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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

Ensuring Security of Cloud Backups After Data Modification

N. P. Ponnuviji[1], M. Vigilson Prem[2]

Research Scholar, Department of CSE, R.M.D. Engineering College, Kavaraipettai, India[1]

Professor, Department of CSE, R.M.K. College of Engineering and Technology, Puduvoyal, India[2]

Abstract: Cloud storage acts as a cloud computing model, where the data is stored on the remote servers that could be accessed over the internet or the cloud. The cloud storage is completely operated and maintained by several Cloud Storage Service Providers (CSSPs). The CSSPs use storage servers for storing huge data in cloud. These servers are constructed by applying several virtualization techniques. There have been more contradictions on the terms 'Cloud Storage' and 'Cloud Backup'. A cloud storage server only stores the files in the cloud and maintains the data as long as it is retrieved again for future use. As the size of the data grows, the complexity within it also increases. The expectation arises on the ability to make the data available constantly without any interruption. In such cases, we need to adopt more advanced sophisticated backup strategies, by making use of the cloud services to deliver consistent back-up solutions to the users and the organizations and also provide quick disaster-recovery solutions. In this paper, we discuss about the secure storage of data and analyse possible solutions on secure storage of backup data in the cloud.

Keywords: Cloud Storage Service Providers (CSSPs), Backup as a Service (BaaS), Third-Party Auditor, Cloud storage, Cloud backup, key update, verifiability, Remote server

I. INTRODUCTION

With the advancement in the development of cloud techniques, there has been a growing demand in the number of cloud-based applications. Most of the applications are dependent on the cloud platform for storing their huge volumes of data. At one end, when the data is continuously stored in the cloud, in the other end the data is retrieved, modified and again stored in the cloud. Different users may access the same data to perform modifications [1]. Few examples in the publishing sector are to be cited. When bulk data is stored, there arises the demand for backing up the data in the cloud to overcome and protect the data from natural disasters, recover the files from theft, etc. Frequent modifications from multiple users are done extensively in the cloud-based synchronization platforms like Dropbox mostly used in business applications [2] and Sugarsync that allows the team members to sync and work in accessing and modifying the same file on the cloud servers from any place at any time. The process involved in the modifications of data in cloud and data backup in cloud are different. In this paper, we discuss the multi-user modification in the cloud data using the efficient public integrity [3]. In this paper, we mainly focus on the security of the data in the cloud after it is modified and backed up in a remote cloud server. We also propose an algorithm that ensures the security of the cloud backups after modifying the data.

II. RELATED KNOWLEDGE AND RESEARCH STATUS

In section 3, the paper discusses about the cloud backup solutions and the ways to update or restore a cloud backup. We further discuss about how the customers use the service provider's particular client application or a browser interface. [5]
In section 4, we discuss the data integrity checking scheme that supports many writers to share data. We also assess how the cloud server provides data storage services to group users. We analyze about the Third Part Auditor (TPA) and the role of master user. [3]
In section 5, we analyze the auditing of the cloud storage using the verifiable outsourcing of key updates. The use of blinding technique with homomorphic property, where encryption is done using the secret keys is monitored by the TPA. We discuss about the auditing protocols and the algorithms related to it. [4]
In section 6, we explain about the proposed system where the security is discussed while we backup the data after modification. By introducing a monitor for the master user wherein the secret keys are generated by the TPA using the homomorphic property, which could be applied at the remote server, when backup of data is taking place and conclude the paper highlighting the future enhancements.

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

III. CLOUD BACKUP AND ENTERPRISE CLOUD BACKUP

There are various cloud backup solutions that enable enterprises and the individuals to store huge amounts of data and the files of the computer over the internet using a Cloud Storage Service Provider (CSSP) instead of storing the data on to a local physical disk like hard drives or tape backups. The files have the option of automatically getting saved to the cloud backup service on a scheduled regular basis. The information automatically gets backed up at any point of time by means of 'cloud sync'. These solutions add important features such as archiving and disaster recovery. The enterprise's legal requirements for data retention are taken care by archiving features as part of the concern's disaster recovery plan, at the remote off-site storage that is provided by the cloud backup.

