

Swindling Detection Component for Allowing Mutual Trust for Cloud Storage Systems

K. LALITHA & S.NITHA

Associate Professor, Department Of CSE

AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

M.Tech, Computer Science &Engineering

AURORA'S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

Abstract:

In Cloud Computing, Storage –as –a – Service is one of the most wanted services, but the security of the data stored in the cloud using these services is the key issue. The outsourced data in the cloud has to be guaranteed with confidentiality, integrity and access control. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, a cloud-based storage scheme is proposed that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has two important features: i) It allows the owner to outsource sensitive data to a CSP, and it ensures that only authorized users (i.e., Those who have the right to access the owner's file) receive the outsourced data i.e. It enforces the access control of the outsourced data can be done by sending a

key through email to the registered users and ii) Enables indirect mutual trust between the owner and the CSP using Cheating detection module.

Index Terms: Mutual trust, Dynamic environment, Outsourcing data storage, Access control, TTP.

1. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this Information age, several organizations possess huge amount of data which needs to be kept secured. These data includes personal information, health information and financial data. Local maintenance of such huge amount of data will be cost effective and problematic. Hence Cloud Service Provider offered Storage as a Service to alleviate the burden of huge local data storage and to reduce the cost by means of outsourcing data storage to the cloud. Since the data owner outsources their sensitive data to the cloud, they want their data to be guaranteed with some security concerns like confidentiality, integrity and proper access control. In some practical applications data confidentiality is not only a security concern but also a juristic issue.

The Data produced in the Organization is Huge and very Confidential and maintaining this data to the organization is challenging so they may go for



outsourcing the data to CSP, This data may be Distributed and stored for a long time due to operational purposes and regulatory compliance. The local management of such huge amount of data is problematic and costly. While there is an observable drop in the cost of storage hardware, the management of storage has become more complex and represents approximately 75% of the total ownership cost. Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. The proposed model provides trusted computing environment by addressing important issues related to outsourcing the storage of data, namely confidentiality, integrity, access control and mutual trust between the data owner and the CSP. This means that the remotely stored data should be accessed only by authorized users (i.e., those who have the right to access the owner's file) and should remain confidential. The CSP needs to be safeguarded from any false accusation that may be claimed by a data owner to get illegal compensations. In this work, we propose a scheme that addresses some important issues related to outsourcing the storage of data, namely data dynamic, newness, mutual trust, and access control. One of the core design principles of data outsourcing is to provide dynamic scalability of data.

The main contributions of this paper are:

- 1) The design and implementation of a cloud-based storage scheme has. It allows a data owner to outsource the data to a remote CSP, and perform full dynamic operations at the block-level, i.e. it supports operations such as block modification, insertion ,deletion, and append It ensures the newness property, i.e., the authorized users receive the most recent version of the data.
- 2) Detection of False accusation by using Cheating detection module.

2. RELATED WORK

A solution to detect cheating from owner side as well as CSP side is done through digital signatures. For each file owner attaches digital signature before outsourcing. The CSP first verifies digital signature

of owner before storing data on cloud. In case of failed verification, the CSP rejects to store data and asks the owner to resend the correct signature. If the signature is valid, both the file and signature are stored on the cloud servers. The digital signature achieves non-repudiation from the owner side.

2.1 EXISTING SYSTEM:

When an authorized user (or the owner) requests to retrieve the data file, the CSP sends file, owner's signature and CSP's signature on (file || owner's signature). The authorized user first verifies the CSP's signature. In case of failed verification, the user asks CSP to re-perform the transmission process. If CSP's signature is valid, the user then verifies owner's signature. If verification fails, this indicates the corruption of data over the cloud servers. The CSP cannot repudiate such corruption for the owner's signature is previously verified and stored by the CSP along with file. Since CSP's signature is attached with the received data, a dishonest owner cannot falsely accuse the CSP regarding data integrity.

The outsourced data can be modified and scaled by the data owner. After doing modification, the authorized users are enabled to get the most recent version (newness property) of the outsourced data. A technique is required to identify the staleness of the received data. This issue is dangerous for applications in which critical decisions are made based on the received data. Mutual trust between the data owner and CSP is enabled in the proposed scheme. A method is established to resolute dishonest party from any side. Finally, the access control is considered, which allows the data owner to grant or revoke access rights to the outsourced data.

The above solution increases the storage overhead on cloud as owner's signature is stored along with the file on cloud servers. Moreover, there is an increased computation overhead, CSP has to verify signature of owner before storing file on cloud, and the authorized user verifies two signatures for each received file. If the CSP receives file from trusted entity other than the owner, the signature verification is not needed since the trusted entity has no incentive for repudiation or collusion. Therefore, delegating small part of owner's work to the TTP reduces both the storage and computation overheads. However the outsourced data must be kept private and any leakage of data toward the TTP must be prevented.

1. The CSP is untrusted, and thus the confidentiality and integrity of data in the cloud may be at risk.
2. Computation Overhead is more in owner side As well as CSP side
3. A data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement.
4. The Owner May Loss the direct control over the sensitive data.

