ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Identity Based Approach for Cloud Data Integrity in Multi-Cloud Environment

Ali Mohammed Hameed Al-Saffar[1]

Department of Master of Computer Science (Information System), Al- imam Al-Kadhum College for Islamic science Al-Najaf, Iraq[1]

Abstract: Cloud computing is a new computing model which enables individuals and organizations to gain access to huge computing resources without capital investment. It does mean that users can utilize computing resources in pay per use fashion. With virtualization technology the commoditization of computing resources has become a reality. The world is experiencing the advantages of cloud computing as industry giants like Microsoft, Google, Amazon etc. are providing cloud computing services. However, the cloud environment is considered in trusted as it is accessed through Internet. Therefore people have security concerns on data storage security of cloud computing. Many techniques have been proposed in the literature for ensuring data storage security in cloud computing. This paper proposes a model for cloud data integrity in the distributed multi-cloud environment. The proposed method is testing using a prototype application which demonstrates the proof of concept. The empirical results revealed that the proposed system is exhibits higher performance when compared with existing solution.

Keywords: Cloud computing, security, data integrity, multi-cloud.

I.INTRODUCTION

With the advent of new technologies like Web Services and Virtualization, cloud computing became a reality. With cloud computing people can get three kinds of services such as platform as a service, software as a service and infrastructure as a service. The cloud deployment models include private cloud, public cloud, community cloud and hybrid cloud. The private cloud is the cloud within an organization's network. Public cloud is the cloud accessible to entire world through internet based on certain standards. The community cloud is among companies privately while the hybrid cloud is the combination of two or more types of cloud. As the cloud is becoming more popular, there are growing security concerns. These security concerns led to the research in the area and many researchers proposed protocols and techniques to ensure cloud data security. The cloud service providers take care of compete security of cloud data.

However, as the cloud is in trusted (accessed through Internet), lot of research went on storage security in cloud. Some of the papers and their techniques are briefly provided here. In [1] distributed verification protocols are invented for ensuring data storage security in cloud computing. This is achieved by implementing a distributed auditing mechanism which ensures that the data dynamics of all cloud users are ensured and tested for integrity. In [2] a third party auditing mechanism is implemented in order to secure cloud storage. Continuous correctness of data is the SLA (Service Level Agreement) implemented in this paper. Public auditing of this paper helps in data integrity of multiple cloud users. In [3] a new approach is presented. It is known as distributed accountability for data sharing. It is achieved by implementing a JAR which has data and security mechanism besides accessibility lists for various cloud users.

In [4] multi clouds are implemented in order to safeguard data of clients. In other words it is the cloud of clouds for improving robustness of storage security. In [5] a novel approach is used to store, retrieve and forward data in the cloud. It uses secure erasure code to ensure data security and encryption mechanisms for forwarding data to other legitimate users. In [6] cooperative provable data possession concept is used. It ensures that cloud environment works cooperatively and secure data. In [7] security to cloud data is provided using Sobol Sequence. This paper implemented a distributed verification protocol that relays on erasure code. In [8] also public auditing is implemented for cloud storage security. The third party auditor checks for data integrity and ensures that the data is not tampered with in the server. The rest of this paper is devoted to review three papers pertaining to data storage security problems in cloud. Almost all papers assumed that, the cloud storage is not secure as the service provider may delete data or the cloud owner does not disclose storage problems in the cloud.

II.RELATED WORKS

There are many security challenges or threats in cloud computing. They include insecure API, inadequate infrastructure, data loss, hardware failure, natural disaster, hijacking, malicious insider, abuse, malware and CPU closure [21]. To overcome security and data integrity problems in cloud computing many schemes came into existence. Provable Data Possession (PDP) and its variant is one of the schemes employed to ensure cloud data integrity [11], [13], [15], [16], [17], [18], [19], [24], [26]. Many solutions came into existence on secure sharing [14]. Third Party Auditing (TPA) based solutions came into stance [20]. They provide auditing service that

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

verified data integrity. Mangaiyarkkarasi & Dhamodaran [1] studied multi-cloud environment for availability and data integrity verification. Multi-cloud environment can provide flexible storage facilities. However, data integrity needs to be carried out. Towards this end many provable data possession techniques came into existence.

