membership approval for Resource-Constrained Devices*

If the authenticator is a resource-constrained device, such as a TPM, a smart card, or a secure coprocessor; it can outsource part of the signing operation to a semi trusted host. Essentially, the signing operation is split between a computationally weak device (denoted as the principal authenticator) and a resource a bundant but less-trusted host. Observe that if the host does not cooperate, then it is a denial of service. Thus, the host platform is trusted for performing its portion of computation correctly. However, the host is not allowed to learn the private key of the authenticator or to forge a signature without the principal authenticator's involvement. This model is used in the original cryptographic protocol scheme with a concrete security model.

For our scheme, the same technique from can be applied. Let (R, i, m, q) be the principal authenticator's private key. The principal authenticator sends (R, i) to the host but keeps(m, q). The signing operation in the membership approval can be conducted as follows:

1. The principal authenticator picks a random$\mathcal{D} \leftarrow \langle a \rangle$ and computes $P \equiv \mathcal{D}^m (mod\, u)$
2. The principal authenticator sends $(\mathcal{D}, P)$ to the host.
3. The host randomly chooses two integers $\mathbb{O}, \mu \leftarrow \{0,1\}^{r_M + r_\theta}$ and computes

   $\mathbb{P}_1 := Rt^{\mathbb{O}}\ mod\ M, \quad \mathbb{P}_2 := s^{\mathbb{O}} t^i (s^{'})^{\mu}\ mod\ M$
4. The principal authenticator and the host jointly produce a signature of knowledge that $\mathbb{P}_1$ and $\mathbb{P}_2$ are commitments to (R, i) and P was computed using the authenticator's secret m. That is, they compute the signature of knowledge

$$\begin{aligned} &QUP\{m, q, i, \mathbb{O}, \mu, i\mathbb{O}, ii, i\mu : A \\ &\equiv\ {\mathbb{P}_1}^i G^m Q^q t^{-i\mathbb{O}} (mod\ M) \wedge \mathbb{P}_2 \\ &\equiv\ s^{\mathbb{O}} t^i (s^{'})^{\mu} (mod\ M) \wedge 1 \\ &\equiv {\mathbb{P}_2}^{-i} s^{i\mathbb{O}} t^{ii} (s^{'})^{i\mu} (mod\ M) \wedge P \\ &\equiv \mathcal{D}^m (mod\, u) \wedge m \\ &\in (0,1)^{r_M + r_\theta + r_\psi + 1} \wedge (i - 2^{r_i}) \\ &\in \{0,1\}^{r_{i'} + r_\theta + r_\psi + 1}\}(l_q \parallel s) \end{aligned} \tag{13}$$

With the following steps:

a. The principal authenticator chooses a random integers

$\mu_q \leftarrow \{0,1\}^{r_q + r_\theta + r_\psi}, \qquad \mu_m \leftarrow \{0,1\}^{r_m + r_\theta + r_\psi}$

And computes

$\widetilde{\mathbb{P}}_{1\wp} := G^{\mu_m} Q^{\mu_q} (mod\ M) \qquad \tilde{P} := \mathcal{D}^{\mu_m}\ mod\ u$

And sends $\widetilde{\mathbb{P}}_{1\wp}$ and $\tilde{P}$ to the host.

b. The host picks random integers

$\mu_i \leftarrow \{0,1\}^{r_{i'} + r_\theta + r_\psi}, \qquad \mu_{ii} \leftarrow \{0,1\}^{r_i + r_\theta + r_\psi + 1}$

$\mu_{\mathbb{O}}, \mu_\mu \leftarrow \{0,1\}^{r_M + 2r_\theta + r_\psi},$

$\mu_{i\mathbb{O}}, \mu_{i\mu} \leftarrow \{0,1\}2^{r_i + r_M + 2r_\theta + r_\psi + 1}$

c. The host computes

$\widetilde{\mathbb{P}}_1 := \widetilde{\mathbb{P}}_{1\wp} {\mathbb{P}_1}^{\mu_i} t^{-\mu_{i\mathbb{O}}} (mod\ M)$

$\widetilde{\mathbb{P}}_2 := s^{\mu_{\mathbb{O}}} t^{\mu_i} (s^{'})^{\mu_\mu} (mod\ M)$

$\widetilde{\mathbb{P}}_3 := {\mathbb{P}_2}^{-\mu_i} s^{\mu_{i\mathbb{O}}} t^{\mu_{ii}} (s^{'})^{\mu_{ii}} (mod\ M) \tilde{P} := \mathcal{D}^{\mu_m}\ mod\ u$

d. The host computes

$z_t := \psi(M \parallel s^{'} \parallel s \parallel t \parallel G \parallel Q \parallel A \parallel u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \mathbb{P}_1 \parallel \mathbb{P}_2 \parallel \widetilde{\mathbb{P}_1} \parallel \widetilde{\mathbb{P}_2} \parallel \widetilde{\mathbb{P}_3} \parallel \tilde{P} \parallel l_q)$

and sendsz_t to the principal authenticator.

e. The principal authenticator chooses a random $l_{\mathbb{P}} \leftarrow \{0,1\}^{r_\theta}$ and computes

   $z_1 := \psi(z_t \parallel l_{\mathbb{P}} \parallel s)$

And sends z_t and $l_{\mathbb{P}}$ to the host

f. The principal authenticator computes (over the integers)

$b_q := \mu_q + z_1 \cdot q, \qquad b_m := \mu_m + z_1 \cdot m$

And sends b_q and b_m to the host

g. The host computes

   $b_i := \mu_i + z_1 \cdot (i - 2^{r_i}), \quad b_\mu := \mu_\mu + z_1 \cdot \mu, \quad b_{\mathbb{O}} := \mu_{\mathbb{O}} + z_1 \cdot \mathbb{O},$

   $b_{i\mathbb{O}} := \mu_{i\mathbb{O}} + z_1 \cdot \mathbb{O} \cdot i, \quad b_{ii} := \mu_{ii} + z_1 \cdot i^2, \quad b_{i\mu} := \mu_{i\mu} + z_1 \cdot i \cdot \mu$

h. The host sets

   $\mathbb{S}_1 = (\mathcal{D}, P, \mathbb{P}_1, \mathbb{P}_2, z_1, l_{\mathbb{P}}, b_q, b_m, b_i, b_\mu, b_{\mathbb{O}}, b_{i\mathbb{O}}, b_{ii}, b_{i\mu})$

5. The principal authenticator produces a signature of knowledge that his private key has not been blacklisted in V_{sign} and V_{vp}, the same as in the sign algorithm.

Note that the verification operation in the membership approval protocol will change slightly to be consistent with the signing operation. More specifically, the verifier now verifies

$$z_1 := \psi(\psi(M \parallel s^{'} \parallel s \parallel t \parallel G \parallel Q \parallel A \parallel u \parallel v \parallel a \parallel \mathcal{D} \parallel P \parallel \mathbb{P}_1 \parallel \mathbb{P}_2 \parallel \widetilde{\mathbb{P}_1} \parallel \widetilde{\mathbb{P}_2} \parallel \widetilde{\mathbb{P}_3} \parallel \tilde{P} \parallel l_q) \parallel l_{\mathbb{P}} \parallel s)$$

Also note that the steps 3 and 4 cannot be outsourced to the host, because the host does not know the m value. As we shall discuss in the following Section, for implementing our scheme intamper-resistant hardware devices, the blacklists (V_{priv}, V_{sign}, V_{vp}) expect to be very small, asthese blacklists only grow when there are physical attacks on these devices.

g) Using TPM Hardware

We could have the following benefits using the TPM hardware: 1) less computational work for trusted hardware device, 2) portability and 3) more efficient blacklist mechanism. The main design principle is that the host and the hardware jointly perform the membership approval as the authenticator. The host, if corrupted, could break the anonymity of the user but cannot get to know the user's membership private key. Because in any case, the host can pad some identifier to each message sent by the hardware device. Another advantage of using trusted hardware device is to have more efficient blacklist. Thus, a user is blacklisted in the following cases. The user's membership private key was removed from the trusted hardware device, and was published widely so that everyone knows this compromised private key, it's been blacklisted. When the user's membership private key was extracted from the trusted hardware device by the adversary. The cloud provider suspects that the user's hardware device was compromised, but has not obtained the user' sprivate key. Thus, blacklisted. The user's membership private key was extracted from the hardware device by the adversary. The blacklisting controller suspects that the hardware device was corrupted. The blacklisting controller obtains a signature from the corrupted device but has not obtained the private key becomes blacklisted. The cloud provider blacklists the user for some management reason, e.g., the user's membership expired. The user is blacklisted from transactions, more specifically the user abuses his group privilege and is blacklisted by the blacklisting controller after the user conducted a membership approval.

IV. Experimental Study

The portable TPM based user attestation architecture for cloud environments model has been developed for highly authenticated and secured cloud computing environment. The system model presented has been developed on Visual Studio 2012 framework 4.0 with C#. The overall system has been developed and implemented with Microsoft Windows Azure platform.

We mainly focused on data leakages that can occur in the cloud environment. Portable TPM based user attestation architecture supports hardware-based key management by using TPM devices to provide better security and hence device portability is attained. Therefore, a user can access to cloud storage's contents in secure environment and securely store user data to the remote cloud server using this portable devices which provides added security.

The developed system has been simulated on live Microsoft Windows Azure cloud for different performance parameters like cloud memory utilization, user attestation overhead and the Qos perspective for CPU utilization. The relative study for these all factors has been performed. This system or model performance has been verified for various user size with the assigned authentication devices and the effectiveness as well as performance parameters have been checked for its robustness justification.

