

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.95 – 101

A Novel and Distributed Approach for Data Integrity in Cloud Computing

B.Swapna¹, A.Siva Kumar²

Computer Science & Engineering, JNTU Hyderabad

byri.swapna@gmail.com

TUDI RAM REDDY INSTITUTE OF TECHNOLOGY & SCIENCES

aluri.kumar@gmail.com

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 presents the details of three most recent techniques that came into existence to protect clients data stored in cloud. The empirical results of these papers proved that they are effective and can be used in real time cloud computing.

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 complete 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

This section review literature of three most recent techniques that are used to ensure cloud data security. Each technique is different from other technique. However, all the three techniques or approaches are meant for ensuring data storage security in cloud computing. These three papers give enough insights into the storage problems in cloud, which are real or assumed and required security measures in some detail.

2.1 Toward Secure and Dependable Storage Services in Cloud Computing

Cong Wang *et al*. [2] presented a mechanism for dependable and secure storage services that are meant for cloud computing. The proposed mechanism in this paper allows cloud users to audit their data to prevent cloud data problems. The auditing results reflect guarantee of cloud storage security.

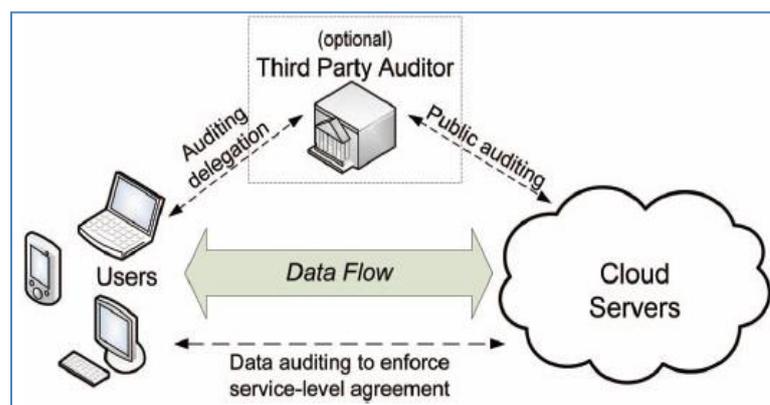


Fig. 1 – Architecture of cloud storage service [2]

From the above figure, it is evident that there are three parties involved. The users of cloud, the cloud service provider and the third party auditor. Public auditing of cloud users data is the responsibility of TPA. The users of cloud delegate auditing job to TPA. This approach allows users of cloud to securely store data. It is achieved using encryption in the form of a security setup module. Then data can be retrieved by users. It also has a mechanism to allow data dynamics that are essential. This architecture achieves security using homomorphic tokens and also the distributed erasure coded data. The adversary model used in this paper captures various kinds of security threats. It uses some approaches such as file distribution preparation, challenge token precomputation, and correctness verification [2]. The data auditing helps the data owners to feel good as it proves the integrity of data. Here the service level agreement is nothing but the agreement between parties. For instance, in this paper, the SLA on the continuous data integrity of the cloud storage is one of the service level agreements. The moment the integrity of data is lost and verified, and then it does mean that there are inconsistencies in the cloud storage. To avoid such inconsistencies and ensure that data owners gain in confidence on cloud storage this paper including others came into existence.

III. Experiments and Future Work

Experiments are made on various aspects using auditing scheme. The proposed work in this paper is meant for securing cloud data. Towards, it implemented mechanisms that support storage, retrieval, and data dynamics such as update, delete and append operations. Performance is evaluated in terms of file distribution propagation, challenge token recomputation etc [2]. Here the data is divided into blocks, encrypted and stored in cloud storage. Thus it gives security. This paper did not give any directions for future work. However, this paper can be extended by implementing more service level agreements and also letting the server to keep track of misbehaving nodes.

