ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Enhancing Cloud Computing Trust using TBLC Algorithm

Er. Sunita Rani

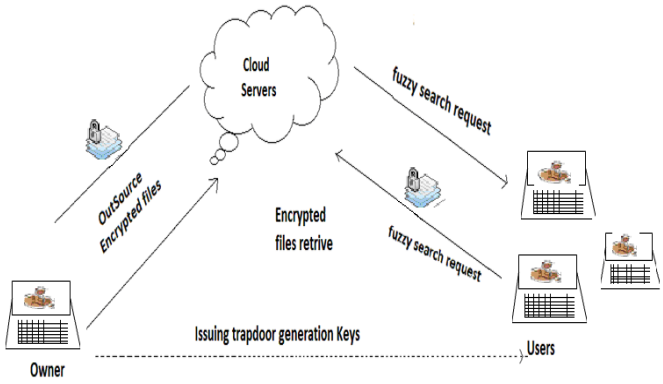
A.P & COD, Department of CSE, Universal Institute of Engineering & Technology, Lalru, India

ABSTRACT: Cloud computing brings a lot of challenges and is in fact advancement of on demand online services where users can remotely store their data into the cloud infrastructure. But protection of data and to maintain trust between clients and cloud service provider remains an issue. Therefore, trust confidence between cloud user and cloud service provider must be improved. In order to introduce Third party auditor for increasing the trust between CU and CSP following things are required: 1) TPA must be efficient enough to verify the cloud user as it is genuine or not and also reducing the burden of cloud user on verification.
2) Time parameters must be more enough to satisfy the time constraints, no. of file blocks must be of dynamic nature and TPA must be aware of the number of file blocks at run time. The proposed algorithm helps to enhance the trust between CU and CSP as well as enhancing the number of file blocks by make them dynamic and increasing the size of file blocks that are requested at a time, server computation time, TPA computation time as these are very critical points in order to use cloud services in appropriate and correct way.

KEYWORDS: Virtualization, TPA, Cloud Security, Trust, Virtual Machine**, CU, CSP**

I. THORETICAL FOUNDATION AND INTRODUCTION TO SUBJECT

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds services are used over the internet and it tries to masquerade complexity for clients. [8]. During the past few years, cloud computing services has been growing from being a capable. IT organizations have expresses their concern about crucial issues (such as security) that is the major issue while using cloud based services. These kind of issues derived from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location.[8] Generally, Cloud computing has several customers such as ordinary customers, academic circles, and enterprises who have different motivation to move to cloud. If cloud clients are academic circles then security will effect on the performance of computations and for them cloud providers have to find a way to combine security and performance.



[6] Figure 1 Architecture of cloud data utilization service

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

The issue of cloud security is keeping many IT managers from fully embracing the cloud—even with large potential savings in infrastructure costs and improved business flexibility. With Gartner's point of view an acceleration of cloud based services in the organization; there is a need to find out how IT professionals are addressing the challenges of cloud based services, especially the issue on security as data is handled remotely.
Virtualization is becoming the new norm for organizations data center. This technology is very much helpful for using the cloud services. If cloud based services are on high priority for your agenda the you are almost certainly assumed a way to improve server utilization, improve efficiencies in the cloud based data center, improve scaling, effectiveness etc. to an enterprise.

The virtualized data center is the first step and the foundation for implementing a cloud environment. Along with the promise of significant benefits, the cloud also places greater demands on the data center. IT managers are seeing increases in virtual machine (VM) density per server and running into bottlenecks with existing storage and networking based services. As a effect, it has the capability to greater capacity demands, increased complexity, and more and more massive interconnections. Although this setup may work for a while, IT managers are finding that it doesn't scale—reducing the flexibility and efficiency benefits associated with cloud environments.

