International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue No. 12, December 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURE ENVIRONMENT FOR CLOUD COMPUTING USING MODIFIED THIRD PARTY AUDITING (TPA) SYSTEM

Alok Kumar[1], Kavi Bhushan[2], Manik Chandra Pandey[3]

[1]*M.tech Computer Science & Engineering, Subharti University, Meerut, (India)*

[2.]*Assistant Professor, Sir Chhotu Ram Institute of Engineering and Technology, Meerut, (India)*

[3] *Assistant Professor, Department of Computer Science, Subharti University, Meerut, (India)*

ABSTRACT

Cloud computing is a technology for user according to their need on the basis of resources. Many facilities and resources are shared in cloud computing technology at a huge level over the internet due to which the resource security is needed. This paper is proposed to control the security issues in the files stored in the cloud environment. These data stored in the cloud is made secure with break and join encryption module where the key is break and further joined to generate the actual key. The work proposes a new mechanism which leads to the formation of smart confidential supervise to controls the cloud storage and also secures confidential information as like tender quotations and the other contract details.

I. INTRODUCTION

Everything has cloud linked to it by one means or the other. Let it be a technical magazine or a blog, all talk about fresh and new emergent technology so called cloud computing. Definition of Cloud computing varies from professionals to professionals and from individual to individual. Everyone has their own way of defining cloud computing. Basic working motto of cloud computing is to provide cheap and efficient service to the mass. This reduces infrastructure cost, data management cost, etc. cloud providers offers vast services such as software as a service, infrastructure as a service, platform as a service and also few hints of monitoring as a service. These are services faces a common problem of data integrity problem. In recent times, most of the enterprise application is deployed in cloud. [1][2][3][12]Cloud is of three types, public cloud which is mostly maintained by third parties, private cloud which is used for Specific application and hybrid cloud which is a combination of both the above mentioned clouds. Recent times, lot of hacking stuff are coming into report. This is due to poor security measures of corporation. In addition to the fault of corporation, there is a third party often at fault, the users.

Data Migration in Cloud: Data Migration is a process which involves moving a large amount of data or applications to the target cloud. The target cloud can be a public cloud, a private cloud or hybrid cloud. An organization's business needs large numbers of applications to fulfil and to improve its growth, now data migration process is provided as DaaS (Database as a service). The data can be migrated in several ways such as —from any organization to a target cloud or from one cloud to another cloud. Although it is relatively tough

task to migrate data and data migration involves various major security issues such as data integrity, confidentiality, security, portability, data privacy, data accuracy etc.[2][3][4]

1. Pre-Migration: In pre-migration scheme before migrating the data to cloud, some transformational activities are done previously. These activities include server virtualization, server platform upgrades or data separation. The foremost purpose of this scheme is to make transformation easier by changing data into required format. So main advantage of this scheme is that it makes the migration process easier, faster or less risky.
2. Post-Migration: In this method, transformational activity is done after the migration has completed to the cloud. Once the migration services have been successfully transitioned to the cloud, Data Centre Migration programmed should wind-down.

II. CLOUD COMPUTING SECURITY

Third party Auditor (TPA): Third Party Auditor is kind of supervisor. There are two categories of TPA: private TPA and public TPA. Although, private TPA can achieve higher scheme efficiency than the public TPA. Public TPA allows anyone, not just the client (data owner), [12] to challenge the cloud server for the correctness of data storage while keeping no private information. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. To let off the burden of management of data of the data owner, TPA will audit the data of client. The released audit report will be beneficial to the cloud service provider to improve their cloud based service platform and would also help owners to evaluate the risk of their subscribed cloud data services. Thus TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

Security as well as data storage correctness is primary concern since cloud consumers save their data in cloud server. A new secure mechanism is introduced to provide security to different cloud types. The Secure Socket Layer (SSL) protocol is implemented to achieve data storage security. SSL protocol is efficient and safer than the other former secured algorithms.