3. IMPLEMENTATION

3.1 System Model

3.1.1 Owner Model.

That can be an organization / individual generating sensitive data to be stored in the cloud and made available for controlled external use.

3.1.2 Cloud service provider (CSP)

Who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users.

3.1.3 Authorized Users

A set of owner's clients who have the right to access the remote data.

3.1.4 Trusted Third Party (TTP)

An entity who is trusted by all other system components, and has capabilities to detect/specify dishonest parties. The cloud computing storage model considered in this work consists of four main components as illustrated in Figure 1. The relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the CSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relationship between the data owner and the authorized users.

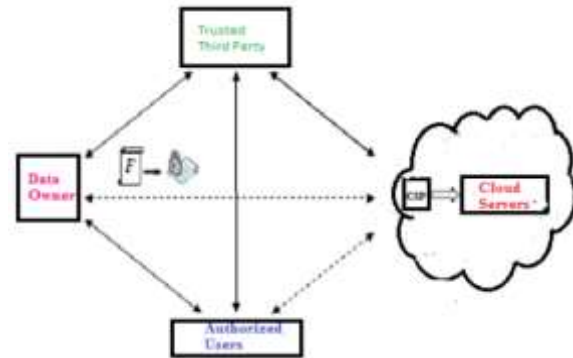


Fig 1: Cloud computing data storage system model

3.2 Updating and Access Control

The Outsourcing of the confidential data has been done by the data owner to the cloud storage servers in an encrypted form. When the authorized users request for data, they will get data in an encrypted form this data can be decrypted by them using the secret key shared among the authorized users. It is assumed that the interaction between the owner and the authorized users to authenticate their identities has already been completed, and it is not considered in this work.

The TTP and CSP must be always Online, while the owner is intermittently Online. The authorized users able to access data file from CSP even when the owner is offline.

3.3 Cheating model

The CSP resides in an untrusted domain and thus the confidentiality and integrity of data in the cloud may be at risk. For economic incentives and maintaining a reputation, the CSP may hide data loss, or reclaim storage by discarding data that have not been or is rarely accessed. On the other hand, a data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement. They may dishonestly claim that data integrity over cloud servers has been violated.

3.4 Security Requirements

3.4.1 Confidentiality

Outsourced data must be protected from the TTP, the CSP, and users that are not granted access.

3.4.2 Integrity

Outsourced data are required to remain intact on cloud servers. The data owner and authorized users

must be enabled to recognize data corruption over the CSP side.

3.4.3 Access control

Only authorized users are allowed to access the outsourced data.

3.4.4 CSP's Defence

The CSP must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behaviour is required to be revealed.

4. FRAMEWORK

Framework consists of notations, setup and file preparation for data outsourcing, data, access and cheating detection of dishonest owner/user.

4.1 Notations

- F is a data file to be outsourced
- h is a cryptographic hash function
- k is a data encryption key/secret key
- Ek is a symmetric encryption algorithm under, e.g., AES (advanced encryption standard) K
- E-1K is a symmetric decryption algorithm under K
- F1 is an encrypted version of the file F
- F1H_{TTP} is a hash value for F1, and is computed and stored by the TTP
- F1H_u is a hash value for F1, and is computed by the authorized user
- ENC_s(K) is an encrypted version of secret key under S
- S is a secret shared between owner and his authorized users.

4.2 file preparation for data outsourcing

The system setup has two parts: one is done on the Owner side, and the other is done on the TTP side and CSP will store only encrypted file as shown in figure 2.

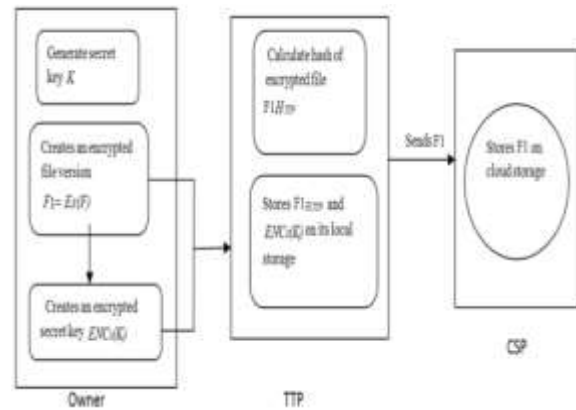


Fig 2: file preparation for data outsourcing

4.2.1 Owner role

The data owner generates a secret key K for a file. To achieve privacy-preserving, the owner creates an encrypted file version $F1 = E_k(F)$. For access control he creates encrypted secret key enables only authorized users to decrypt secret key and access the outsourced file. The owner sends F1 and ENC_s(K) to the TTP, and deletes the data file from its local storage.

4.2.2 TTP role

A small part of the owner's work is delegated to the TTP to reduce the storage overhead and lower the overall system computation. For the TTP to resolve disputes that may arise regarding data integrity it computes and locally stores hash value for the encrypted file F1H_{TTP}. The TTP sends encrypted file F1 to the CSP. The TTP keeps only F1H_{TTP} and ENC_s(K) on its local storage.