II. RELATED WORK

[1]Cong Wang et al. in 2010 has proposed public auditability with achieving economy of scale for the environment of cloud computing platform. They presented public auditing scheme for security on database of cloud computing platform. They discussed two types of paradigms for the purpose of public auditing system and data security as well as showing how to extent their in order to support batch auditing system for TPA upon delegations from multiusers.
[2] Alok Tripathi, Abhinav Mishra in 2010 provides the details of security issues that occur in an environment of CSP that is cloud service provider. They has paid attention on technical database security issues that arises from the usage of cloud computing services and also provided an overview of security issues that are related to cloud computing with the view of a secure cloud architecture environment.
[7] I-Hsun Chauang et al. in 2011 proposed an effective Privacy Protection Scheme to provide the suitable privacy protection which is satisfying the user-demand privacy requirement and maintaining system performance concurrently. So for achieving their scheme they analyze the requirement for privacy level users and quantify security degree and performance those algorithms that provides encryption scheme and after that a suitable security composition is derived by the results of analysis and quantified data as well as showing simulation results that shows that their proposed scheme is not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments.
[9] Qian wang et al. in 2011 proposed a paradigm for the problem of ensuring the integrity of data storage in the platform of Cloud Computing in which they considered the task of allowing a third party auditor (TPA) on the behalf of cloud user for verifying the integrity of the dynamic data stored in the cloud that eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indubitably intact, which may be vital in achieving economy of scale for the platform of Cloud Computing. So for supporting proficient supervision of multiple auditing tasks as well as they explored the technique of bilinear aggregate signature in order to extend their main result into a multi-user setting, where a number of auditing tasks can be performed concurrently by TPA.

III. CHARACTERISTICS OF CLOUD COMPUTING [14]

1. Very large-scale: The scale of cloud is too large. The cloud of Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, have more than thousands of thousands servers. There are hundreds of thousands of servers in an enterprise.
2. On demand service: Cloud is a large resource pool where resources can be purchased according to the requirement. cloud is just like facility of water, electricity, and gas that is charged based on the amount used by the customer as per their requirements.
3. Virtuality: Cloud computing makes user to get service anywhere, through any kind of terminal. Everything can be completed through net service using a PC or a mobile. Users can get or share these services securely anytime, anywhere over the internet. Users can complete a task that can't be completed in a single computer.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

4. Extremely inexpensive: The centered management of cloud make an organization need not to undertake the management cost of data center that is raising very fastly. The flexibility can increase the utilization rate of the available resources as compare to traditional system, so clients can fully enjoy the low cost advantage by using cloud services.

5 High reliability: Cloud uses data multi transcript fault tolerant and ensures the high reliability of the cloud service. Cloud computing is more reliable than local computer.

6 Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

7. High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.[14]

IV. CLOUD COMPUTING DEPLOYMENT MODELS

As cloud computing provide pay as per requirement and use, the amount of database security is intended for adhering to enterprise standards and legislations among cloud users. The structure based on cloud computing can be categorized into following types of clouds: [10]

1) **Private cloud:** The cloud infrastructure is operated for an organization. It is not available to general public. It may be organized or controlled either by that organization which is using this or by the third party.
2) **Public Cloud:** it is available for general public for use. The consumers have to pay for the services which are consumed by them or some services are also free. It is managed by the organization which is providing cloud services.
3) **Community Cloud:** In this type of cloud several organizations share the cloud infrastructure like polices or security requirements etc.
4) **Hybrid Cloud:** This is the mixture of two or more clouds i.e. public or private or community that is bound together by some standardized technology

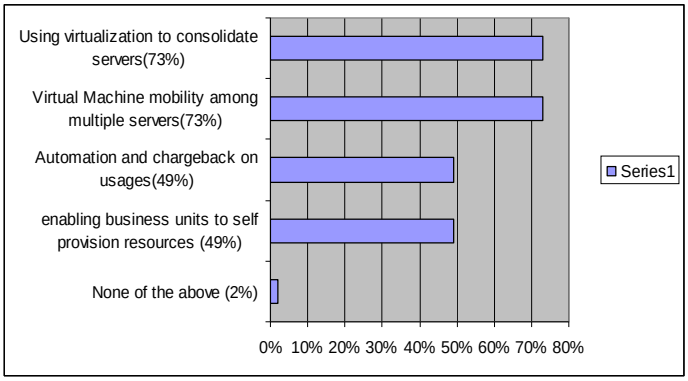


Figure 2: Percentage of cloud environment

Developers had asked IT professionals to tell what technologies they were currently using that support a cloud environment. Most of them are interested in virtualization to consolidate servers and enabling virtual machine (VM) mobility across multiple servers (73 percent) in order to support a cloud based services.