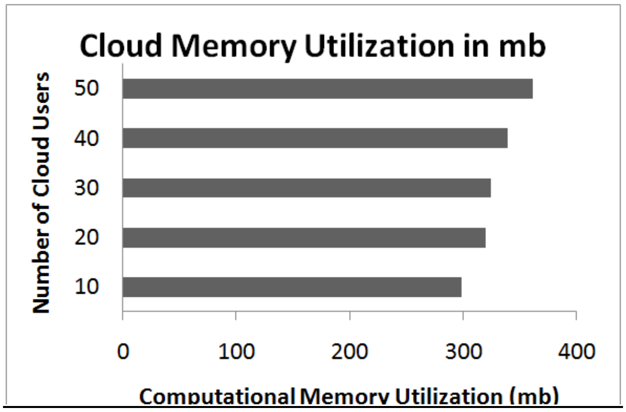


Figure 1 : Cloud Memory Utilization

The above mentioned figure (Figure 1) depicts the cloud memory utilization in megabytes based on the respective set of cloud users from 10 to 50. Here, the memory utilization is computed based on the user which is able to access the cloud service through his credentials along with the additional authenticated device, TPM. Usually for users to access cloud, cloud providers may be concerned about the memory utilization of varied users. From the graph, it can be justified that not much memory is utilized with the additional security parameter. It clearly shows that even though the cloud users are 50, the cloud memory utilization is not differing much. Thus, memory computation is highly adaptive.

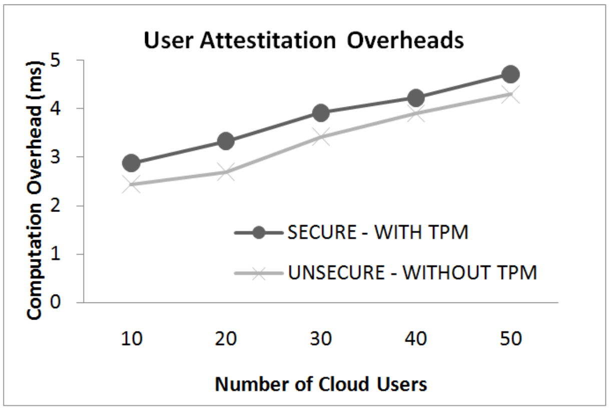


Figure 2 : User Attestation Overhead

Based on the simulated data, the graph (Figure 2) is plotted making the comparison of the user attestation overhead of our proposed system with portable TPM device against the user attestation without TPM. The computation overheads with and without TPM [18] is being evaluated in milliseconds. Without the external device it is obvious that the computation is of less value. Therefore, from the figure it is evaluated that the average computation overhead without the TPM device (without added security) is 5.58ms. The average computation overhead with the usage of TPM which provides additional security is evaluated to be 6.35ms.

Thus, the average computational overhead increase is $\approx 13ms$ which is very negligible when considering a highly secure cloud environment with the cryptographic protocols.

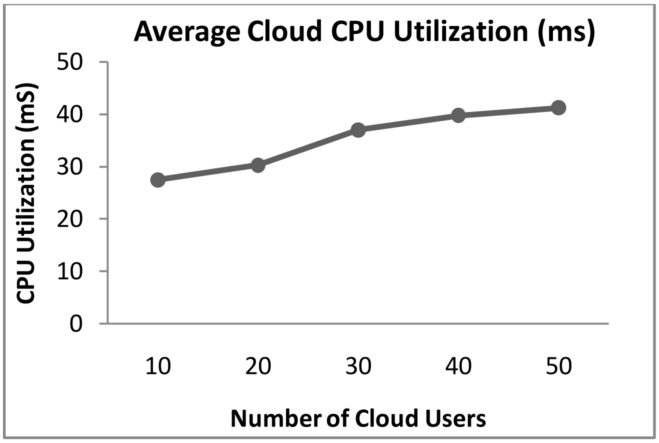


Figure 3 : Average Cloud CPU Utilization

There must be the processing time of the virtual machines considered when accessing the cloud services. The average cloud CPU utilization is been depicted in milliseconds which is plotted in the above graph. For every user interaction with the cloud services, the CPU is utilized. Here, users are accessing the cloud with the portable TPM devices and the average cloud CPU utilization is plotted. As the users increase from 10 to 50, the processing time also increases. The average utilization of the CPU is found to be $\approx 35ms$.

Therefore from these results, we have established that the proposed model can be an effective, secure and optimum adaptable approach for portable TPM based user attestation architecture for cloud environment.

V. Conclusion

There is a growing demand for sharing data with a large number of consumers using the Cloud. One of the main issues with data sharing in such environments is the privacy and security of information. In particular, the issue of preserving confidentiality of the cloud data and also the need to keep the credentials while respecting the policies set out by the cloud provider. We mainly focused on data leakages that can occur in either client-side or server-side [17]. In this paper we have proposed novel property based attestation techniques for the cloud. We have designed a hardware based device which is portable for further security. We propose a portable device which is used in the authentication and verification of the cloud user. We have discussed our secure data sharing protocol, which allows highly confidential data sharing. The portable TPM based user attestation architecture for cloud environments model exploits client-side authentication with encryption technique to mitigate server-side data leakages such as malicious insider attack or exploiting vulnerabilities of server platform. Due to remote attestation protocol for verifying the client, we ensure that malicious behaviors cannot occur. Therefore, a user can access to cloud storage's contents in secure mobile environment and store user data to the remote server in encrypted form using securely created and managed data encryption key. We also developed a set of security models such as public key cryptographic protocols and carried out a security analysis on our protocol.

Asp.Net MVC is lightweight, provide full control over mark-up and support many features that allow fast & agile development. Hence it is best for developing interactive web application with latest web standards. Thus, our future work we will aim to improve the performance of our protocol based on the Asp.Net MVC Cloud architecture and thus providing security for SaaS cloud with the help of the portable TPM which will be feasible for the cloud users.

VI. Acknowledgment

The authors would like to express their cordial thanks to Mr. Ashutosh Kumar and Mr. Kashyap Dhruve of Planet-/ Technologies for their much valued support and advice.

References Références Referencias

1. Benoit Bertholon, Sebastien Varrette and Pascal Bouvry, "CERTICLOUD: a Novel TPM-based Approach to Ensure Cloud IaaS Security" 2011
2. FarzadSabahi, "Cloud Computing Security Threats and Responses", IEEE 3488 rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715.
3. Houlihan, R.; Xiaojiang Du, "An effective auditing scheme for cloud computing," Global Communications Conference (GLOBECOM), 2012 IEEE , vol., no., pp.1599,1604, 3-7 Dec. 2012
4. Xin Wan; Zhiting Xiao; Yi Ren, "Building Trust into Cloud Computing Using Virtualization of TPM," Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on , vol., no., pp.59,63, 2-4 Nov. 2012
5. Jaebok Shin; Yungu Kim; Wooram Park; Chanik Park, "DFCloud: A TPM-based secure data access control method of cloud storage in mobile devices," Cloud Computing Technology and Science (Cloud Com), 2012 IEEE 4th International Conference on, vol., no., pp.551,556, 3-6 Dec. 2012
6. Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2 International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010,

Vol 2, pp 11-15, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.

7. Duflot "Getting into the SMRAM: SMM reloaded" Proc. of the 10thCanSecWest conference, 2009.
8. Hua Wang; Yao Guo; Xia Zhao; Xiangqun Chen, "Keep Passwords Away from Memory: Password Caching and Verification Using TPM," Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on , vol., no., pp.755,762, 25-28 March 2008.
9. I.Corporation. Software developer's manual vol. 3: System programming guide, June 2009.
10. Thilakanathan, Danan; Chen, Shiping; Nepal, Surya; Calvo, Rafael A.; Liu, Dongxi; Zic, John, "Secure Multiparty Data Sharing in the Cloud Using Hardware-Based TPM Devices," Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on , vol., no., pp.224,231, June 27 2014-July 2 2014
11. Varadharajan, V.; Tupakula, U., "TREASURE: Trust Enhanced Security for Cloud Environments," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.145,152, 25-27 June 2012
12. J. McCune, B. Parno, A. Perrig, M. Reiter, and H. Isozaki. "Flicker: an execution infrastructure for TCB minimization." Proc. of the ACM European Conference on Computer Systems (EuroSys), March, April 2008.
13. ARM, "ARM Securtiy Technology, Building a Secure System using Trust Zone Technology", 2009
14. Trusted Computing Group. TPM specifications version 1.2. https:llwww.trustedcomputinggroup.org/downloads/specifications/tpm, July 2005
15. Dan Boneh, Hovav Shacham "Group Signatures with Verfier -Local Revocation", Proceeding of the 11th ACM conference on Computer and communications security, NY 2004. Pages 168-177
16. TPM. http://www.trustedcomputinggroup.org/resources/tpm_main_specification
17. Amazon S3, "Using Data Encryption" http://docs.amazonwebservices.com/AmazonS3/latest/dev/Using Encryption.html
18. R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang. Enabling Security in Cloud Storage SLAs with Cloud Proof. In Proceeding of the 2011 USENIX Annual Technical Conference, June 2011.

Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 1 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A New Efficient Cloud Model for Data Intensive Application

By Rama Satish K V & Dr. N P Kavya

Abstract- Cloud computing play an important role in data intensive application since it provide a consistent performance over time and it provide scalability and good fault tolerant mechanism. Hadoop provide a scalable data intensive map reduce architecture. Hadoop map task are executed on large cluster and consumes lot of energy and resources. Executing these tasks requires lot of resource and energy which are expensive so minimizing the cost and resource is critical for a map reduce application. So here in this paper we propose a new novel efficient cloud structure algorithm for data processing or computation on azure cloud. Here we propose an efficient BSP based dynamic scheduling algorithm for iterative MapReduce for data intensive application on Microsoft azure cloud platform. Our framework can be used on different domain application such as data analysis, medical research, dataminining etc… Here we analyze the performance of our system by using a co-located cashing on the worker role and how it is improving the performance of data intensive application over Hadoop map reduce data intrinsic application. The experimental result shows that our proposed framework properly utilizes cloud infrastructure service (management overheads, bandwith bottleneck) and it is high scalable, fault tolerant and efficient.