Bhuvaneshwaran et al. [2] proposed Security as a Service for cloud computing. The proposed method takes care of auditing and enforces Service Level Agreements (SLAs) that are mutual agreements between cloud service provider and cloud users. Zhu et al. [3] proposed provable data possession method with zero proof concepts that could ensure data integrity. Their scheme also optimizes performance in spite of strict security mechanisms. Manjunath et al. [4] contributed to an encryption standard that can be used in cloud computing for enhancing security. Chandar et al. [5] presented a secure and flexible framework that enhances cloud security. Chozom et al. [6] also focused on multi-cloud storage issues and presented a scheme that ensures data integrity. The scheme is known s provable data possession.

Kumar & Prasad [7] contributed towards maintaining server logs that could be used to enhance cloud computing features. Tate et al. [8] proposed a hardware based approach for provable data possession. Their solution provides both data integrity and freshness. Bose & Minimal [9] explored secure data sharing in cloud computing. They proposed cloud information accountability framework for achieving this. In [10], [12] similar kind of work was done using security – mediator. Digital watermarking is employed in [22] for clod data security. A good survey of many schemes for data integrity in multi-cloud environment can be found in [23].

Remote Data Possession (RDP) [24] was in introduced with authentication for cloud data security and scalability. The PDP scheme proposed by Feng et al. proposed a new flavour of PDP (O-PDP) scheme that makes use of six polynomial time algorithms. The scheme is meant for detecting corrupted data and also recovers the corrupted blocks besides being able to mitigate data corruptions. In order to achieve the notion of provable data possession, they used online codes (kind of erasure codes) in such a way that the corrupted data can be recovered using some portion of the encoded data available. The combination of provable data possession and the coding procedure is used in the scheme.

The authors claimed their scheme to be robust for two reasons. They are the client can detect corruption of data and also recover data when it is corrupted. The protocol has four steps such as pre-processing, generating challenge (done by client), proof of possession (generated by server) and verification (done by client). This study helps to protect the outsourced data in the context of cloud computing or any outsourcing of any sort. The key results of this paper are the performance of O-PDP pre-processing and challenge time with each block size and detection probability vs. number of request blocks.

III.PROPOSED SYSTEM AND PROTYPE IMPLEMENTATION

The proposed system is based on the concepts introduced in [17]. According to the proposed system there are many cloud servers that work in coordinated fashion. The clients send request to cloud which uses the proposed framework for provable data possession. In other words, the proposed system is capable of ensuring data integrity in multiple clouds.