V. CLOUD SECURITY REQUIEREMENT

When it comes to aspect of developing a software, issue of security arises – it is possible by pushing the past operational view of security that can be start to build software systems that can stand up under attack. Security threats must be treated like software threats and managed by making a part of the development process as the error that causes a system failure today that could be demoralized by an intruder in future.In coincidence with consortiums like SAFE Code and BSIMM, different companies such as Microsoft, Adobe and Cisco have taken the lead to establish secure code development initiatives that inject a set of security deliverables into each phase of the software development process.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

The need to consider security and privacy "at user end" is a basic aspect of secure system development process. The accurate point to define faith in privacy requirements for a software project is during the initial planning stages. So there is requirement to identify key problems and deliverables, and allows the incorporation of security and privacy in a way that is helpful to reduce any problem in the database for planning and scheduling.

VI. PROBLEM FORMULATION

In recent times of economic conflict and internet cloud based burst of services has given birth to new models to doing business and new types threats which include abuse and nefarious use of cloud computing, malicious insider issues, shared resources problems, data loss & leakage issues etc. Various solutions have framed and implemented to secure the trust of various cloud users and cloud service providers by using third party arbitration etc.

However there is no framework where business continually is supported by traceability, verifiability and publically accountability with efficiency in computational time in executing continues auditing the cloud based service.
So the auditing and security schema must provide a mechanism that makes both the parties Cloud Service Provider and Cloud user traceable, verifiable and publically auditable. To achieve this a lot of message protocol has been developed and is already implementation by various cloud based project managers. Most of these are automatic software, algorithms that are working together to make things securely and safely. However, there is very less being work done on enforcing certain policies that are sometimes ignored or exploited due to mismanagement of these algorithms which interact or are part of human interface,

So computational requirements increases as more and more round tips of audit as well as security tips are required to run such type of algorithms. Therefore we need to find paths and dummy process that can removed or appended from these kinds of processes but still it provides higher level of security and auditability with less overhead of the cloud service provider and cloud user thereby, increasing the trust between all the parties and stack holder.
In order to enhance the trust of various cloud users and cloud service providers by using third party arbitration etc, there is need of auditing and security scheme that must provide a mechanism that makes both the parties Cloud Service Provider and Cloud user traceable, verifiable and publically auditable..
So my research paper has the following objectives:

1) To develop a public auditing system that uses TPA i.e. third party auditor in order to provide privacy preserving system as well as security protocol that verifies the correctness of on demand data without retrieving the actual data content.
2) To enhance and scalable the public auditing in the cloud computing which cost minimum resources and time.
3) To enhance the batch auditing system as compare to previous scheme by increasing the batch audits or sampled blocks.

VII. METHODOLOGY

The requirement of high degree of confidence and transparency is needed by which cloud providers can keep user data protected so that cloud users heavily rely on web browsers. The privacy and security of cloud computing depends on whether the cloud service provider has implemented security policies or security controls required by the users. Protecting privacy in cloud providers is a technical challenge. In cloud environment, this challenge is complicated by distributed nature of clouds and lack of subscriber knowledge over where the data is stored i.e. about data center and accessibility of the users.When an organization subscribes to a cloud then all the data that is processed will reside in the premises owned and operated by a provider. But here the issue is that whether a subscriber can obtain assurance that a cloud provider is implementing or generating this information in secure manner.

