INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2339 - 2343
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

SECURING CODE BASED CLOUD STORAGE AGAINST POLLUTION ATTACKS BY CREATING CONVINCING FAKE FILE

S.Vani, PG Scholar, Dept Of Computer Science Engineering, Mailam Engineering College, Villupuram.

P.R.Jayanthi: Associate Professor Of Computer Science Engineering, Mailam Engineering College, Villupuram.

Abstract:

Cloud computing has emerged as a new computing model that brings about plethora of benefits including storage and processing services in pay as you use fashion. The outsourced to data is stored in multiple servers maintained by cloud service providers. The servers are treated to be "untrusted" from cloud data owner's perspective. There are many security concerns over outsourced data to cloud. The existing encryption related techniques to secure outsourced data are proved to be costly and not suitable for securing cloud data in a fool proof manner. Moreover such techniques do not support data dynamics properly. To overcome this problem recently Lin et al. proposed a security scheme that makes use of two kinds of servers namely data servers and key servers in order to store data and security keys respectively. Though this scheme is secure, it suffers from inconsistencies in communication among the servers.

Keywords: Cloud Computing, Security Scheme, Servers.

1. INTRODUCTION

In the history of computing, many innovations were realized. For instance distributed computing, grid computing and so on. The latest computing model is cloud computing that allows users to access remote resources in pay per use fashion. This computing model avoids the need for capital investment. Anyone can use cloud services without investment. However, one needs to pay bills as per the usage. This will have great utility as the resources are commoditized. There are many vendors providing cloud computing services. They include Microsoft, IBM, Amazon and Google. The cloud has different deployment strategies like private cloud, public cloud, community cloud and hybrid cloud. It also has various service models such as Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). Any individual from any corner of the world can utilize these services of cloud.

The data is stored in many storage servers and the security related keys are stored in key servers. Erasure codes are used to recover any data which is lost. The security requirements like privacy, confidentiality, non-repudiation, and authentication are provided by the scheme. Before the scheme proposed by Lin et al., many schemes came into existence. Many of them are based on cryptography. The cryptographic schemes can secure data well but they do not support data dynamics easily. This is the reason why the cryptographic methods are not suitable for securing cloud data. Securing cryptography related keys is another problem in this area. In the solution provided by Lin et al. security of the data is lost if the key server is compromised.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2339 - 2343
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

Or it is difficult to achieve storage consistency when there is lack of proper cooperative communication among the servers.

To overcome that problem, this paper explores timestamp based approach. It also assumes that there are communication concerns among the servers in the system proposed in [1]. Multiple data server can help to improve the efficiency. Out timestamp based approached solves the problem of inconsistency among the storage servers in the cloud. The system also supports threshold proxy re- encryption scheme that helps in making the data storage and retrieval robust without causing security vulnerabilities. The remainder of this paper is organized as follows.

2. RELATED WORK

Distributed file system like Hadoop is required by cloud computing technology to have its benefits. There were many file systems used in the history of computing. They are Network Attached Storage, Network File System and so on. These file systems are decentralized, scalable and distributed in nature. Techniques like replica management, virtual machines, virtualization are widely used along with these file systems. File systems with features like efficiency and scalability are explored. For security reasons erasure codes are used in distributed and complex environments. These techniques are used to convert the given text into a format that cannot be understood. Each erasure code is like a vector of symbols which can represent storage problems in outsourced data.

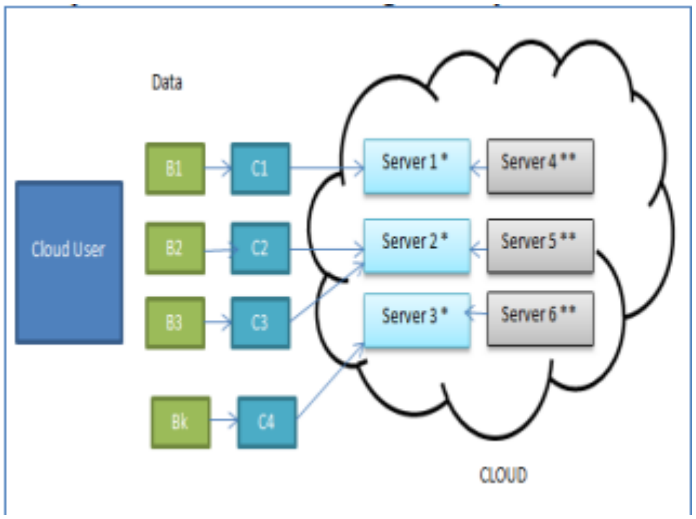

Fig.1.Basic System

In cloud computing, data owners host their data on cloud servers and data consumers can access the data from cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. However, the existing solutions are not specific to the multimedia data. Moreover copyright protection is not provided.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2339 - 2343
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

3. PROPOSED SYSTEM

We consider the auditing system model for Regenerating- Code-based cloud storage as Figure 1, which involves four entities: the data owner, who owns large amounts of data files to be stored in the cloud; the cloud, which are managed by the cloud service provider, provide storage service and have significant computational resources; the third party auditor (TPA), who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers; and a proxy agent, who is semi- trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may becomes off-line even after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy.