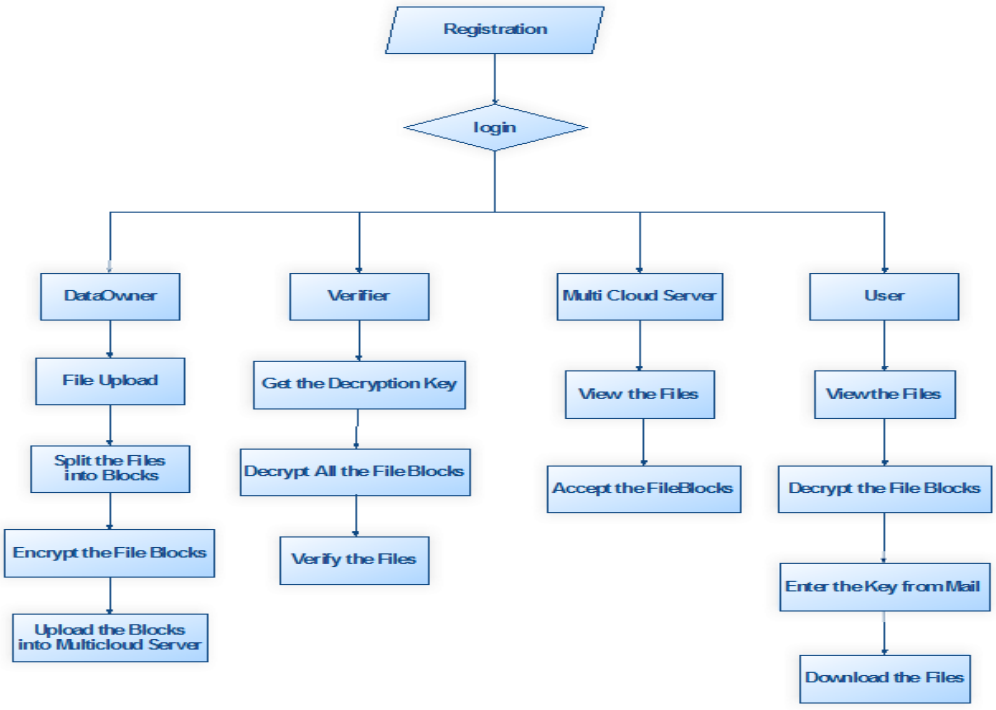

Figure 1 – Overview of the activities of the parties in proposed system

DOI 10.17148/IJARCCE.2015.48110

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

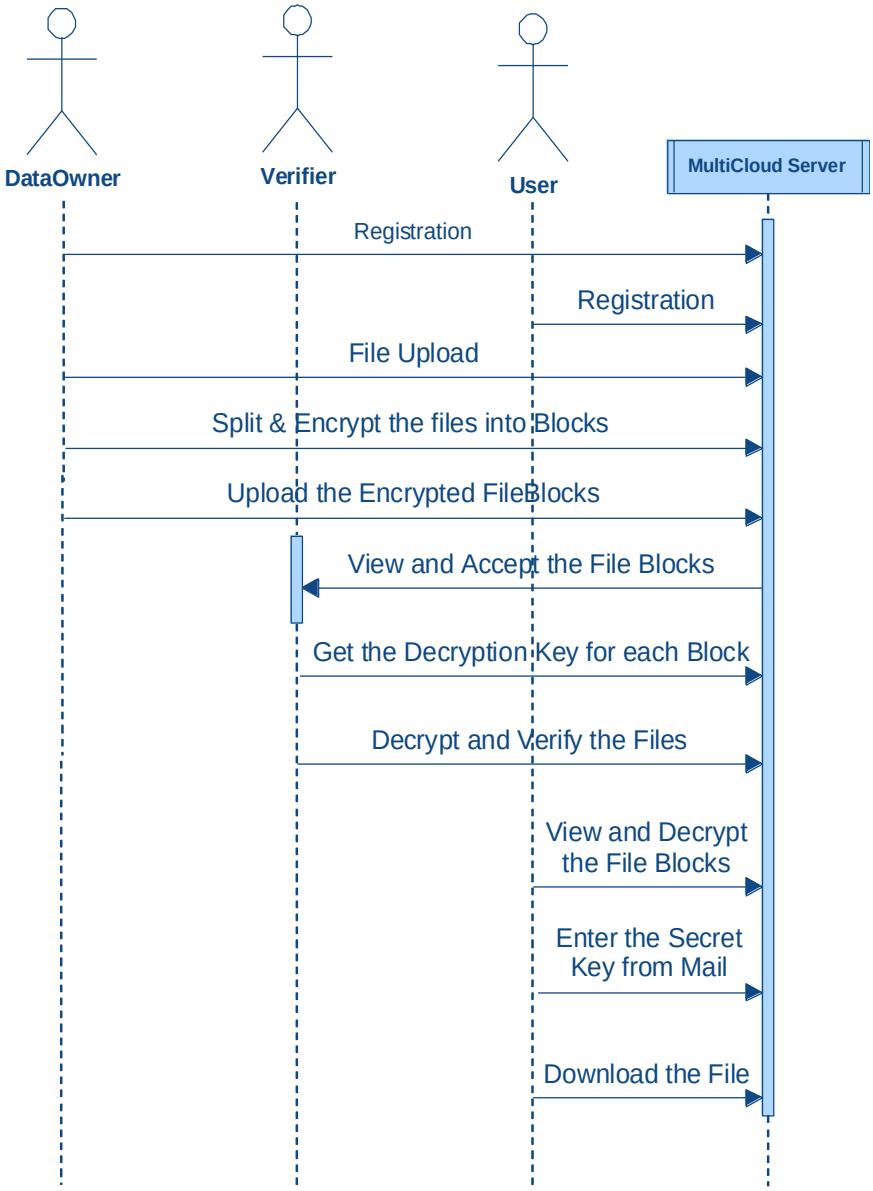

Figure 2 – The communication dynamics among parties involved

As can be seen in Figure 1, it is evident that there are different parties involved. They are known as data owner, verifier, multi-cloud server and user with respective operations performed generally.

We built a prototype application in Microsoft.NET platform that demonstrates the proposed model. Identity based approach is used to achieve this. There are four modules in the prototype application. They include data owner, verifier, user and multi-cloud server. Data owner is the user who outsources data to cloud. Verifier is responsible to verify cloud data integrity. User is the data user who gets permissions from data owner. The data user can access cloud data based on the privileges. Verifier can check the data integrity based on the keys provided. The cloud data owner can involve in encryption and decryption procedures besides allowing other users to share his data.

As can be seen in Figure 2, different parties are performing different operations as presented in Figure 1. The operations include uploading files, downloading files, performing encryption and decryption. Data owner can upload data in encrypted format. Each block in the file gets encrypted and thus decryption of the same is required by data owner when it had expected.

EXPERIMENTAL RESULTS

Experiments are made in terms of computational cost at different cloud servers in order to perform operations. The communication cost for response is also considered.

The results reveal that the proposed system is able to enhance cloud data security in the presence of multiple clouds. Moreover it also shows performance improvement when our system is compared with prior works.

As seen in the above results, it is evident that the proposed system outperforms the existing system in terms of computational time for various activities.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