Algorithm for proposed auditing framework (TBLC):
After applying the TBLC algorithm we get the improved results of CSP , Server Computational Time , No. of file Blocks etc which is wholly dependent on various time analysis process. Here, we get the improved results for various parameters.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

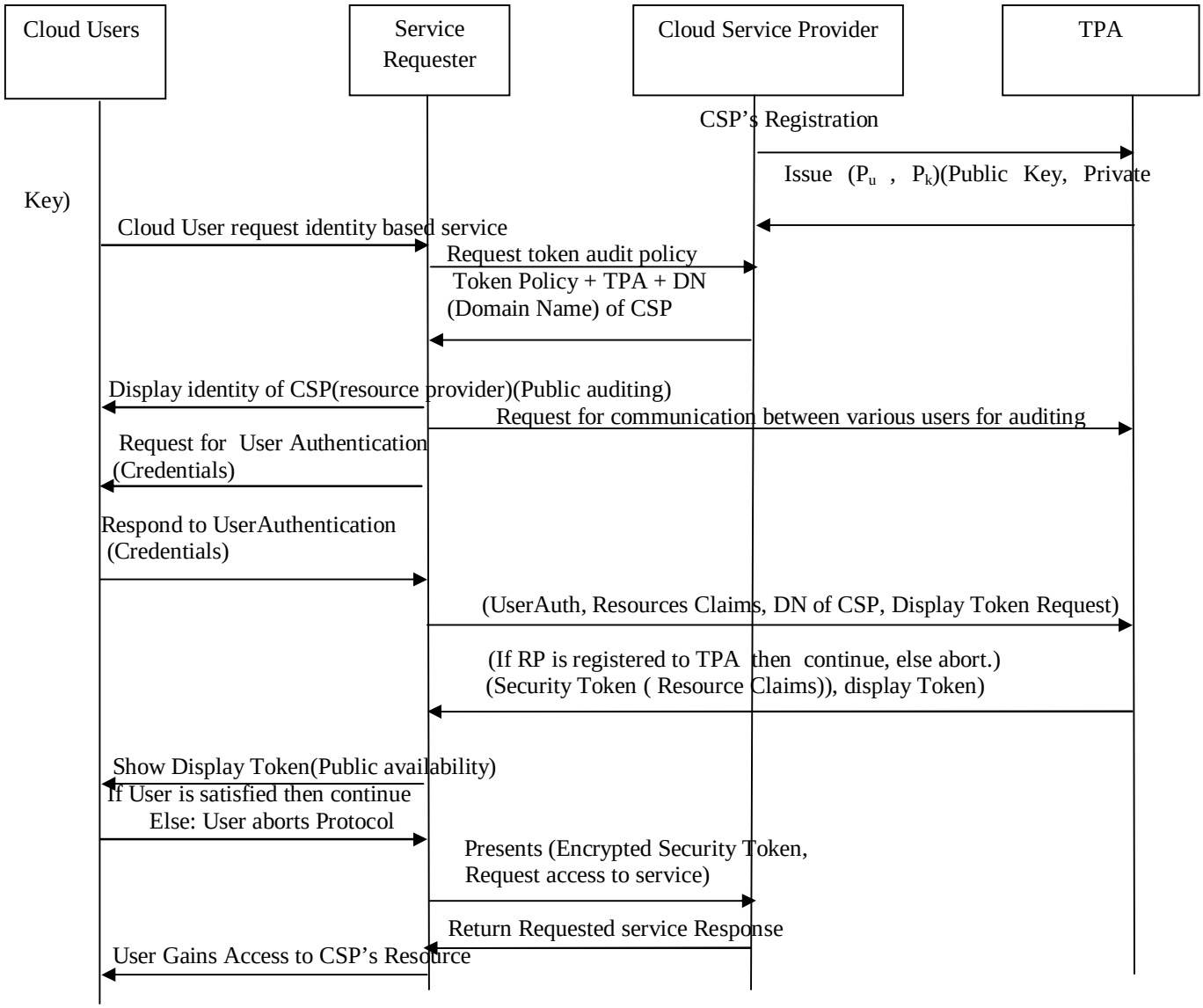


Figure 3 Proposed framework or methodology (TBLC)