IV. Ensuring Distributed Accountability for Data Sharing in the Cloud

Smitha Sundareswaran and Squicciarini [3] proposed a new cloud storage model that ensures distributed accountability. The proposed framework is an object oriented solution that leverages JAR programming for ensuring data security. It exploits JAR's programming capabilities. Besides this, this paper also uses distributed auditing mechanism. The security mechanism involves data owner, cloud service provider, certificate authority, and JAR entity. JAR is programmable and dynamic. JAR stands for Java Archive. The JARS are possible with various extensions in Java. For instance .jar files for storing data in compressed format. Data owners are supposed to create a JAR file which contains data as well as security mechanisms. Such JAR is kept in cloud for scalability reasons [3]. Fig. 2 shows overview of this approach.

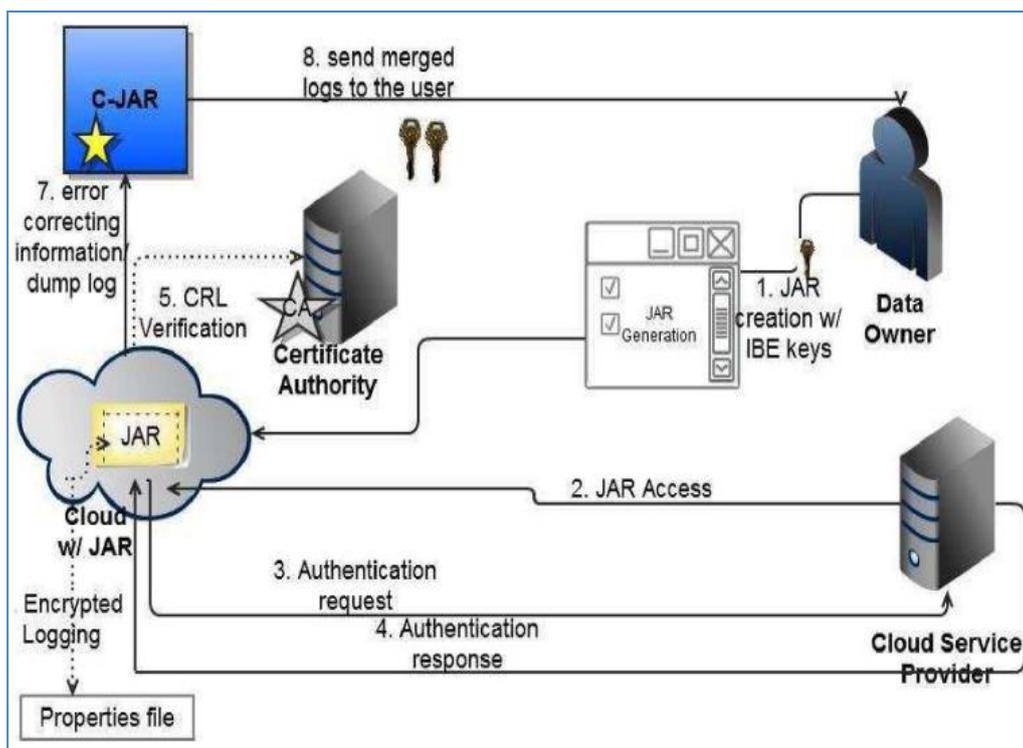


Fig. 2 – Distributed Accountability Framework [3]

As can be seen in fig. 2, it is evident that the security mechanism is distributed in nature. First of all the data owner creates a JAR file which encapsulates other JAR files with data and encryption, decryption mechanisms. The JARs are nested. The outer JAR is responsible for authentication while the inner jars contain actual data in encrypted format and also cryptographic mechanisms. After creating the JAR the data owner keeps that JAR in cloud [3]. The cloud service provider and other users can access it from cloud based on their privileges and accessibility privileges. This is a secure mechanism that prevents data inconsistency, privacy, confidentiality and other security problems [3]. A certificate authority is also involved in the security mechanisms. The CA is responsible for providing digital certificates to the participants. These digital certificates will help the candidates or parties to prove themselves as they contain identity of the people. This framework is supporting encrypted logging. Logging does mean recording events. The events are recorded as they happen. The logging data is encrypted first and logged for security reasons. With regard to encryption when data owner creates JAR file, the data being stored is encrypted and kept in an inner JAR file. The decryption takes place when the JAR is accessed by an authorized user [3]. Complete log information is provided to the data owner from time to time. Various kinds of log files are merged into a single one and sent to the data owner [3].