4.3 Data Access and Cheating Detection

An authorized user sends a data-access request to both the CSP and the TTP. The authorized user receives F1 from the CSP and (F1H_{TTP}, ENC_s(K)) from the TTP.

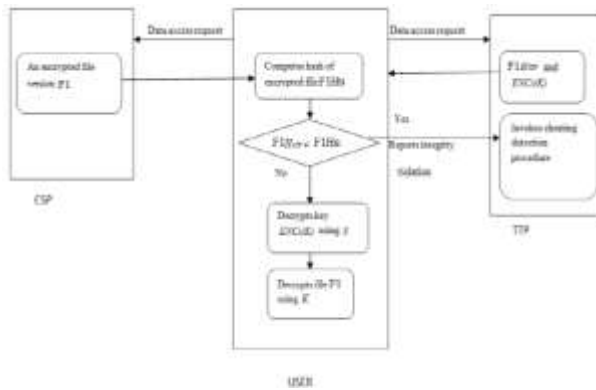


Fig 3: Data Access and Verification of encrypted data file

4.3.1 Verification of encrypted data file

The authorized user computes hash of encrypted file $F1Hu$ received from the CSP and compare it with one received from the TTP $F1HTTP$. If $F1HTTP \neq F1Hu$ then invoke cheating detection procedure at TTP. And if $F1HTTP = F1Hu$ then decrypts $ENCs(K)$ to get Secret Key K and hence decrypts file. Data Access and Verification of encrypted data file is shown in figure 3.

4.3.2 Cheating detection procedure

TTP is invoked to determine the dishonest party. The TTP receives encrypted file $F1$ from the CSP and computes temporary hash value for encrypted file $F1Htemp$. If $F1HTTP \neq F1Htemp$ then reports “dishonest CSP and data is corrupted” to owner. If $F1HTTP = F1Htemp$ then reports “dishonest owner/user and data is not corrupted”. Cheating detection procedure is shown in figure 4.

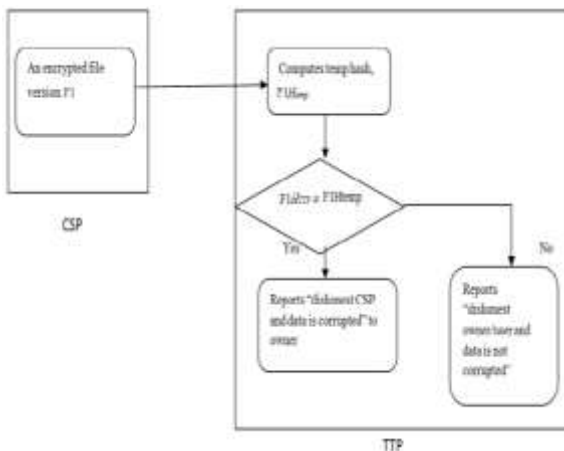


Fig 4: Cheating detection procedure

5. CONCLUSION

The cloud based storage scheme is proposed that allows owner to benefit from facilities offered by the CSP and enables Detection of Dishonest entity (i.e. owner/CSP). It enables cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. data owners to release their concerns regarding confidentiality, integrity, access control of the outsourced data. To resolve disputes that may occur regarding data integrity, a trusted third party is invoked to determine the dishonest party (owner or CSP). Also the security related issues are resolved they are: (i) Access control is enabled using the Login Modules of each entity, while Login It will validate the credentials given by the each entity. (ii) Data Confidentiality is achieved using the encryption algorithms. (iii) Detection of Dishonest Owner/CSP Using the TTP alert module.

REFERENCES

- [1] NIST SP 800-145, “A NIST definition of cloud computing”, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
- [2] 104th United States Congress, “Health Insurance Portability and Accountability Act of 1996 (HIPAA),” Online at <http://aspe.hhs.gov/admsimp/pl104191.htm>, 1996.
- [3] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, “Enabling security in cloud storage SLAs with cloud proof,” in Proceedings of the 2011 USENIX conference, 2011.
- [4] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 55–66.
- [5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable secure file sharing on untrusted storage,” in Proceedings of the FAST 03: File and Storage Technologies, 2003.
- [6] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short cipher texts and private keys,” in Advances in Cryptology - CRYPTO, 2005, pp. 258–275.
- [7] F. Seb'e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, “Efficient remote data possession checking in critical



information infrastructures,” IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[8]. A. F. Barsoum & M. A. Hasan, “On Verifying Dynamic Multiple Data Copies Over Cloud Servers,” Cryptology ePrint Archive, Report 2011/447, 2011, 2011, <http://eprint.iacr.org/>.

[9]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, & K. Fu, “Plutus: Scalable Secure File Sharing On Untrusted Storage,” in Proceedings of the FAST 03: File & Storage Technologies, 2003.

Authors

K. LALITHA Completed Master of Technology in Computer Science and Engineering from JNTU Hyderabad. Currently working as an Associate Professor at AURORA’S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.

S.NITHA pursuing M.Tech in Computer Science Engineering from AURORA’S SCIENTIFIC , TECHNOLOGICAL & RESEARCH ACADEMY, Bandlaguda, Hyderabad.