Steps of Proposed Algorithm (Trust Building logical computation algorithm i.e. TBLC)

In this proposed scheme, similar definition for key generation process, prime number generation, sign generation, pseudo random number etc in order to generate security token or keys has been followed from base paper.[1]
During the auditing process, the TPA picks random element subset I = {s1, ….,sc} of set [1,n] and upon receiving auditing message during these process the CSP runs GenrateProof to generate a response proof of data storage accuracy. Particularly, the CSP chooses a random number r ← Zp via r = f (k)kdf where (k)kdf is the randomly chosen KDF key by CSP for each auditing and calculates P = e(u, v). Meanwhile, the CSP also calculates an aggregated signature σ = Ji ε I σi. Then It forwards the response proof of storage accuracy of the TPA. With the response from

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

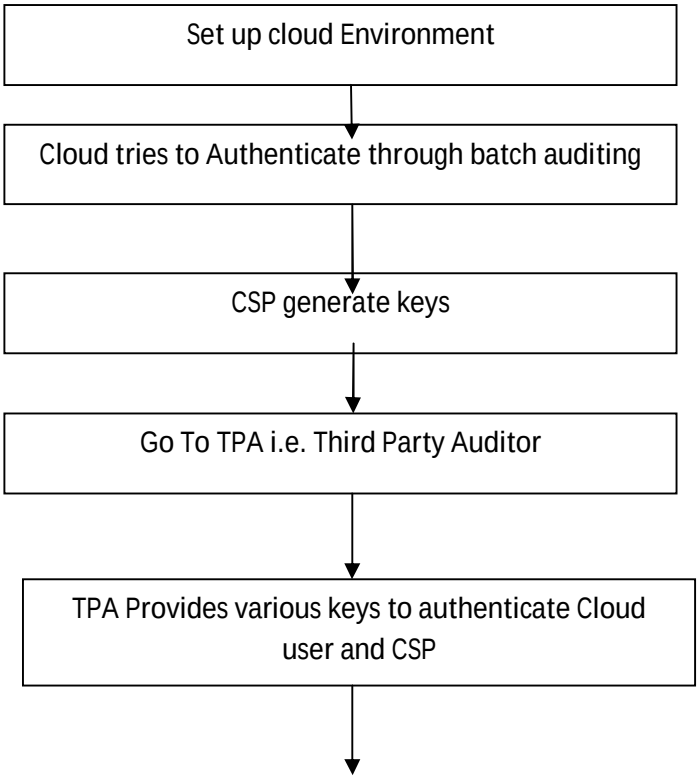
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

the CSP , the TPA runs Proof verification to validate the response by first Computing γ and then verify the all credentials.

1. Let Tx be the number of resource acessable by CloudUser
   Tx = { Resource 1, Resource 2, Resource 3,Resource 4, ….Resource$_n$}
2. Let Cu be the number of CloudUsers that can access the resource
   Cu = { Cu1, Cu2, …. Cu$_n$}
3. Basic structure of cloud user be represented as
   CloudUser : Name Email ID Public key Security token
4. Let n be number of requests to the cloud service provider.
5. Let CSP be number of cloud service provider
   CSP = { CSP1, CSP2, …. CSP$_n$}
   Fundamental structure of Cloud service provider be represented as
   CSP: Name ID Resource ID Private key Public key
6. Apply whole process of TBLC algorithm for getting credentials for various time analysis depending upon various parameters and terms like Key generation , Generation of sign , proof verification etc.
7. Let n be the number , Let TPA be the external Third Party Auditor represented by variable.
8. Basic Structure Of Third Party Auditor:
   TPA: VName RIssue RIssue RIssue Register then Register and at last Verify
9. Get the improved results of various parameters like Server Computational time , no. of auditing batch etc on the basis of TBLC algorithm as discussed above.