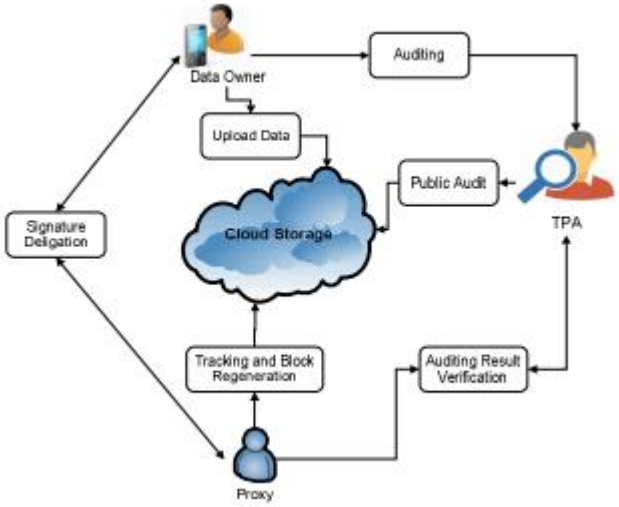

Fig.2.Proposed Architecture

After the attribute keys are prepared, the trait power and the key requester are occupied with a 1-out-of-k OT where the key requester needs to get one attribute key among k. By presenting the 1-out-of-k OT in our Key Generate calculation, the key requester accomplishes the right attribute key that he needs, however the attribute authority does not have any valuable data about authority is accomplished by the requester. At that point, the key requester accomplishes the full anonymity in our plan and regardless of what number of attribute authorities conspire; his identity data is kept secret. Owner module is to upload their files using some access policy. First they get the public key for particular upload file after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file. User module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means we do not get the file, otherwise server ask the public key and get the encrypted file. If user wants the decrypted file means user must have the secret key.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 5 (2017) PAGES 2339 - 2343
RECEIVED : 12.09.2017 PUBLISHED : 15.10.2017
Oct 15, 2017

4. ANALYSIS

All operations such as data storage, data retrieval and data forwarding are to be taken place with integrity. For instance when users send data to cloud, the storage process involves multiple servers. The timestamp based solution monitors the transaction and ensures that perfect storage takes place as expected. In case of communication concerns, the new technique has to take steps to ensure consistency. This approach is followed in data retrieval and data forwarding also. We built a prototype application for testing the efficiency of the proposed solution. The experimental results revealed that the timestamp based solution can prevent inconsistencies in cloud storage. We have made experiments in custom simulator built in Java platform. The cloud servers, cloud server providers and the data owners, the operations involved are simulated. The simulation results reveal that the proposed timestamp approach outperforms the existing approach. I

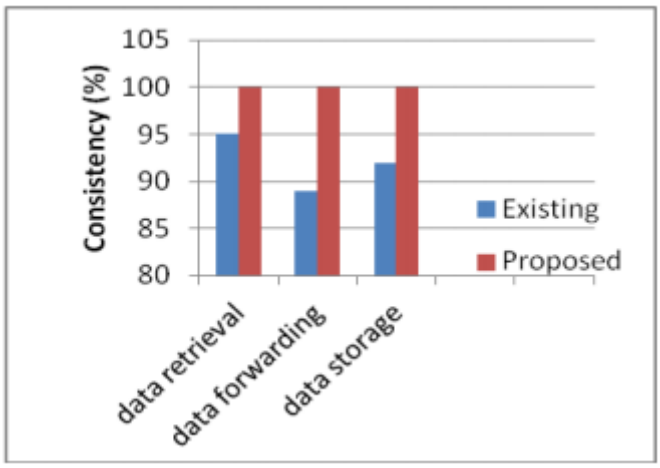

Fig.3. Analysis Comparison

n fact in all operations such as Enc, Encode, KeyRecover, ReKeyGen, ReEnc, ShareDec and Combine, a timestamp is associated for integrity of operations associated with a single transaction. The timestamp is somehow related to the ID of the present transaction. The aim of the timestamp-based operations is to ensure that all operations in a single transaction, where multiple servers are involved, are executed as a unit. Thus more cooperation and robust integrity of the operations can be achieved.

CONCLUSION

In this paper we study the cloud storage security provides more security as it used an effective architecture. We found some problems with the architecture when there are technical issues that prevent proper communication among the servers used in the architecture. In this paper we improve the architecture using time-stamp based approach that prevents communication problems among servers and ensure consistency which leads to robust communication mechanisms that help in data storage, retrieval and forwarding. We built a prototype application that demonstrates proof of concept and the empirical results are encouraging.

REFERENCES

[1] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 6, JUNE 2012.

[2] R. Sandberg, D. Goldberg, S. Kleiman, D. Walsh, and B. Lyon, "Design and Implementation of the Sun Network Filesystem," Proc. USENIX Assoc. Conf., 1985.

[3] D.R. Brownbridge, L.F. Marshall, and B. Randell, "The Newcastle Connection or Unixes of the World Unite!," Software Practice and Experience, vol. 12, no. 12, pp. 1147-1162, 1982.

[4] P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29- 42, 2003.

[6] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least-Authority Filesystem," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.

[7] S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, and J. Kubiatowicz, "Pond: The Oceanstore Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003.