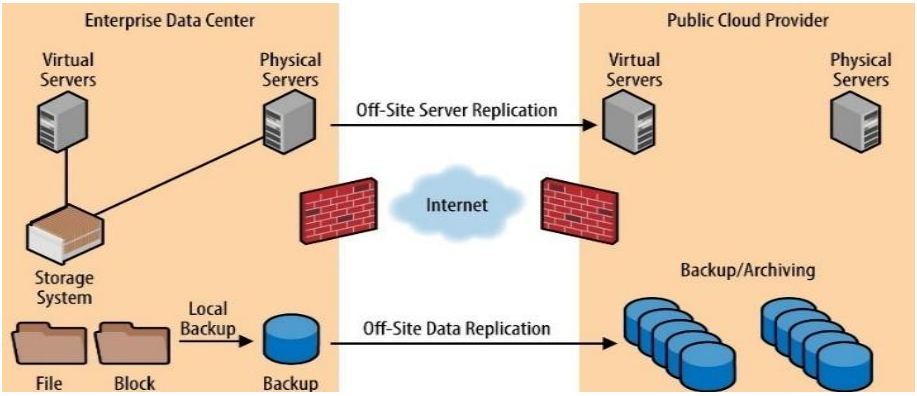

Fig 1. Scenario of Enterprise Cloud Backup

The above scenario shows the Backup as a Service (Baas) in the organization that uses cloud computing. The backup and recovery as a service actually replicates data to multiple systems and data centers, wherein the primary data that is lost or corrupted should be recovered. In the scenario, the backup and recovery servers, applications and data is a usual happening to a datacenter. Generally, in a cloud environment, the changes in the backup hardware and the processes are required to backup and protect a cloud environment. But in all the cases, the security to the backup data proves to be a nightmare at certain cases, wherein few exclusive measures need to be incorporated.

IV. SHARING CLOUD DATA WITH MULTI-USER MODIFICATION

This section explains the concept of public integrity checking for cloud data sharing that supports multiple writers. It proved highly scalable, efficient and resistant from collusion. The authentication tags that were used served as independent tools to locate and find the application easily using the verifiable keyword search. The security is achieved and seemed to be robust after modifying data in a multi-user environment.

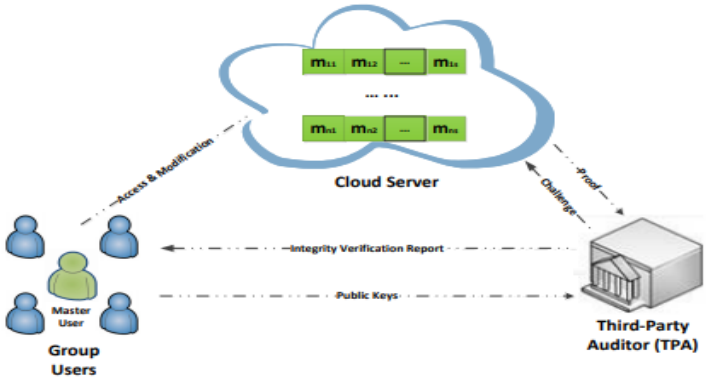

Fig 2. System model with Third-Party Auditor

The cloud server provides data storage services to the group users. In this case, the group users have a master user, who is considered as the owner for sharing data, handles and manages the access rights and membership rights of other group users. The integrity is checked by the TPA, where all the users have the right to access and modify the data. The public keys can be accessed by any cloud user, who can be a TPA. This design overcomes the Computational Diffie-Hellman problem, t-Strong Diffie-Hellman problem and Bilinear Diffie-Hellman problem. The model achieves the security goals of restricting the cloud servers from accessing the corrupted data. It prevents forging of authentication, when collusion happens among the cloud and group users other than the master user, who will not provide

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

authentication rights and details. This design fails to achieve the solution, when the master user U_0, leaves the group. Secondly, fails to address the problem when the user revokes the permission rights. There is no solution provided on the security of data backup after modification.