III. RELATED WORK

Ateniese et.al (2007) [1] proposed a framework named as Provable Data Possession (PDP).In this PDP protocol is used which verifies outsourced data storage site retains a file which consist n blocks. With PDP, client first process the file named as F and add some data and expands it to a new file F'. After that client add some VMd (Verification metadata) named as M for file F' and stored it on cloud server. [12][18][22][8]Generated M will also store on client local storage with metadata M. Client deleted metadata but before deletion client will execute a data possession to server by giving challenge to server to make sure that server successfully retained the file Yes or No response from server verifies the existence of file at cloud storage. In this Provable Data Possession system client issue a challenge and a send request(R) to compute proof of possession P and sends to client to verify results of integrity.

Cloud computing is becoming more and more popular nowadays, where data is outsourced into the cloud. Its

advantages are obvious: relief of the burden of storage management on data owners, universal data access with independent geographical locations, and avoidance of capital spending on hardware, software, personnel maintenance, etc. [1]. However, outsourcing data leads to new security issues as listed below.

- The first issue is data integrity and data loss. [2][3][4] Describes a wide range of both internal and external threats to data integrity. Data loss examples are mainly cloud service providers (CSP), for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed [5], or even hiding data loss incidents to maintain a reputation [6].
- The second issue is data leak. To keep the data confidential against un-trusted CSPs, the main method is to store only the encrypted data in the cloud [7], [8].
- The third issue is authorization and access control for data files. That is, operations on files must be authorized, and the cloud server (CS) must control operations on files according to the authorization information.

  The first issue and the second issue are addressed by proof-of-storage schemes [9], [10], [11] and encryption schemes respectively [7][8], while the third issue is now under consideration by the NIST, who introduces a standard reference model, named role-based access control (RBAC) [12]. The basic idea of RBAC is establishing permissions for accessing data based on the functional roles, and then appropriately assigning data users to a role or a set of roles. Finally, access controls are based on the roles that individual data users have.

The existing scenario flows with paper work [12][18][14][21] which as to be authorized manually, the take-down procedures are manual. These manual works must be monitored duly in order to avoid any type of procedural fault. Manual process also engages with uncovered money perseverance, and if any type of sight fault will lead to missing of paper work which sometimes tends to re-establishment of the entire scenario by the management person. In particular, when account information is transferred by manual process then defining to the protection mechanism must also be considered. The time concept plays a role in the manual process, which sometimes extremes if the person/management in-charge is unavailable of a period of time.

In addition [12][18][15][21] the superior complexity is also to be considered in the manual definition of government oriented paper made work scenario. Even in case of any small error then the entire work flow must be re-defined from the scratch. Taking down old file will be also a tedious process for long time pending process by an applicant. The work generally, decreases by paper work since any type of error will lead to work fault. The un-signed must duly, verify all the scenario every time in the progression

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages [10].

5.1.1 Security and Privacy — Perhaps two of the more “hot button” issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers[12][18][13][19]. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust

and a Hybrid cloud could support such a deployment.

5.1.2 Lack of Standards — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable [11].

5.1.3 Continuously Evolving — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving [11].

5.1.4 Compliance Concerns — The Sarbanes-Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. As with security and privacy mentioned previously, these typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization [11].

Storage in cloud is an area of concern for confidential departments. The files over network can be sniffed by any malicious intruder. This makes many vendors and small companies hesitate to use cloud service. This forces the use of manual process. The most incurred problems by use of manual work and paper work is time consumption, error and misplacement of documents. Search of any particular detail becomes too time consuming and tedious. Many problems go unseen such as survey reports, etc.

To maintain the secure environment a new mechanism is required to secure the source sharing on cloud.