V. Experimental Results and Future Work

Using Emulab testbed the proposed framework is tested. The environments include open SSL servers. The experimental results reveal that the proposed framework is very secure and integrity of data can be prevented strictly. There are many experiments done for knowing its performance. For instance log creation time, logging time, log merging time, authentication time etc. are experimented using profiling. The results reveal that the framework is computationally viable. The authors provided directions for future work i.e. to refine the present approach by verifying the JVM and JRE at runtime besides authenticating the JARs.

The future research focuses on developing tamper resistant applications that work with complete security. Such applications are inherently secure and the adversaries can't break the security of such applications [3].

VI. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding

Hsiao-Ying Lin and Wen-Guey Tzeng [5] proposed a new secure storage mechanism for cloud. The new framework is based on securer erasure codes. The proposed system allows data owner to perform secure data storage, secure retrieval of data and secure data forwarding. It has robust mechanisms for storing data and also securing the data. The server side environment has both storage servers and security servers. The storage servers are responsible to store data in encrypted format while the security servers or key servers are meant for maintaining security keys and involving in authentication and authorization mechanisms. The security mechanism is based on proxy re-encryption scheme. The decentralized erasure code pertaining to cloud data is integrated with distributed storage system. The key features of this paper is that the proxy re-encryption scheme. This scheme enables encoding operations on already encrypted data and also let the user to forward it to other users using public key cryptography [5].

Public key cryptography is the asymmetric cryptography which does not involve in exchange of private keys. In this approach every participant has a public key and private key combination. The public key is known to all partners while the private key is kept secret. When a person sends data to other person by decryption the message with the public key of the recipient, only the private key of the recipient is allowed to decrypt it. This mechanism is used for secure data forwarding. Fig. 3 shows the proposed system and its architecture [5].