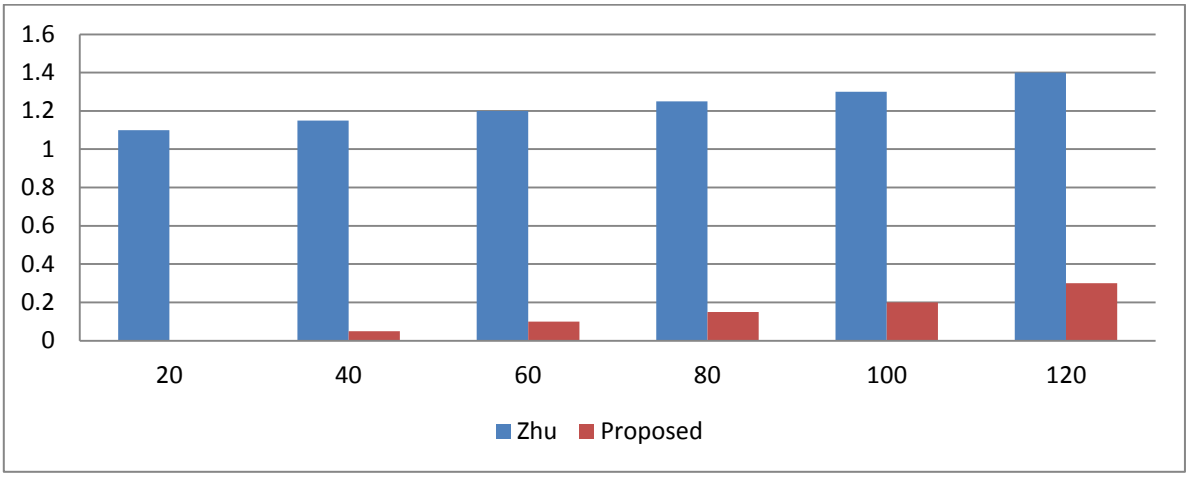

Figure 3 – Computational cost based on CS response

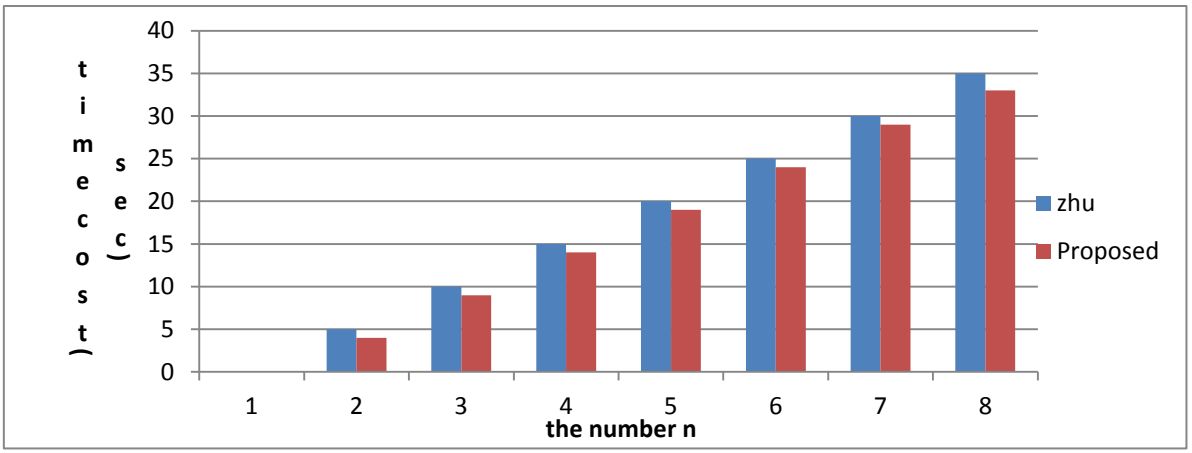

Figure 4 – Computational cost for tag generation

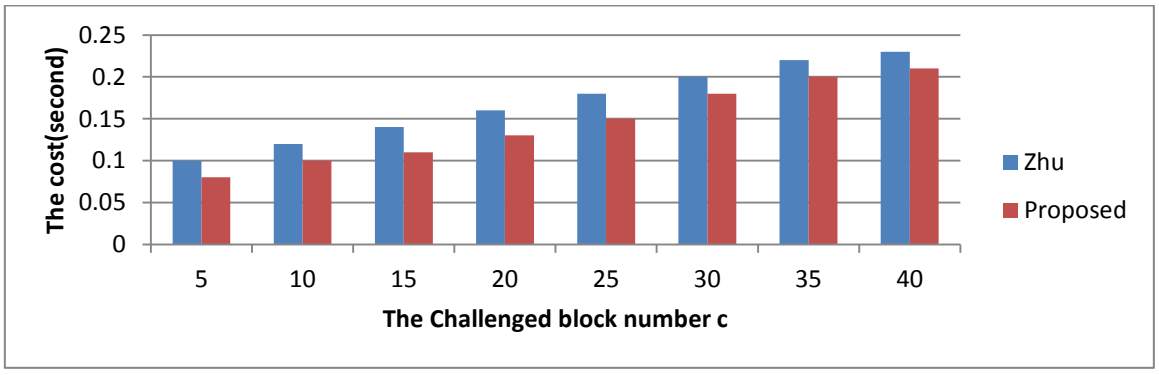

Figure 5 – Computational cost for verification

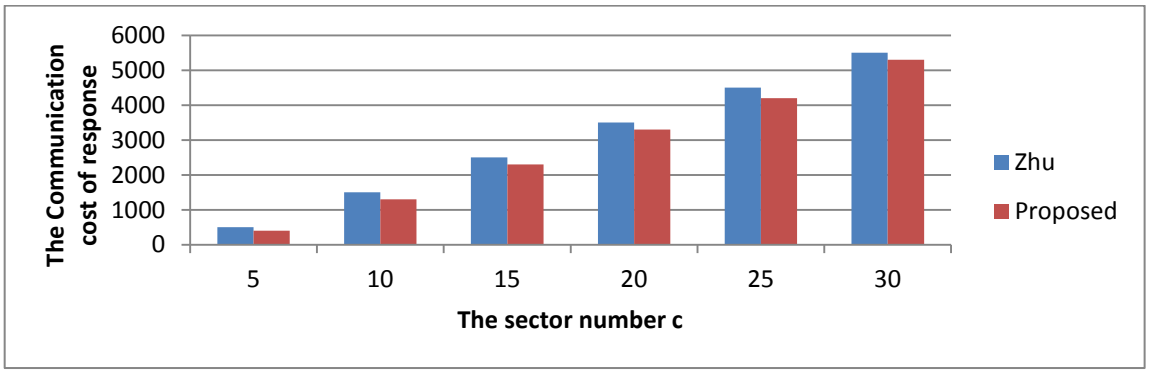

Figure 6 – Communication cost of response from server

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

IV.CONCLUSION AND FUTURE WORK

This paper focuses on data integrity in cloud computing environment. Data integrity plays a vital role in cloud computing. Many schemes came into existence in order to secure cloud data. The schemes include public auditing, provable data possession and a host of other techniques. Recently identity based distributed provable data possession was explored in [17] in the multi-cloud storage environment. In this paper we proposed a model based on provable data possession in multi-cloud storage. The proposed framework has a combiner that takes request from client and distributed block-tag pairs to various cloud servers. When the combiner gets retrieval request, it gets a challenge and that is distributed among the servers and the server responses are aggregated prior to sending response back to client. The Private Key Generator used in the framework can produce private key based on the identity given. The client and cloud servers do their respective job while the proposed model is capable of ensuring data integrity in distributed environment. We built a prototype application that demonstrates the proof of concept. The empirical results reveal that the proposed system is very secure and can ensure data integrity and availability. This research can be extended further to focus on data freshness problem in cloud computing.

REFERENCES