IV. PROPOSED WORK

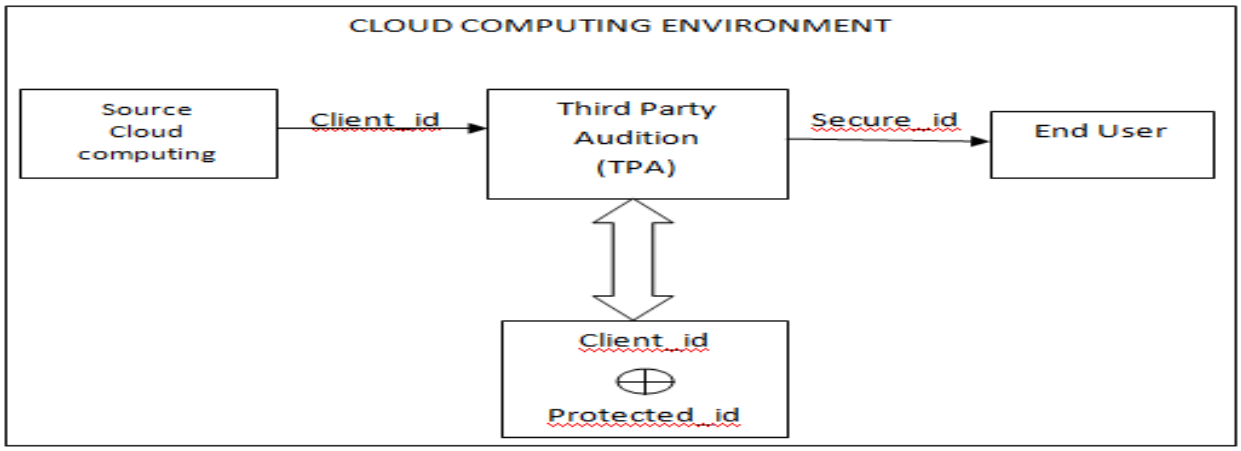
4.1 Mechanism

Distributed Denial of Service (DDOS) attack is a major problem for any kind of server. It not only affects the performance of the server but also it takes a lot of burden over the user using the server. A lot of different mechanisms have been already implemented to prevent the DDOS attack such as third party authentication (TPA) was integrated with access control mechanism but there was problem with that mechanism because TPA was outsourced to third party that was result in higher cost and the system was totally relay on third party that effects the reliability of the system .In this proposed architecture a new and a secure authentication system is proposed using HASH function/ Digital Signature for TPA.

User sends a request comes for process to TPA, detect by their CLIENT_ID i.e. Encrypted Hash function/ Digital Signature that helps to communicates with that client. This CLIENT_ID is resolved by TPA and combined with PROTECTED_ID that contain by TPA itself to create a SECURE_ID. When SECURE_ID is authentic and protected then the grants will further provide to the user. It is method that helps to detect the request of the genuine user on the basis of CLIENT_ID and PROTECTED_ID. The TPA server secure on the

basis of roles mechanism that implemented with the detection and prevention of DDOS attack.

4.2 Architecture



4.3 Algorithm

Algorithm for security in TPA

For all the requests from users

for (i= 1 to n)

{

user sends CLIENT_ID to the TPA

// CLIENT_ID is combined with PROTECTE_ID to create SECURE_ID

SECURE_ID=CLIENT_ID + PROTECTED_ID;

```
        if(PROTECTE_ID == valid)
                {
                        access grants;
                        i= i+1;
                }
        else
                {
                        Access denied;
                        i= i+1;
                }
}
```

V. CONCLUSION AND FUTURE WORK

As studies quote, Cloud computing is an end user technology. Corruption takes a great hindrance to economy of any developing country. Many facilities and resources are shared in cloud computing technology at a huge level over the internet due to which the resource security is needed. This paper is proposed to control the security issues in the files stored in the cloud environment. These data stored in the cloud is made secure with break and

join encryption module where the key is break and further joined to generate the actual key. These manual works must be monitored duly in order to avoid any type of procedural fault. In particular, when account information is transferred by manual process then defining to the protection mechanism must also be considered. These data stored in the cloud is made secure with break/retrieve encryption module. The work proposes a new architecture which leads to the formation of smart confidential supervisor and bug handler which controls the cloud storage and also secures confidential information as like tender quotations and the other contract details.