V. CLOUD STORAGE AUDITING WITH VERIFIABLE KEY UPDATES

In this section, the resistance to key-exposure is dealt. We discuss the key exposure problem, wherein the clients are forced to update their secret keys at regular timer intervals with limited computation resources like smartphones. The auditing of the cloud storage with verifiable outsourcing of key updates in a more secured manner has been discussed. Henceforth, the key update burden is reduced to minimal. Unlike in the previous section, the TPA holds only the client's secret key in an encrypted form. The client may download the encrypted key from the TPA, when uploading new files to the cloud. The validity of the secret key expires once the files are uploaded to the cloud successfully. To maintain a high-level security, the key update operations are outsourced to an authorized party and are not performed by the clients themselves. Here, the TPA acts as the authorized party to perform the key updates. To incorporate this feature, the blinding technique with the homomorphic property has been used along with the encryption algorithm to encrypt the secret keys.

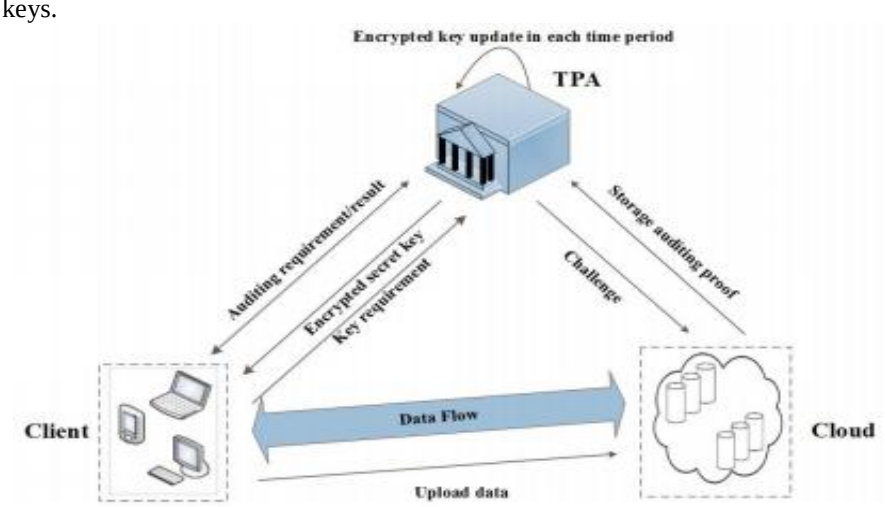

Fig 3. Cloud storage auditing model

The cloud storage auditing protocol design can satisfy the desired requirements by outsourcing the key updates. The Key Update algorithm computes the homomorphic property to the secret key that makes verifying the secret key possible. The ultimate aim of encrypting the secret keys through the key update has reduced the burden of the clients. This section fails to explain the auditing of the key updates to be performed, after data modification and back up of the modified data in the cloud.

VI. PROPOSED WORK

In our proposed work, we keenly focus on the remote server of the cloud, which maintains the backed up data and modified data. The data modification and data backup are two extreme ends to be focused. We take up the format of the master user, who takes care of the entire process of data backup, by coordinating with the TPA. The format of the data block before data modification will have the fields of: original data block, the authentication tag of the master user, secret key K_s.

Table I Original Data Format Before Modification

DATA BLOCK	AUTH TAG	K_s Secret key

After the modifying the data, the format of the data block will have the fields of: modified data block, the authentication tag of the master user, modified secret key, wherein the user will be identified the authentication tag. When the user performs 'n' number of modifications to the data, the user's 'n' secret keys generated will be stored along with the data in the secret key table of that user by the TPA. But only the modified data format will be available to the master user.