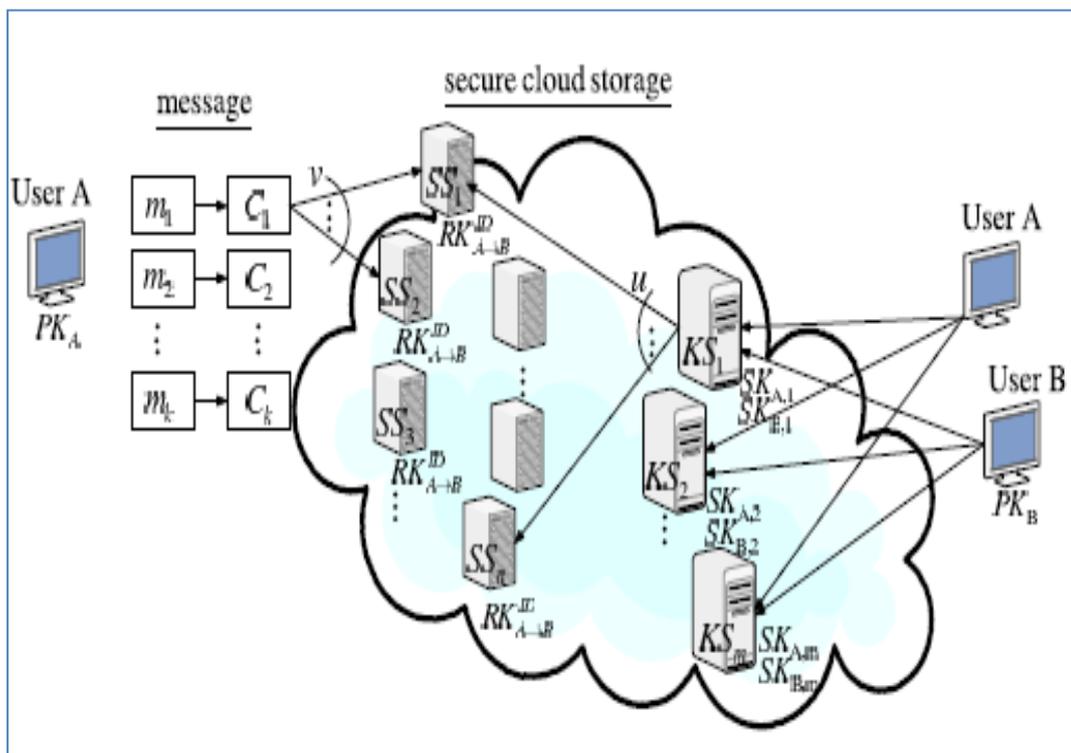


Fig. 3 – Secure Cloud Storage Architecture [5]

As can be seen in fig. 3, the data owner takes a file and divides it into many blocks such as m1, m2, etc. Each block is further subjected to encryption. The result is cipher text represented by c1, c2, etc. The cipher text is then stored in multiple storage servers. Before performing storage, the user has to do generate keys which are stored in Key Servers. The Key Servers are meant for storing security keys while the storage servers. When data owner wants to retrieve data, then the key servers have to authenticate him and the storage servers take the responsibility of storing data securely. Therefore, the storage and retrieval operations are carried out by data owner. On the other hand, the data forwarding is supported by the framework. In case of data forwarding, the data owner gives instructions to cloud storage to forward so and so message to other user. Then the cloud servers will do actual forwarding using public key encryption.

6.1 Experimental Results and Future Work

Experiments are made using the proposed framework in terms of storing data, retrieving data and also forwarding data. The experiments are intended to evaluate the system in terms of security, correctness and computational complexities. The experimental results reveal that the system is computationally feasible and provides secure environment with data retrieval, data storage and data forwarding provisions.

VII. Conclusion

This paper presents, the three most recent techniques that came into existence, to implement data storage security in cloud computing. All the papers have provided different architectural framework to ensure the data security in cloud storage. This is required as the cloud is considered in trusted. The first paper has focused on the auditing mechanism for cloud security. The second paper focused on the distributed accountability of cloud storage. In this paper a JAR programming model has been leveraged in order to accommodate security primitives in a distributed environment. It contains features like secure logging, secure data retrieval as per the privileges or access rights given. The third paper focused on the erasure code based cloud security with two types of servers namely storage servers and key servers. This has got more sophisticated security with support for data storage data retrieval and secure data forwarding.

References

- 1. Distributed Verification Protocols for Data Storage Security in Cloud Computing** Priodyuti Pradhan, P. Syam Kumar, Gautam Mahapatra, R. Subramanian 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.
- 2. Toward Secure and Dependable Storage Services in Cloud Computing** Cong Wang Qian Wang Kui Ren Ning Cao, Wenjing Lou IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012 .
- 3. Ensuring Distributed Accountability for Data Sharing in the Cloud** Smitha Sundareswaran, Anna C. Squicciarini IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012.

4. **Cloud Computing Security: From Single to Multi-Clouds** Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference on System Sciences.
5. **A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding** Hsiao-Ying Lin Wen-Guey Tzeng IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 6, JUNE 2012.
6. **Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage** Yan Zhu, Hongxin Hu, Gail-Joon Ahn Mengyang IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.
7. **Ensuring Data Storage Security in Cloud Computing using Sobol Sequence** P. Syam Kumar, R. Subramanian and D. Thamizh Selvam 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
8. **Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing** Cong Wang, Qian Wang, and Kui Ren Wenjing Lou IEEE Communications Society IEEE INFOCOM 2010.