Keywords: big data, scheduling, iterative mapreduce, microsoft azure, hadoop.

GJCST-B Classification : C.2.1, E.1

ANEWEFFICIENTCLOUDMODELFORDATAINTENSIVEAPPLICATION

Strictly as per the compliance and regulations of:

A New Efficient Cloud Model for Data Intensive Application

Rama Satish K V [α] & Dr. N P Kavya [σ]

Abstract- Cloud computing play an important role in data intensive application since it provide a consistent performance over time and it provide scalability and good fault tolerant mechanism. Hadoop provide a scalable data intensive map reduce architecture. Hadoop map task are executed on large cluster and consumes lot of energy and resources. Executing these tasks requires lot of resource and energy which are expensive so minimizing the cost and resource is critical for a map reduce application. So here in this paper we propose a new novel efficient cloud structure algorithm for data processing or computation on azure cloud. Here we propose an efficient BSP based dynamic scheduling algorithm for iterative MapReduce for data intensive application on Microsoft azure cloud platform. Our framework can be used on different domain application such as data analysis, medical research, datamininingetc… Here we analyze the performance of our system by using a co-located cashing on the worker role and how it is improving the performance of data intensive application over Hadoop map reduce data intrinsic application. The experimental result shows that our proposed framework properly utilizes cloud infrastructure service (management overheads, bandwith bottleneck) and it is high scalable, fault tolerant and efficient.

Keywords: big data, scheduling, iterative mapreduce, microsoft azure, hadoop.

I. Introduction

Cloud computing technology is increasingly getting attention as a future paradigm for hosting, computing and delivering service over the internet. Cloud provides different service which are classified as follows and Infrastructure (Infrastructure as a Service: IaaS), Platform (Platform as a Service: PaaS), Software (Software as a service: SaaS). Cloud service provider provides user to access different type of service such as storage, software or hardware. In particular, in recent years IaaS have become increasingly popular for user to deploy his application on to the cloud for execution and use the cloud resource efficiently. Cloud computing also provides scalable resource computing and storage resources through the Internet [1]–[2]. It also allow cloud users to access services irrespective to where the cloud services are provided and how they are delivered, similar to other essential commodity(electricity, water)[3]. With the adaptable, transparent and scalable features in the service provisioning and resource allocation, more and more data-intensive applications are developed by using cloud computing environment. The data intensive applications spend most of their execution time in disk I/O operation for processing a huge volume of data, e.g. data mining of different enterprises transactions, satellite data processing, medical research computation, etc. Hadoop [4] is a well-known cloud computing platform which is used for data-intensive applications. Due to a large number of nodes in the cloud computing system, the probability of hardware failures is not a big issue based on the statistical analysis of hardware failures in [5]–[6]. Some hardware failures will damage the disk data of nodes. As a result, the running data-intensive applications may not fetch/read map data from disks properly. To come out of these map failures, the data replication technique is used in the cloud computing environment which provides high data availability [7]–[8]. When data map failure occurs, the QoS requirement of the application cannot be supported continuously. The reason is explained as follows. With a large number of nodes in the cloud computing environment, it is practically not possible ask all nodes with the same performance and capacity in their CPUs, memory, and disks [9]. For example, the Amazon EC2 is a well-known heterogeneous cloud platform, which provides various infrastructure resource types to meet different user needs in resource computing and storage [10].

The Microsoft Azure is a cloud computing environment which offers services on demand. It offers on demand computing services such as Windows Azure Compute, Storage Blob, Queue, Table service etc. Azure Compute is a platform as a service infrastructure which allow the users to lease hourly charged virtual machine instances in the form of different types of Roles such as(e.g.: Worker Role, Web Role, etc…). The Azure storage queue is an eventual consistent, reliable, scalable and distributed message queue service, which is ideal for small and transient messages (short period/impermanent). The Azure Storage Blob service provides a shared storage service where users can store and retrieve any type data by using web services interface. Azure Storage Table service provides scalable non-relational highly available structured data storage. However Azure platform currently do not offer a distributed computing framework, other than the simple queue based model.

Goal of our model is to provide and process the efficient execution of Map Reduce and iterative Map Reduce applications in the Azure cloud environment.

Author α σ : e-mails: ramasatish.k.v@rnsit.ac.in, n.p.kavya@rnsit.ac.in

Our model is a distributed decentralized Map Reduce runtime for Windows Azure cloud environment that utilizes Azure infrastructure services. Our model overcomes the latencies of cloud services by using sufficiently fine grained map and reduces tasks. It overcomes the eventual data availability of cloud storage services through re-trying and by explicitly designing the system to not rely on the immediate availability of data across all distributed workers. Our systems uses Azure Queues for map and reduce BSP task scheduling, Azure Tables for metadata storage and for monitoring data storage, Azure Blob storage for data storage (input, output and intermediate) and Compute worker roles to perform the computations. In order to with stand the breakdown/failure of cloud infrastructures and to avoid single point of failures, our model was designed as a decentralized control architecture which does not rely on a client side. It provides users with the capability to scale up/down the number of computing resources such virtual machines dynamically or during runtime. The map and reduce tasks of the proposed model runtime are dynamically scheduled using azure global queues achieving efficient scheduling natural load balancing of tasks. Our system models handles BSP task failures and slower tasks through re-execution and duplications. Map Reduce infrastructure requires the reduce tasks to ensure guarantee of all the intermediate data products from Map tasks before starting the reduce phase.

Data Iterative computation generally relies on a set of static data that remain fixed across different iterations and a set of ephemeral dynamic data between iterations. Here we introduces an in memory co-located Data Cache to store the reusable static data across the iterations, avoiding the fetching and parsing cost of such data from Azure Blob storage for every iteration. Each worker role will have one managed collocated cache with a given memory limit. Since the existing model do not have proper mechanism which can utilize the knowledge about cached data products to assign tasks to workers, scheduling tasks to take advantage of caching presents a significant challenge. At the same time, it's important to maintain the efficient scheduling and fault tolerance of our model in the new scheduling mechanism. In order to address these issues, our model utilizes a new efficient scheduling approach using a combination of Azure Queues and Tables. The first iteration of our model will get scheduled only through Azure queues. Our model uses a special table for caching, where the tasks are retrieved from second iteration onwards. Map Workers first query this table to identify any similarity between the data items they have in their collocated cache vs the data items needed for the retrieval of tasks. With this prototype the static data for data iterative Map Reduce computations will get reused from the second iteration onwards. Meanwhile the newly joined or a worker who has completed processing all the tasks for the cached data will be able to pick up BSP tasks directly from the queue and will use the Azure Tables and the monitoring infrastructure to check the tasks processed or not. This also ensures that our model retains the fault tolerance features of efficient azure cloud structure.

II. Existing System

Over the year cloud computing is growing enormously in various fields. Data intensive application is one of those fields that have been one of the popular topics. In recent research, the valuable knowledge that can be retrieved from petabyte scale datasets is known as Big Data. Using these analyses the researcher can provide better provide better result. This Big Data analysis is used in different domain such data mining, medical research etc… There exists a substantial body of research on resource allocation and scheduling in clouds and data centers that does not consider the resource utilization efficiency (e.g., [12], [13], and [14]). However, here in this literature review, we only discuss briefly the studies that are directly related to resource utilization in data centers. Kaushik and M. Bhandarkar. [11] Proposed a technique to segregate or divide the servers in a HDP cluster into hot zone and cold zones based on their various performance characteristics, where cold zone servers are mostly idling and hot zone are always powered on. Resource utilization/allocation and scheduling in cloud data centers. Mahadik and Hacker [16] proposed scheduling algorithm policy for virtual HPC clusters. They introduced a resource prediction cloud model for each policy to assess the resources required within a cloud, the task queue wait time for requests, and the size of the additional resources required. Palanisamy et al. [15]proposed a Map Reduce cloud model for creating task. Here they create cluster configurations for the Task using Map Reduce to predict and maximize performance based on deadline-perception, allowing the CSP to optimize its resource allotment and reduce the cost. Zaharia et al. [17] have analyzed the problem of (slower node) speculative execution in Map Reduce. Here they developed a simple robust scheduling algorithm called LATE (Longest Approximate Time to End), which uses predicted completion times to execute the job that hurt the response time the most. Lai and Sandholm [18] have developed a system for resources allocation in shared data and compute resource clusters that enhance Map Reduce job scheduling. Their technique is based on keeping apart Map Reduce clusters in VMs with a dynamically modifiable performance. Wang et al. [19] proposed a new job scheduling technique for Map Reduce that improves the overall throughput in job-intensive application without considering the resource consumption. Ren et al. [20] proposed a task scheduling algorithm that boost the completion time of small Map Reduce jobs. Their system is based on task priorities to make sure the fast response for small tasks. Chang et al. [21] proposed numerous offline and online system for the Map Reduce scheduling complication to minimize the overall task finishing times. Their system is based on resolving a linear program (LP) relaxation. Changjian Wang et al. [22], here they have presented an optimal scheduling algorithm for data map reduce application. Here they have divided algorithm into two stages which are as follows firstly to estimate the node execution time and then to produce proper or optimal task assignment time. Here they only considered map status that is idle or busy for scheduling job to mappers. This approach leads to few problems like long tail and very high scheduling overhead. Qi Chenwe et al. [23]here they provide an analysis of the downfall of existing or recent speculative execution strategies in Map Reduce. Here they present model which affect the overall performance of those technique: jobs that start asynchronously, improper configuration of phase percentage, data skew and abrupt resource competiveness. Based on these terms, here they developed a new speculative execution model called MCP to handle these scenarios. It takes the task cost performance of cluster computing resources into account, aiming at not only reducing the task execution time but also improving the overall cluster throughput. Yang Wang et al. [24] here they have analyzed two general constraints on budget and deadline for the scheduling of a group of Map Reduce tasks as a workflow on a set of vm'sin the cloud. Here first, they focused on the scheduling-length under budget constraints. Then they designed a new algorithm by combining greedy algorithm with dynamic programming techniques for budget allocation on per-stage basis, which was also shown to be balanced. Then, with this result, here they designed two new heuristic algorithms, GGB and GR, which are based on greedy strategies to reduce the time complexity to reduce the scheduling lengths of the workflows without affecting the budget. Our research reveal that both the algorithms exhibiting a unique or significant advantage over the other, are very close to the optimal algorithm in terms of the scheduling time but obtain much lower time overhead. Amrit Pal et al. [25] here they shows the behavior of the hdp cluster with increasing number nodes. The criterion for which the performance is analyzed is the memory parameters. This research will be useful for the developing a hdpcluster. The number of interaction increases as the size of the cluster size increases. If the data size increases and there may be a chance of out of disk then the normal copy script should be used for increasing virtual disks size. Fan Yuanquan et al.[26] here they shows that the existing Map Reduce platform performs poorly on heterogeneous clusters due to skew loads among the reduce jobs. Here they analyze the downfall of current task distribution method in heterogeneous systems. Here they identify two key reasons for the skew loads: and the heterogeneity of worker nodes and the native hash partitioning. Based on these facts they proposed a performance based prediction model which is based on support vector machine called PM-SVM. Here they also proposed a HAP (heterogeneity- aware partitioning) algorithm based on PM-SVM. They implemented the proposed load balance approaches in the HDP. The hadoop load balancer can improve the performance of reduce jobs, and can also improve the resource utilization of hdpclusters.