REFERENCES

[1] Aiiad Albeshri, William Caelli," Mutual Protection in a Cloud Computing Environment" in 12th IEEE International Conference on High Performance Computing and Communications 2010.

[2] Balachandra Reddy Kandukuri, Ramakrishnaaturi V, Dr.Atanu Rakshit," Cloud Security Issues" in IEEE International Conference on Services Computing 2009.

[3] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham," Security Issues for Cloud Computing" in International Journal of Information Security and Privacy, April-June 2010

[4] Lombardi, R. Di Pietro, "Secure Virtualization for cloud computing".Journal of Network and Computer Applications, Elsevier, June 2010

[5] Riley, X. Jiang, D. Xu, "Guest-transparent prevention of kernel rootkits with vmm- based memory shadowing". In RAID '08: Proceedings of the 11th international symposium on recent advances in intrusion detection, Springer-Verlag, Berlin, Heidelberg, 2008.

[6] Samoud Ali, Cherif Adnen," RSA ALGORITHM IMPLEMENTATION FOR CIPHERING MEDICAL IMAGING", Signal processing Laboratory - Science Faculty of Tunis, 1060 Tunis

[7] Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013

[8] https://www.eucalyptus.com/eucalyptus-cloud/iaas/architecture

[9] R. Balasubramanian, M., Aramudhan "Security Issues: Public vs Private vs Hybrid Cloud Computing" International Journal of Computer Applications, Volume 55 - Number 13, 2012

[10] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, "Research Challenges and Security Issues in Cloud Computing" International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3

[11] Rajesh Piplode, Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012

[12] Shyamli Dewan, Devendra Kumar, Sandeep Gonnade "Secure Data Migration across Cloud System Using Third Party Auditor (TPA)" International Journal of Innovative Research in Science Engineering and Technology Vol. 4, Issue 6, June 2015

[13] Ateniese G., R.Burns, R. Curtmola, J.Herring and L.Kissner et al., "Provable data possession at

untrusted stores.", Alexandria, Virginia, USA,ACM 978-1-59593-703-2/07/0011,page-598-610,2007.

[14] Wang, C., Q. Wang, K. Ren and W. Lou,"Privacypreserving public auditing for data storage security in cloud computing",IEEE Computer Society, ISSN:0018-9340,Vol.62,Issue 2,page-362-375, 2010.

[15] Venkatesh, M., M.R.Sumalatha and C.Selva Kumar,"Improving public auditability, data possession in data storage security for cloud computing."International Conference on Recent Trends in Information Technology (ICRTIT),IEEE,ISBN:978-1-4673-1599-9, page-463-469,2012.

[16] Sarfraz Nawaz Brohi, Mervat Adib Bamiah, SuriayatiChuprat and Jamalul-lail Ab Manan 2013 "Design and implementation of a privacy preserved off-premises cloud storage". Journal of Computer Science 10 (2): 210-223, 2014, ISSN: 1549-3636, page-210-224, 2014.

[17] Rashmi Rao, Pawan Prakash, "Improving security for data migration in cloud computing using randomized encryption technique.

[18] Sukhvinder Kaur, Mandeep Kumar Kashyap , Ms. Jagdeep Kaur" Implementation of Effective Third Party Auditing for Data Security in Cloud", Volume 5, Issue 1, January 2015 International Journal of Advanced Research in Computer Science and Software Engineering

[19] Chandramouli R., (2000), "Application of XML Tools for Enterprise-Wide RBAC Implementation Tasks", 5th ACM workshop on Role-based access control.

[20] T. Finin et. Al (2008), "ROWLBAC – Representing Role Based Access Control in OWL", ACM SACMAT'08, Vol.11.

[21] .M.R. Chowdhury et. Al (2008), "Enabling Access Control and Privacy through Ontology", 4th International Conference on Innovations in Information Technology, IEEE.

[22] Rodolfo Ferrini et. Al (2009), "Supporting RBAC with XACML+OWL", 14th ACM Symposium on Access Control Models and Technologies (SACMAT '09).