VIII. GENERAL FLOW GIAGTRAM FOR PROPOSED METHODOLOGY



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

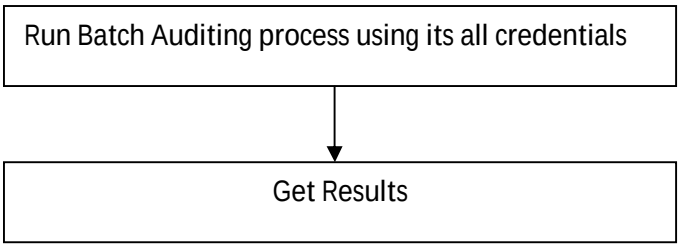


Figure 4 General flow graph of proposed Methodology

IX. CONCLUSION AND FUTURE SCOPE

This paper has lot of implications for cloud based service provider and uses in terms of understanding the uses of public auditing and security framework demonstrated here.
This includes following recommendations and conclusions for building trust between Cloud user and Cloud Service Provider:-

a) First of all austere registration and validation of the process and ensures good intend of both Cloud user and Cloud Service Provider.
b) Auditing will lead to compare desire introspection of CSP network traffic, this would help to build a public blacklist of people who misbehave while accessing cloud based services.
c) The auditing and security model of cloud service provider based on our proposed framework would lead to ensure the strong authentication access controls while understanding the dependency chain of events associated with the service which the cloud user is trying to access.
d) Proposed framework would ensure ratio of transparency into overall system as well as compliance reporting which would further help in determining any securely breach.
e) My work in future can help and inspire to collaborate the cloud user and cloud service provider together to form backup and retention strategies that would make the cloud safe to work.

For future, still a lot of work needs to be done to build adverting incidence reporting system which work across multi-cloud service providers publically whose data can be useful for identifying black listed cloud users and cloud service providers and no system has been build yet in which disclosure of infrastructure retains (for e.g. patch levels, firewalls etc.) can be integrated between both cloud user and cloud service providers.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou" Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM 2010.
[2] Alok Tripathi, Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur CentreGorakhpur, India, 2010, IEEE.
[3] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE,Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member," Toward Secure and Dependable Storage Services in Cloud Computing", IEEE , April-May 2012
[4] Cong Wang, Student Member, IEEE, Sherman S.M. Chow, Qian Wang, Student Member, IEEE,Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member," Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE 2011.
[5] Cong Wang, Qian Wang, and Kui Ren," Towards Secure and Effective Utilization over Encrypted Cloud Data", 2011 31st International Conference on Distributed Computing Systems Workshops, 2011 IEEE.
[6] Federico Maggi, Stefano Zanero ," Is the future Web more insecure?", 2011 EWI
[7] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo," An Effective privacy protection scheme for cloud computing",IEEE 2011.
[8] Jianfeng Yang and Zhibin Chen ," Cloud Computing Research and Security Issues", IEEE 2010.
[9] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE,Wenjing Lou, Senior Member and Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE, in May 2011
[10] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010 IEEE.
[11] Ru wei huang , wei zhuang, xiaoLin gui," Design of Privacy-Preserving Cloud Storage Framework", IEEE 2010.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

[12] S. Bertram1, M. Boniface, M. Surridge, N. Briscombe1, M. Hall, "On-Demand Dynamic Security for Risk-Based Secure Collaboration in Clouds", IEEE 2010.
[13] Shigeaki TANIMOTO, Manami HIRAMOTO, Motoi IWASHITA, Hiroyuki SATO, Atsushi KANAI," Risk Management on the security problem in cloud compluting", IEEE 2011.
[14] Uma Somani, Kanika Lakhani, Manish Mundra," Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing",IEEE 2010.
[15] Subashis Biswas1, Meghdut Roy Chowdhury2, Arun Kanti Manna3, Argha Roy4 Hybrid Cloud Technology: New Model For Reliable Data Storage At Users" End", Int. J. on Information Technology, Vol. 5, 2014