III. Proposed System

A Map Reduce job divides the input data into individual chunks which are processed by the map jobs in a completely parallel synchronization manner. The output of the maps are fed as the input to the reduce tasks. Thus, the whole framework is involved in scheduling jobs, monitoring them and re-executes the failed jobss.

A cluster is composed of multiple engines. The number of map and reduce tasks is compromised as Map Reduce job which is executed on cluster.Every worker node applies the map function to the local data, and writes the output result to intermediateblob storage. Worker nodes distribute or schedulemap data based on the output keys (produced by the map function), such that all map data belonging to one key is located on the same azure worker node. The worker nodes now process each and every group of output map data, per key, in parallel.

Map Reduce allows for parallel distributed processing of the maps and reduction operation. Provided that each and every mapping operation is self-reliant of the others, all maps can be performed in parallel – though in real scenario this is limited by the number of self-reliant data sources and/or the number of VM's near each source. Similarly, a set of 'reducers' can perform the reduction phase, provided that all data outputs of the map data operation that share the same key are presented to the same reducer at the same time, or we could say that the reduction function is associative. While this method can often appear to be inefficient compared to model that are more sequential, Map Reduce can be applied to significantly larger volume of data than normal servers can handle – a large server farm can use Map Reduce to sort a petabyte of data in only a few hours. The parallelism also provide some possibility of recovering from partial failure of blob storage or server during the operation: if any one mapper or reducer fails, the work can be rescheduled – assuming the input data is still available.

Let us consider a large data application consisting of map and reduce tasks. The Map Reduce job is executed on a cluster. The Map and Reduce functions of Map Reduce are defined with respect to data pattern/structured in (key, value) pairs. Map takes one pair of data with a type in one data format, and returns a list of pairs in a different format. Then it is processed in the reduce phase by the reduce task with the key-value pair along with the same key. Thus, the reduce phase can only begin only after the map phase ends. This large data application must be completed by deadline$\mathbb{T}$. $\mathbb{X}$ and $\mathbb{Y}$ represents the set of tasks of map and reduce of the application. The set of slots available for executing these map and reduce tasks are indicated by S_1 and S_2 respectively. The resource utilization is symbolized by $\mathbb{R}_{st}$, where s is the slot $\in (S_1, S_2)$ and t is the task $\in (\mathbb{X}, \mathbb{Y})$ executed on the respective slot. The processing time of the task t when executed on the slot s is represented as τ_{st}. The dependencies of the map and reduce tasks are characterized by the variable $\Psi_{vt}, \forall v, t \in (\mathbb{X} \cup \mathbb{Y})$, where Ψ_{vt} will possess the value 1 if t is assigned after the task v else 0.

The main objective is to minimize the resource utilization when executing the Map Reduce application based on the dependencies of reduce tasks on the map tasks. The resource utilization Map Reduce scheduling problem is given as:

$$\sum_{s\in S_1}\sum_{t\in\mathbb{X}} \mathbb{R}_{st} P_{st} + \sum_{s\in S_2}\sum_{t\in\mathbb{Y}}\sum_{v\in(\mathbb{X}\cup\mathbb{Y})} \Psi_{vt}\tau_{st}P_{st} \qquad (1)$$

The above equation has to be minimized. Each map task is assigned to a slot for execution. This is given by:

$$\sum_{s\in S_1} P_{st} = 1, \forall t \in \mathbb{X} \qquad (2)$$

The each reduce task is assigned to a task which is represented by:

$$\sum_{s\in S_2}\sum_{v\in(\mathbb{X}\cup\mathbb{Y})} \Psi_{vt}, Q_{st} = 1\ \forall t \in (\mathbb{Y}) \qquad (3)$$

The processing time of the application should not exceed the deadline. Without exceeding the deadline, the scheduler will assign to the reduce tasks only after finishing the map tasks. This is established as:

$$\sum_{t\in\mathbb{X}} \tau_{st}P_{st} + \sum_{t\in\mathbb{Y}}\sum_{v\in(\mathbb{X}\cup\mathbb{Y})} \Psi_{vt}\tau_{st'}P_{st'} \le \mathbb{T}, \forall s \in S_1, \forall s' \in S_2 \qquad (4)$$

Thus, it is interpreted as:

$$max_{\forall s\in S_1}\sum_{t\in\mathbb{X}} \tau_{st}P_{st} + max_{\forall s'\in S_2}\sum_{t\in\mathbb{Y}} \tau_{st'}Q_{st'} \le \mathbb{T} \qquad (5)$$

As a result, all reducetasks can be assigned after time:

$$max_{\forall s\in S_1}\sum_{t\in\mathbb{X}} \tau_{st}P_{st} \qquad (6)$$

The integrity requirements for the decision variables are given by:

$$P_{st} = \{0,1\}, \forall t \in \mathbb{X}, \forall s \in S_1 \qquad (7)$$

$$Q_{st} = \{0,1\}, \forall t \in \mathbb{Y}, \forall s \in S_2 \qquad (8)$$

The resource utilization solution consists of P and Qˆ where,

$$\hat{Q}_{st} = \sum_{v\in(\mathbb{X}\cup\mathbb{Y})} \Psi_{vt}Q_{st}, t \in \mathbb{Y}\ and\ s \in S_2 \qquad (9)$$

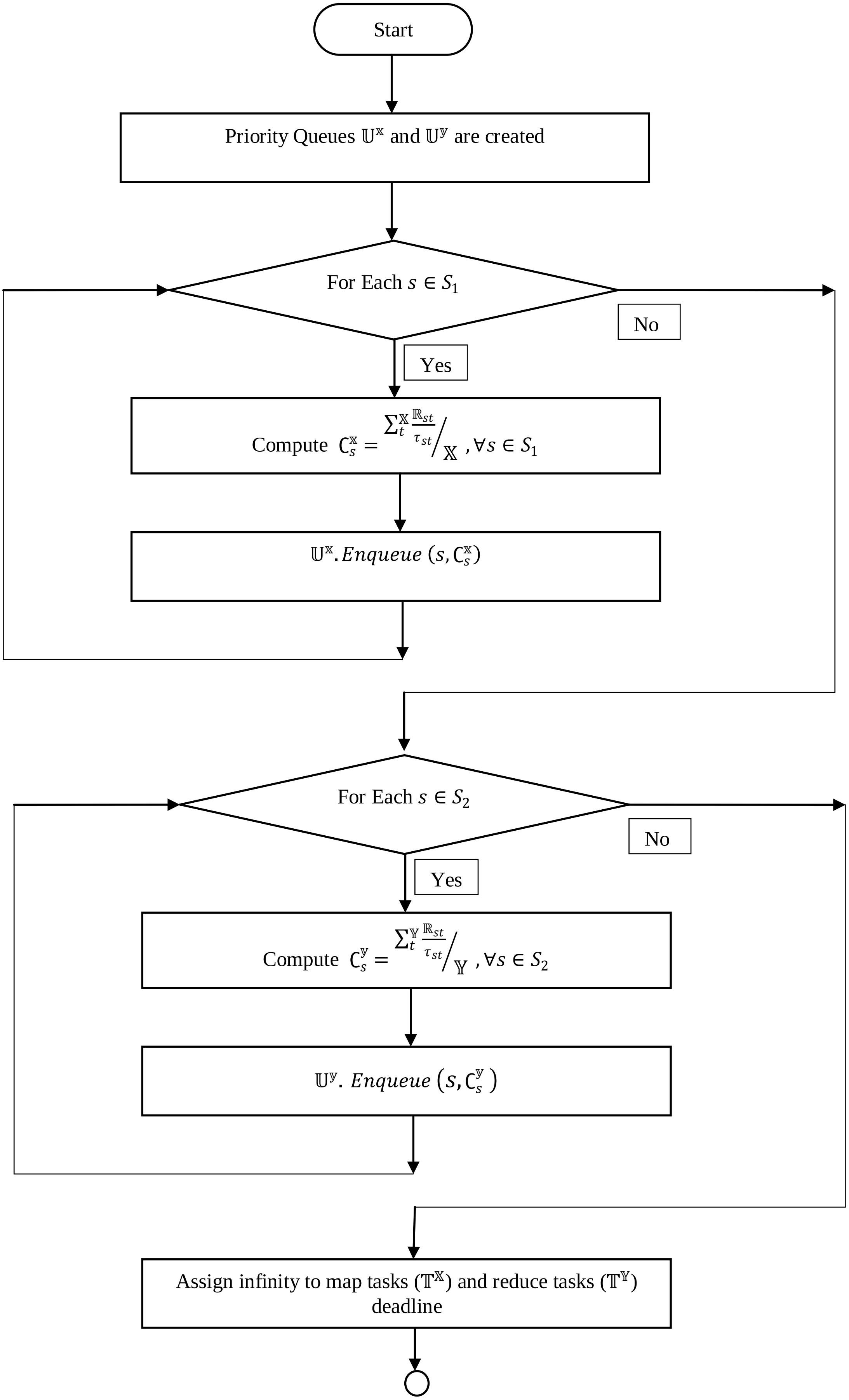
Here we develop the algorithm for resource utilization which is very efficient for scheduling Map Reduce jobs. The deadline T is specified for the completion of the large data application. However, the user here will specify only the deadline of the job but not the map or reduce phase. Reduce tasks are performed only after the completion of map tasks, thus reduce tasks are completely dependent on the map tasks. Therefore, the data centre should define the deadline for map tasks based on the availability of map slots so that further tasks are carried out by reduce tasks in order to utilize the resource efficiently. Once the map tasks are done with its tasks based on the map slots, the assignments of the reduce tasks are performed based on its reduce slots meeting its deadline. Thus, the design of this proposed algorithm characterizes the resource utilization. Therefore, the resource utilization rate of the slot s is given by:

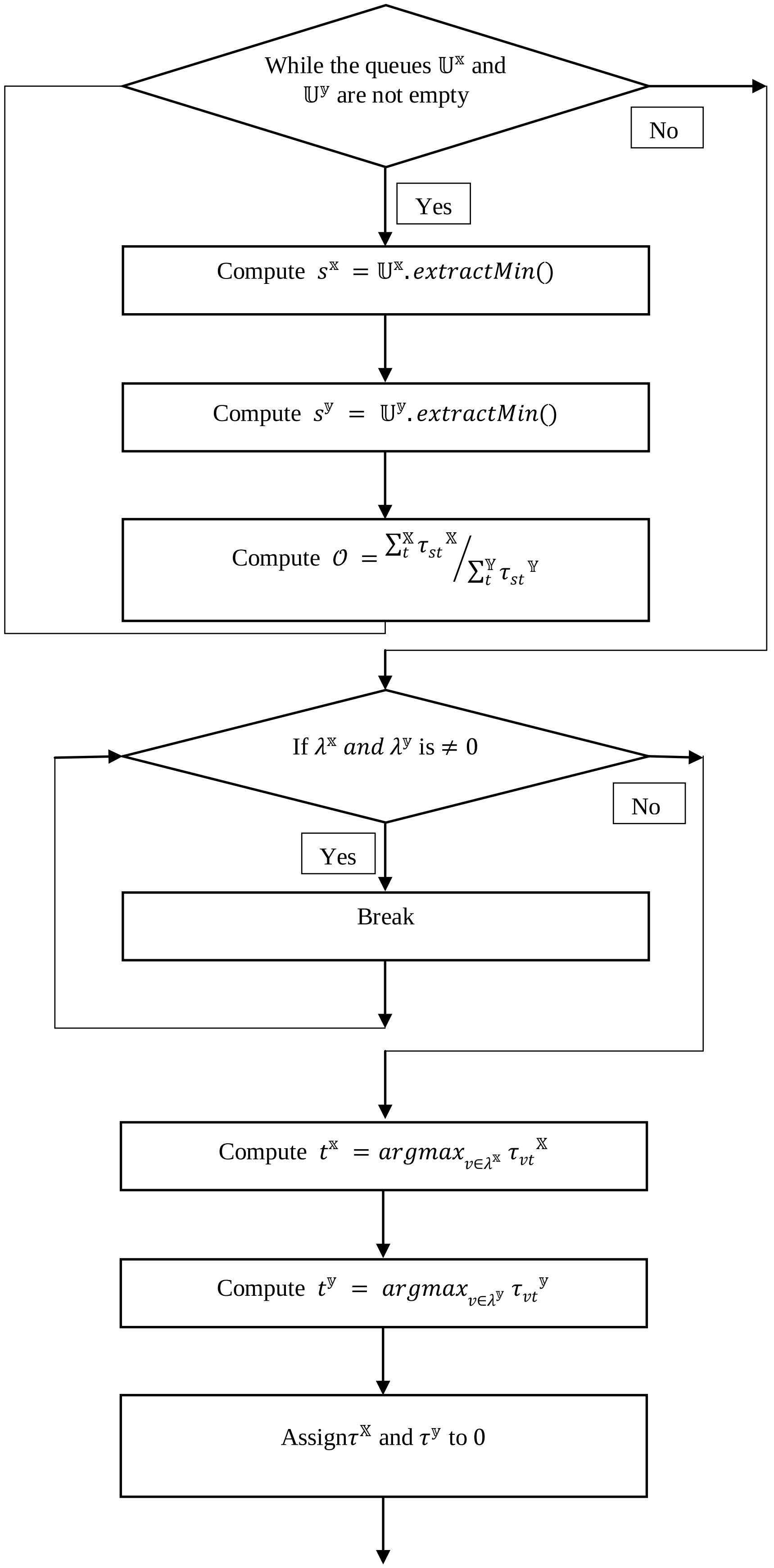
$$\mathbb{C}_s^{\mathbb{x}} = {}^{\sum_t^{\mathbb{X}} \frac{\mathbb{R}_{st}}{\tau_{st}}}\big/_{\mathbb{X}}, \forall s \in S_1 \qquad (10)$$

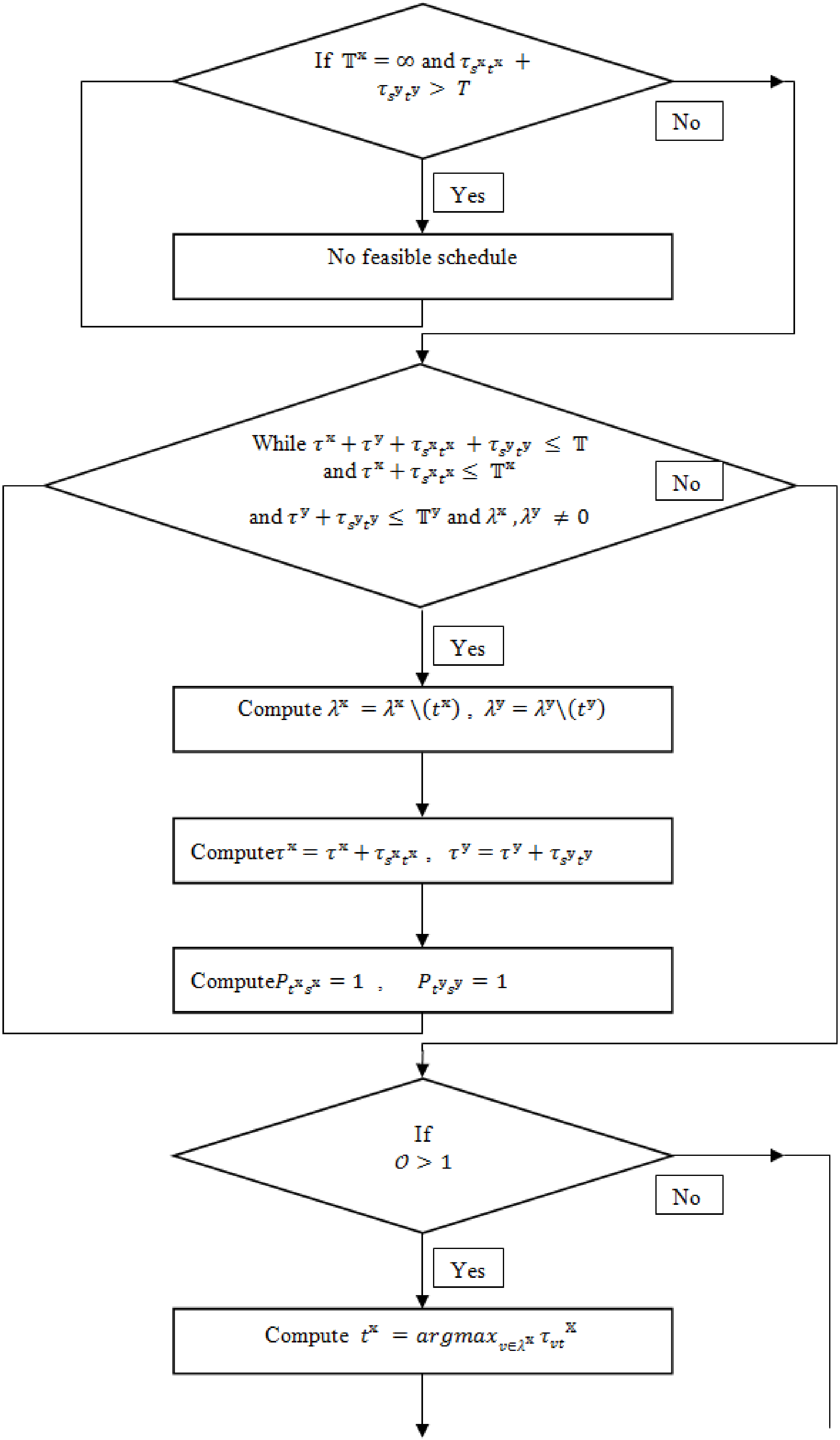
$$\mathbb{C}_s^{\mathbb{y}} = {}^{\sum_t^{\mathbb{Y}} \frac{\mathbb{R}_{st}}{\tau_{st}}}\big/_{\mathbb{Y}}, \forall s \in S_2 \qquad (11)$$