[1]. Ms.V.Mangaiyarkkarasi† and Mr.K.A.Dhamodaran. (2012). A Comparative Survey on Availability and Integrity Verification in Multi-Cloud. IJARCET. 1 (10), p.287-295.

[2]. Bhuvaneshwaran.S, Balamurugan.K, Dr.Vijayaraj.M. (2012). An Overview of Security Challenges in Cloud Computing. IJESIT. 1 (2), p.255-259.

[3]. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Senior Member. (2012). Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage. IEEE. p.1-14.

[4]. Manjunath A E, Pavithra H, Swarnalatha K. S , Sharadhadevi S K. (2013). Adapting Efficient Software Requirement Engineering model to implement AES Algorithm for Mobile Cloud Computing. International Journal of Advanced Research in Computer and Communication Engineering. 2 (10), p.3929-3932.

[5]. R.Bala chandar, M.S.Kavitha, K.Seenivasan. (2013). Manjunath A E, Pavithra H, Swarnalatha K. S , Sharadhadevi S K. (2013). Adapting Efficient Software Requirement Engineering model to implement AES Algorithm for Mobile Cloud Computing. International J. IJSPTM. 2 (1), p.43-54.

[6]. Tenzin Chozom, Dr. Mayilvahanan, Dr. A. Muthukumaravel. (2013). Cognitive highly distributed Cooperative Provable Data Possession scheme for achieving Dynamic Data Operations in Multi-Cloud Storage. IJLTET. 2 (4), p.417-423.

[7]. T.R pavan Kumar, Dr.Ch GVN Prasad. (2013). Distributed logs for Data Sharing using Cloud Service Provider. International Journal of Societal Applications of Computer Science. 2 (10), p.476-480.

[8]. Stephen R. Tate, Roopa Vishwanathan, Lance Everhart. (2013). Multi-user Dynamic Proofs of Data Possession using Trusted Hardware.CODASPY. P.353–364.

[9]. Nilutpal Bose, Mrs. G. Manimala. (2013). SECURE FRAMEWORK FOR DATA SHARING IN CLOUD COMPUTING ENVIRONMENT. International Journal of Emerging Technology and Advanced Engineering. 3 (1), p.512-517.