Table III Data Format After Modification

MODIFIED DATA BLOCK	AUTH TAG	K_s Modified Secret key

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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

We have now seen the data format after modification, but the data backup in the cloud is more important. Hence, the data format at the remote end of the Cloud Storage Server (CSS) may have a different data format that is provided with an additional field of the timestamp.

Table IIIII Data Format With Backup Information

MODIFIED DATA BLOCK	AUTH TAG	K_s Modified Secret key	TIMESTAMP	BACKUP UPDATE

This field stores the details of the modification that is performed on the data by means of maintaining the time and date along with the size of the data. The previous data will be stored as a backup at the remote server. The latest modified data will be stored in the Cloud Storage Server (CSS). The server will be scheduled by the TPA to take up the data backup at regular intervals. The security part will be handled by the TPA, when the backup takes place and during data transmission. When there is any unauthorized data access the proposed scheme has been planned and designed to suspend the entire process retaining the data in original. The scheme is proposed to have 8 algorithms with HMAC: {KeyGen, SetUp, Update, Challenge, Prove, Verify, User Revocation, BackUp}.

CONCLUSION

Our approach is very simple, in which we have planned to implement the above model using the mentioned algorithms. The challenge is about the data backup which is handled with transparency. The application where this model will be tested and implemented is into the publishing sector. It is in this industry, where more frequent modifications and storage of data takes place at very frequent intervals. From in this scheme, all the data that is backed up using storage devices will be reduced and move to the cloud with enhanced security and data backup. The future enhancement would be to check the level of security using different encryption algorithms. The comparison table would show the advantages and disadvantages of each model.

Table IVV Comparison With Other Models

Factors	Sharing cloud data with multi-user modification	Cloud storage auditing with verifiable key updates	Our proposed scheme
Third-Party auditing	YES	YES	YES
Secret-key encryption	YES	YES	YES
Multi-user modification	YES	YES	YES
Cloud storage auditing	NO	YES	YES
Data backup update	NO	NO	YES

REFERENCES

[1]. Jiawei Yuan, Shucheng Yu, "Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification", IEEE Conference on Computer Communications, IEEE INFOCOM 2014.
[2]. Jia Yu, Kui Ren, "Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates", IEEE Transactions on Information Forensics and Security, Vol. 11, No. 6, June 2016.
[3]. "Dropbox for business", https://www.dropbox.com/business.
[4]. "Sugarsync", https://www.sugarsync.com/business/.
[5]. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.
[6]. Kamile Nur Sevis, Ensar Seker, "Survey on Integrity in Cloud", IEEE 3rd International Conference on Cyber Security and Cloud Computing, DOI 10.1109/CSCloud.2016.35.
[7]. Akshita Bhandari, Ahutosh Gupta, Debasis Das, "A framework for Data Security and Storage in Cloud Computing", IEEE International Conference on Computational Techniques in Information and Communication Technologies, 978-1-5090-0082, 2016.
[8]. Y. Zhu, H. Wang, Z. et al., "Efficient provable data possession for hybrid clouds", in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010. Pp. 756-758.
[9]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing", IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717-1726, Sep 2013.
[10]. B. Wang, B. Li, et al., "Oruta: Privacy-preserving public auditing for shared data in the cloud", IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43-56, Jan/Mar. 2014.
[11]. J. Yuan and S. Yu, "Public auditing for dynamic data sharing with multiuser modification", IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp.1717-1726, Aug. 2015.
[12]. J. Yu, K. Ren, C. Wang and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance", IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1167-1179, June 2015.
[13]. G. Yang, J. Yu, et al., "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability", J. Syst. Softw., vol. 113, pp. 130-139, Mar. 2016.
[14]. J. Yu, F. Kong, et al., "One forward-secure signature scheme using bilinear maps and its applications", Inf Sci., vol. 279, pp. 60-76, Sep 2014.
[15]. "Amazon ec2 and amazon rds service disruption", http://aws.amazon.com/message/65648.
[16]. http://crmtrilogix.com/Cloud-Blog/Storage-and-Backup-as-Services/Backup-as-a-Service-or-BaaS/185.