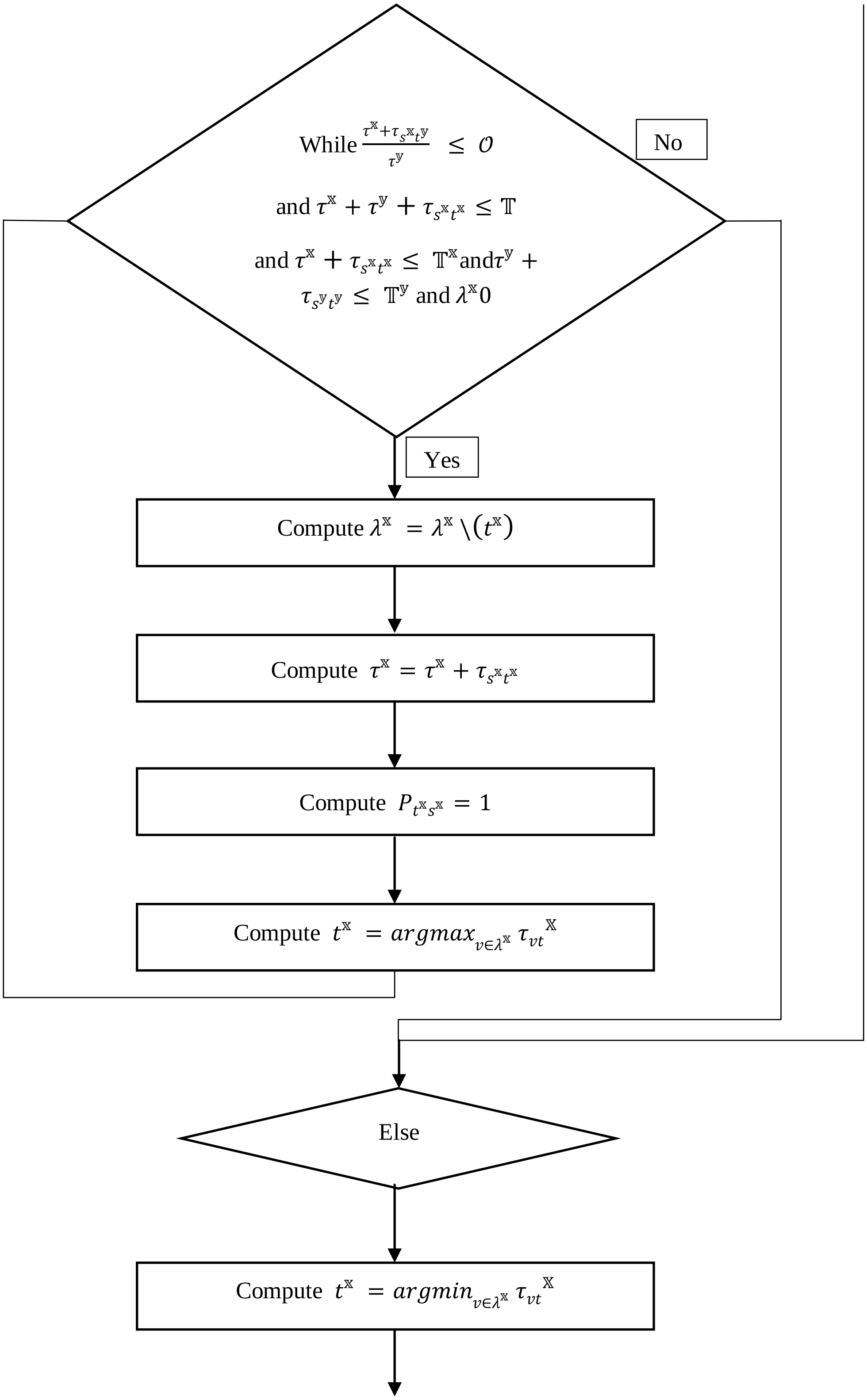
where, it represents the resource utilization rate of map slot s and reduce slot s respectively. The lower $\mathbb{C}_s^{\mathbb{x}}$ represents a higher priority for the slot s to which a task is assigned. There exists two priority queues $\mathbb{U}^{\mathbb{x}}, \mathbb{U}^{\mathbb{y}}$to keepthe order of the map and reduce slots based on their energyconsumption rates. Our proposed algorithm initializes the deadline for map tasks ($\mathbb{T}^{\mathbb{X}}$) and reduce tasks ($\mathbb{T}^{\mathbb{Y}}$) to infinity.

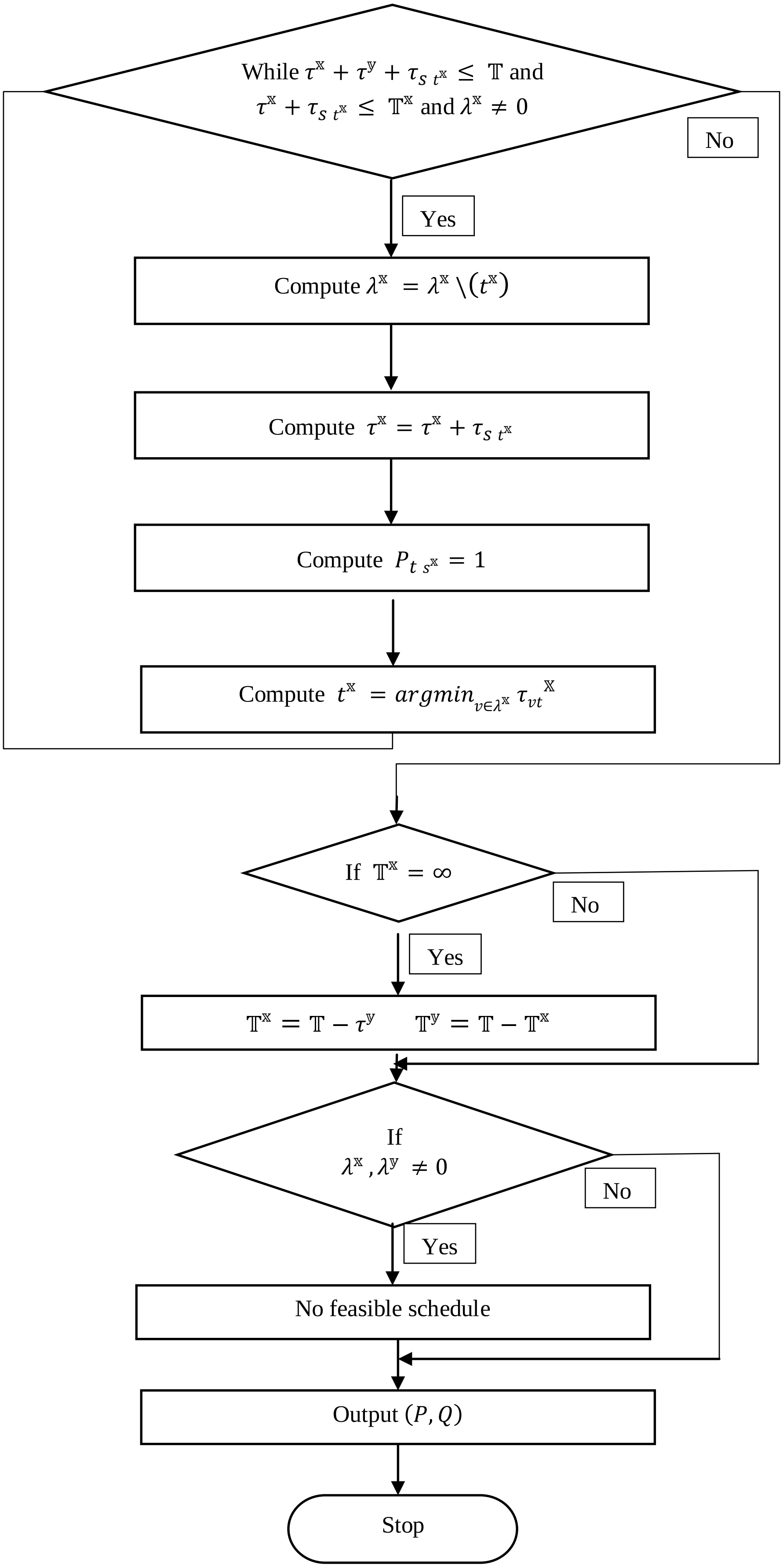
The complete algorithm is given below.