[10]. Boyang Wang, Sherman S.M. Chow , Ming Li , and Hui Li . (2013). Storing Shared Data on the Cloud via Security-Mediator. IEEE. P.124-133.

[11]. Ch.Rajeshwari, S.Suresh. (2014). An Efficient Pdp Scheme For Distributed Cloud Storage To Support Dynamic Scalability On Multiple Storage Servers. IJSEAT. 2 (12), p.985-988.

[12]. R. Bala Chandar, M. S. Kavitha and K. Seenivasan. (2014). A PROFICIENT MODEL FOR HIGH END SECURITY IN CLOUD COMPUTING.ICTACT JOURNAL ON SOFT COMPUTING. 4 (2), p.697-702.

[13]. C. HARI BABU, J. SWAMI NAIK. (2014). A Provable Data Possession Mechanism for Integrity Verification in Multi Cloud Storage. International journal of advanced technology and innovative research. 6 (4), p.251-255.

[14]. Ramakrishna Jadhav, Snehal Nargundi. (2104). A REVIEW ON KEY-AGGREGATE CRYPTOSYSTEM FOR SCALABLE DATA SHARING IN CLOUD STORAGE. IJRET. 3 (11), p.376-379.

[15]. Mrs. K. Saranya, Dr. S. Rajalakshmi,. (2014). AN EFFICIENT AUDIT SERVICE OUTSOURCING FOR DATA IN TEGRITY IN CLOUDS. IJETS. 1 (7), p.194-198.

[16]. Mr. Susheel George Joseph. (2014). Co-Operative Multiple Replica Provable Data Possession for Integrity Verification in Multi-Cloud Storage. International Journal of Engineering and Science. 4 (5), p.26-31.

[17]. G. Rebka Reveen, K. Praveen Kumar. (2014). Identity-Based Integrity Verification using PDP in Multi Cloud Storage. International Journal of Advance Research in Computer Science and Management Studies. 2 (9), p.230-236.

[18]. Megha Patil , Prof. G.R.Rao. (2014). G. Rebka Reveen, K. Praveen Kumar. (2014). Identity-Based Integrity Verification using PDP in Multi Cloud Storage. International Journal of Advance Research in Computer Science and Management Studies.. IJCSIT. 5 (2), p.982-985.

[19]. Ms.N.Elamathi, B.Selvanayagi. (2014). SECURED DATA STORAGE FOR RDPC PROTOCOL WITH ENHANCED TPA AUDITING SCHEME USING MHT IN CLOUD COMPUTING. JIREEICE. 2 (11), p.2173-2178.

[20]. F. Yahya, V. Chang, R.J. Walters, and G.B. Wills. (2014). Security Challenges in Cloud Storage. IEEE. n.d (n.d), p.1051-1056.

[21]. Yongjun Ren, Jian Shen, Jin Wang,JiangXu and Liming Fang. (2014). Security Data Auditing based on Multifunction Digital Watermark for Multimedia File in Cloud Storage. International Journal of Multimedia and Ubiquitous Engineering. 9 (9), p.231-240.

[22]. Trilok Singh Pardhi , Rajeev Pandey , Uday Chourasia. (2014). Survey of Integrity Verification in Multi-Cloud Storage by Efficient Cooperative Provable Data Possession. International Journal of Computer Applications. 102 (8), p.26-28.

[23]. Chandni Nagvanshi , Monali Sahoo. (2015). A Novel Approach in Cloud Storage for Identity Verification of Data Distributed. International Journal of Engineering Technology & Management Research. 3 (1), p.119-122.

[24]. Venkata Pallavi B, E.Padma. (2015). AUTHENTICATION BASED REMOTE DATA POSSESSION IN MULTI-CLOUD STORAGE. International Journal of Science, Technology & Management. 4 (1), p.1462-1466.

[25]. B.Banu priya, V.Sobhana, Prof.Mishmala Sushith. (2015). Concise Survey on Privacy Preserving Techniques in Cloud. International Advanced Research Journal in Science, Engineering and Technology. 2 (2), p.27-29.