Start
Priority Queues $\mathbb{U}^{\mathbb{x}}$ and $\mathbb{U}^{\mathbb{y}}$ are created
For Each $s \in S_1$
No
Yes
Compute $\mathbb{C}_s^{\mathbb{x}} = \sum_t^{\mathbb{X}} \frac{\mathbb{R}_{st}}{\tau_{st}} / \mathbb{X}$, $\forall s \in S_1$
$\mathbb{U}^{\mathbb{x}}.Enqueue\ (s, \mathbb{C}_s^{\mathbb{x}})$
For Each $s \in S_2$
No
Yes
Compute $\mathbb{C}_s^{\mathbb{y}} = \sum_t^{\mathbb{Y}} \frac{\mathbb{R}_{st}}{\tau_{st}} / \mathbb{Y}$, $\forall s \in S_2$
$\mathbb{U}^{\mathbb{y}}.\ Enqueue\ (s, \mathbb{C}_s^{\mathbb{y}})$
Assign infinity to map tasks ($\mathbb{T}^{\mathbb{X}}$) and reduce tasks ($\mathbb{T}^{\mathbb{Y}}$) deadline


While the queues $\mathbb{U}^{\mathbb{x}}$ and $\mathbb{U}^{\mathbb{y}}$ are not empty
No
Yes
Compute $s^{\mathbb{x}} = \mathbb{U}^{\mathbb{x}}.extractMin()$
Compute $s^{\mathbb{y}} = \mathbb{U}^{\mathbb{y}}.extractMin()$
Compute $\mathcal{O} = \sum_t^{\mathbb{X}} \tau_{st}{}^{\mathbb{X}} / \sum_t^{\mathbb{Y}} \tau_{st}{}^{\mathbb{Y}}$
If $\lambda^{\mathbb{x}}$ *and* $\lambda^{\mathbb{y}}$ is $\neq 0$
No
Yes
Break
Compute $t^{\mathbb{x}} = argmax_{v \in \lambda^{\mathbb{x}}} \tau_{vt}{}^{\mathbb{X}}$
Compute $t^{\mathbb{y}} = argmax_{v \in \lambda^{\mathbb{y}}} \tau_{vt}{}^{\mathbb{y}}$
Assign$\tau^{\mathbb{X}}$ and $\tau^{\mathbb{y}}$ to 0


If $\mathbb{T}^x = \infty$ and $\tau_{s^x t^x}$ + $\tau_{s^y t^y} > T$
No
Yes
No feasible schedule
While $\tau^x + \tau^y + \tau_{s^x t^x} + \tau_{s^y t^y} \leq \mathbb{T}$ and $\tau^x + \tau_{s^x t^x} \leq \mathbb{T}^x$ and $\tau^y + \tau_{s^y t^y} \leq \mathbb{T}^y$ and $\lambda^x, \lambda^y \neq 0$
No
Yes
Compute $\lambda^x = \lambda^x \setminus (t^x)$, $\lambda^y = \lambda^y \setminus (t^y)$
Compute$\tau^x = \tau^x + \tau_{s^x t^x}$, $\tau^y = \tau^y + \tau_{s^y t^y}$
Compute$P_{t^x s^x} = 1$, $P_{t^y s^y} = 1$
If $O > 1$
No
Yes
Compute $t^x = argmax_{v \in \lambda^x} \tau_{vt}{}^x$


While $\frac{\tau^{\mathbb{x}}+\tau_{s^{\mathbb{x}}t^{\mathbb{y}}}}{\tau^{\mathbb{y}}} \leq \mathcal{O}$
and $\tau^{\mathbb{x}} + \tau^{\mathbb{y}} + \tau_{s^{\mathbb{x}}t^{\mathbb{x}}} \leq \mathbb{T}$
and $\tau^{\mathbb{x}} + \tau_{s^{\mathbb{x}}t^{\mathbb{x}}} \leq \mathbb{T}^{\mathbb{x}}and\tau^{\mathbb{y}} +$
$\tau_{s^{\mathbb{y}}t^{\mathbb{y}}} \leq \mathbb{T}^{\mathbb{y}}$ and $\lambda^{\mathbb{x}}0$
No
Yes
Compute $\lambda^{\mathbb{x}} = \lambda^{\mathbb{x}} \setminus (t^{\mathbb{x}})$
Compute $\tau^{\mathbb{x}} = \tau^{\mathbb{x}} + \tau_{s^{\mathbb{x}}t^{\mathbb{x}}}$
Compute $P_{t^{\mathbb{x}}s^{\mathbb{x}}} = 1$
Compute $t^{\mathbb{x}} = argmax_{v\in\lambda^{\mathbb{x}}} \tau_{vt}{}^{\mathbb{X}}$
Else
Compute $t^{\mathbb{x}} = argmin_{v\in\lambda^{\mathbb{x}}} \tau_{vt}{}^{\mathbb{X}}$


While $\tau^{\mathbb{x}} + \tau^{\mathbb{y}} + \tau_{s\,t^{\mathbb{x}}} \leq \mathbb{T}$ and $\tau^{\mathbb{x}} + \tau_{s\,t^{\mathbb{x}}} \leq \mathbb{T}^{\mathbb{x}}$ and $\lambda^{\mathbb{x}} \neq 0$
No
Yes
Compute $\lambda^{\mathbb{x}} = \lambda^{\mathbb{x}} \setminus (t^{\mathbb{x}})$
Compute $\tau^{\mathbb{x}} = \tau^{\mathbb{x}} + \tau_{s\,t^{\mathbb{x}}}$
Compute $P_{t\,s^{\mathbb{x}}} = 1$
Compute $t^{\mathbb{x}} = argmin_{v \in \lambda^{\mathbb{x}}} \tau_{vt}{}^{\mathbb{X}}$
If $\mathbb{T}^{\mathbb{x}} = \infty$
No
Yes
$\mathbb{T}^{\mathbb{x}} = \mathbb{T} - \tau^{\mathbb{y}}$ $\mathbb{T}^{\mathbb{y}} = \mathbb{T} - \mathbb{T}^{\mathbb{x}}$
If $\lambda^{\mathbb{x}}, \lambda^{\mathbb{y}} \neq 0$
No
Yes
No feasible schedule
Output (P, Q)
Stop

In every iteration, the algorithm chooses the slots with lowest utilization of resource from the priority queues. For these slots, the ratio of processing timeof map tasks to that of the reduce tasks, denoted by $\mathcal{O}$, is calculated. This ratio is used in the task assignmentprocess in each iteration of the algorithm. Then, algorithm sorts the unassigned map and reduce tasks based on theirprocessing time on the selected slots. It selectsthe longest map task$t^{\mathbb{x}}$ and reduce task $t^{\mathbb{y}}$ from the sortedsets $\lambda^{\mathbb{x}}$ and $\lambda^{\mathbb{y}}$ respectively. Then it checksthe feasibility of allocating map task$t^{\mathbb{x}}$ to slot$s^{\mathbb{x}}$ andreduce task $t^{\mathbb{y}}$ to slot $s^{\mathbb{y}}$ by checking the total processingtime of the tasks against the deadline$\mathbb{T}$. If theassignment of map task $t^{\mathbb{x}}$ and reduce task $t^{\mathbb{y}}$ is feasible, the algorithm continues to select tasks from$\lambda^{\mathbb{x}}$and$\lambda^{\mathbb{y}}$, and updates the variables accordingly. To keep the assignments of the tasks in alignment withthe ratio of processing time $\mathcal{O}$, the algorithm balances theassignment. In doing so, if$\mathcal{O} > 1$ (i.e., the load of processingtime of map tasks is greater than that of reduce tasks) andthe ratio of the current assignment is less than $\mathcal{O}$, then thealgorithm assigns more map tasks to balance the allocatedprocessing time close to $\mathcal{O}$. If the ratio of thecurrent assignment is greater than $\mathcal{O}$, the algorithm assignsmore reduce tasks to balance the allocated processing time. After allocating the map and reduce tasks withthe largest processing time, the algorithm assigns small mapand reduce tasks while satisfying the deadline. At the end of the first iteration, the algorithm sets the mapand reduce deadlines based on the allocated tasks. The time complexity of our algorithm is polynomial in thenumber of map slots, the number of reduce slots, the numberof map tasks, and the number of reduce tasks, respectively.

IV. Result

Cloud provide data iterative map reduce as a infrastructure as a service which is modified and executed here. The modified data iterative protocol is used to compute data in azure cloud, which provides the better resources utilization and more importantly provides better scheduling and efficiency. The system model presented has been developed on Visual Studio 2010 framework 4.0 with C#. The overall system has been developed and implemented with Microsoft Azure platform. We have used virtual machine type small with collocated caching. The virtual machine configurations are as follow it uses windows 2008 r2 server, 2.72 GHz with 4 cores with 1.5GB memory.

The developed system has been analyzed for different performance parameters like map resource utilization, Resource utilization based on our proposed model scheme compared with the existing Hadoop model. The relative study for these all factors has been performed. This system or model performance has been verified for various map size, file size with dynamic scheduling as well as performance parameters have been checked for its fault tolerant, robustness justification. The following are the performance analysis of our proposed model over Hadoop.

a) Map Resource Utilization

The map resource utilization of Hadoop and our proposed model is been plotted in the above graph. We have considered a maximum of 8 maps.Here we have taken the execution time by varying the map size and the analytical result proves that the proposed resource utilization time is reduced by35 secfrom 56 secapproximately over Hadoop.

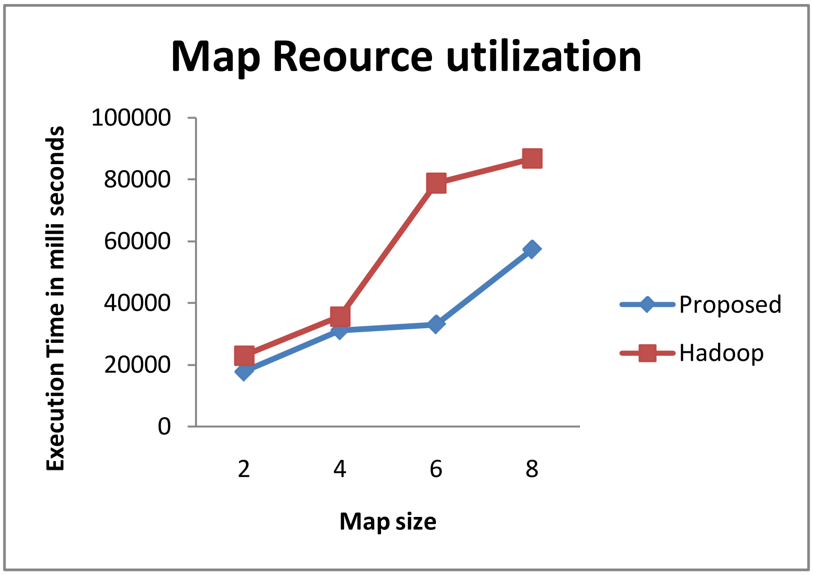


Figure 1 : Map resource utilization

b) Resource utilization

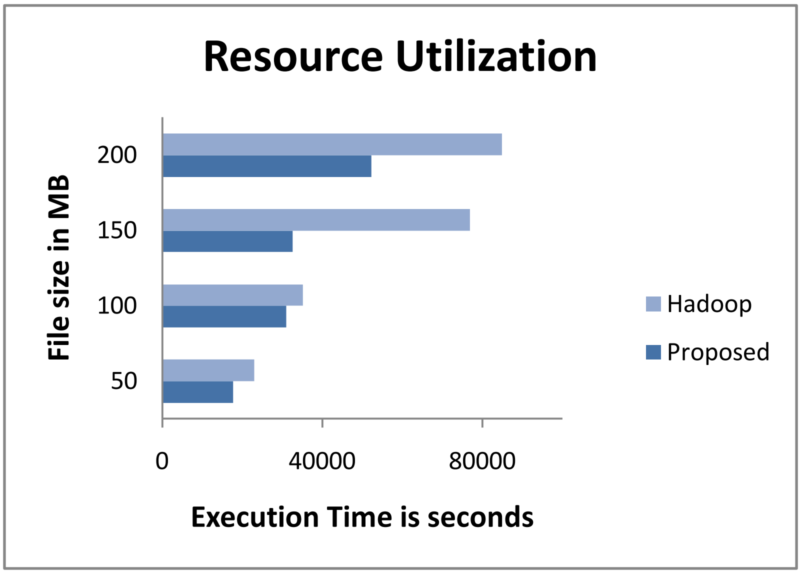


Figure 2 : Map resource utilization

The resource utilization of Hadoop and our proposed model is been plotted in the above graph. We have considered a maximum of 200MB file.Here we have taken the execution time by varying the file size (50, 100, 150, and 200 respectively) and the analytical result proves that the proposed resource utilization time is reduced by33 secfrom 55 secapproximately over Hadoop.

V. Conclusion

Our efficient cloud model provides Map Reduce data intensive computing runtimes for the Microsoft windows azure cloud environment. Our model provides a decentralized iterative expansion to Map Reduce computing environment, enabling the users to easily and efficiently perform task for large scale iterative data analysis/computations on Azure cloud environment. Our model utilizes a BSP scheduling mechanism based on Azure Tables and Queues to provide the caching of static data across iterations in data iterative computations. Our model cloud infrastructure services effectively to deliver robust and efficient applications.
Here we compared the resource utilization and execution time of our proposed model over Hadoop 2.4.0.2.1.3.0-1981. He we analyzed the performance of our model over Hadoop by increasing map size (varying 2, 4, 6, 8 respectively), file size (varying 50Mb, 100Mb, 150Mb, 200Mb respectively) and reduce size by (1, 2, 3, 4) and found that our proposed model is robust and efficient. We also found that by increasing the instance or the number of cores the performance is getting better. We also found how usage collocated caching improves the task execution time.

In future we would like to test this model on different domain type such as data mining, medical research etc… We would also further like to enhance the model by creating a dedicated cache for cache worker which will further improve the performance of our system.

References Références Referencias

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Dept. EECS, California Univ., Berkeley, Tech. Rep. UCB/EECS-2009-28, Feb. 2009.
2. M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Comput. vol. 13, no. 5, pp. 10–13, Sep. 2009.
3. 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 Gener. Comput. Syst., vol. 25, no. 6, pp. 599–616, Jun. 2009.
4. (2013) Apache Hadoop Project. [Online]. Available: http://hadoop.apache.org
5. K. V. Vishwanath and N. Nagappan, "Characterizing Cloud Computing Hardware Reliability," in Proc. ACM Symp. Cloud Computing, Jun. 2010, pp. 193–204.
6. B. Schroeder and G. A. Gibson, "Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You?" in Proc. 5th USENIX Conf. File and Storage Technologies, Feb. 2007, pp. 1–16.
7. F. Wang, J. Qiu, J. Yang, B. Dong, X. Li, and Y. Li, "Hadoop High Availability through Metadata

Replication," in Proc. 1st Int. Workshop Cloud Data Manage., 2009, pp. 37–44.

8. W. Li, Y. Yang, J. Chen, and D. Yuan, "A Cost-Effective Mechanism for Cloud Data Reliability Management Based on Proactive Replica Checking," in Proc. 2012 12th IEEE/ACM Int. Symp. Cluster, Cloud and Grid Computing (CCGrid), May 2012, pp. 564–571.
9. C. N. Reddy, "A CIM (Common Information Model) Based Management Model for Clouds," in Proc. 2012 IEEE Int. Conf. Cloud Computing in Emerging Markets (CCEM), Oct. 2012, pp. 1–5.
10. (2013) Amazon EC2. [Online]. Available: http://aws.amazon.com/ec2
11. R. T. Kaushik, M. Bhandarkar, and K. Nahrstedt, "Evaluation and analysis of greenhdfs: A self-adaptive, energy-conserving variant of the Hadoop distributed file system," in Proc. of the 2nd IEEE International Conf. on Cloud Computing Technology and Science, 2010, pp. 274–287.
12. B. Moseley, A. Dasgupta, R. Kumar, and T. Sarlos, "On scheduling in map-reduce and flow-shops," in Proc. Of the 23rd Annual ACM Symposium on Parallelism in Algorithms and Architectures, 2011, pp. 289–298.
13. L. Mashayekhy, M. M. Nejad, and D. Grosu, "A truthful approximation mechanism for autonomic virtual machine provisioning and allocation in clouds," in Proc. of the ACM Cloud and Autonomic Computing Conf., 2013, pp. 1–10.
14. M. M. Nejad, L. Mashayekhy, and D. Grosu, "A family of truthful greedy mechanisms for dynamic virtual machine provisioning and allocation in clouds," in Proc. of the 6th IEEE Intl. Conf. on Cloud Computing, 2013, pp. 188–195.
15. B. Palanisamy, A. Singh, and L. Liu, "Cost-effective resource provisioning for mapreduce in a cloud," IEEE Transactions on Parallel and Distributed Systems (forthcoming), 2014.
16. T. J. Hacker and K. Mahadik, "Flexible resource allocation for reliable virtual cluster computing systems," in Proc. ACM Conf. High Perf. Comp., Networking, Storage and Analysis, 2011, p. 48.
17. T. Sandholm and K. Lai, "Mapreduce optimization using regulated dynamic prioritization," in Proc. 11th ACM Int'l Conf. on Measurement and Modeling of Computer Syst., 2009, pp. 299–310.
18. X. Wang, D. Shen, G. Yu, T. Nie, and Y. Kou, "A throughput driven task scheduler for improving mapreduce performance in job-intensive environments," in Proc. of the 2nd IEEE International
19. Congress on Big Data, 2013, pp. 211–218.
20. Z. Ren, X. Xu, M. Zhou, J. Wan, and W. Shi, "Workload analysis, implications and optimization on a production hadoop cluster: A case study on taobao," IEEE Transactions on Services Computing, vol. 7, no. 2, pp. 307–321, 2014.
21. M. Pastorelli, A. Barbuzzi, D. Carra, M. Dell' Amico, and P. Michiardi, "Hfsp: size-based scheduling for Hadoop," in Proc. of IEEE International Conference on Big Data, 2013, pp. 51–59.
22. H. Chang, M. S. Kodialam, R. R. Kompella, T. V. Lakshman, M. Lee, and S. Mukherjee, "Scheduling in mapreduce-like systems for fast completion time," in Proc. of the 30th IEEE International Conference on Computer Communications, 2011, pp. 3074–3082.
23. Changjian Wang; Yuxing Peng; Junyi Liu; Mingxing Tang; Guangming Liu; Jinghua Feng; Pengfei You, "Optimal Task Scheduling in Map Reduce," Networking, Architecture, and Storage (NAS), 2014 9th IEEE International Conference on , vol., no., pp.118,122, 6-8 Aug. 2014
24. Qi Chen; Cheng Liu; Zhen Xiao, "Improving Map Reduce Performance Using Smart Speculative Execution Strategy," Computers, IEEE Transactions on, vol.63, no.4, pp.954,967, April 2014doi: 10.1109/TC.2013.15
25. Yang Wang; Wei Shi, "Budget-Driven Scheduling Algorithms for Batches of Map Reduce Jobs in Heterogeneous Clouds," Cloud Computing, IEEE Transactions on , vol.2, no.3, pp.306,319, July-Sept. 1 2014doi: 10.1109/TCC.2014.2316812
26. Amrit Pal, Sanjay Agrawal, "An Experimental Approach Towards Big Data for Analyzing Memory Utilization on a Hadoop cluster using HDFS and MapReduce".
27. Fan Yuanquan, WU Weiguo, XU Yunlong, CHEN Heng "Improving Map Reduce Performance by Balancing Skewed Loads".

Global Journals Inc. (US) Guidelines Handbook 2015

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.

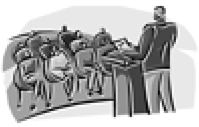
- The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

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.

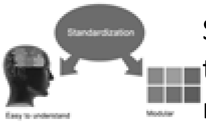


You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

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)

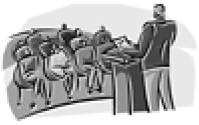
Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

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%.



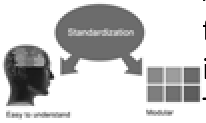
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

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.

Global RESEARCH RADIO

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.

The Administration Rules

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

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

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

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	C-D	E-F
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

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