ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 373-378

Security Enhancement for Enabling Dynamic Data and Mutual Trust in Public Cloud

[1] K.NAGA SANDHYA, [2] D.RAVIKIRAN

[1] M.Tech Research Scholar, Priyadarshini Institute of Technology and Science for Women
[2] Professor, Priyadarshini Institute of Technology and Science for Women

Abstract: In Cloud Computing, Storage as a Service is one of the most required 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. In this work, we device a mechanism of cloud data storage based on indirect mutual trust between the Cloud Service Provider (CSP) and the cloud users through Trusted Third Party Auditor (TTPA). This work facilitates the user to store their data as blocks and enables them to perform dynamic operations on blocks. The stored data can be accessed by a group of users authorized by the data owner. The owner has the privilege to grant or revoke access of the stored data in the cloud. The present system is providing a good security mechanism for stored data and proper sharing of keys among authorized users, and data owner for the cryptographic mechanism.

Key Terms - Mutual trust, access control, dynamic environment, outsourcing data storage

1. INTRODUCTION

Cloud computing has received considerable attention from both academia and industry due to a number of important advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks. Cloud computing is a distributed computational model over a large pool of shared virtualized computing resources (e.g., Storage, processing power, memory, applications, services, and network bandwidth). Cloud service providers (CSPs) offer different classes of services (Storageas-a-Service (SaaS), Application-as-a-Service, and Platformas-a-Service) that allow organizations to concentrate on their core business and leave the IT operations to experts. In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data.

Presently, the amount of responsive data formed by many organizations is outpacing their storage ability. The organization of such massive amount of data is quite exclusive due to the necessities of high storage space capacity and capable personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid capability 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.

The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel.

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 373-378

Therefore, Storage-as-a-Service offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. Through outsourcing data storage scenario, data owners delegate the storage and management of their data to a CSP in exchange for pre-specified fees metered in GB/month. Such outsourcing of data storage enables owners to store more data on remote servers than on private computer systems. Moreover, the CSP often provides better disaster recovery by replicating the data on multiple servers across multiple data centers achieving a higher level of availability. Thus, many authorized users are allowed to access the remotely stored data from different geographic locations making it more convenient for them.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. For the application purposes, the user cooperates with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are allowing for are block update, delete, insert and append.

The data owners lose the control over their responsive data once the latter is outsourced to a remote CSP which may not be trustworthy. This lack of control raises new dreadful and challenging tasks related to data confidentiality and integrity protection in cloud computing. Customers require that their data remain secure over the CSP. Also, they need to have a strong proof that the cloud servers still possess the data and it is not being tampered with or partially deleted over time, especially because the internal operation details of the CSP may not be known to cloud customers.

2 RELATED WORKS

Existing research work can be found in the areas of integrity verification of outsourced data, data storage security on untrusted remote servers and access control of outsourced data.The term cloud had already come into commercial use in the early 1990s to refer to large Asynchronous Transfer Mode networks. By 21st century, he term ‘‘cloud computing’’ had appeared, although major focus at this time was on Software as a Service (SaaS). In 1999, sales- force.com was established by Parker Harris, Marc Benioff. They applied many technologies of consumer web sites like Google and Yahoo! to business applications. They also provided the concept’s like ‘‘On demand’’ and ‘‘SaaS’’ with their real business and successful customers. Cloud data storage (Storage as a Service) is an important service of cloud computing referred as Infrastructure as a Service (IaaS). Amazon’s Elastic Compute Cloud (EC2) and Amazon Simple Storage Service(S3) are well known examples of cloud data storage. On the other side along with these benefits’ cloud computing faces big challenge i.e. data storage security problem, which is an important aspect of Quality of Service (QoS). Once user puts data on the cloud rather than locally, he has no control over it i.e. unauthorized users could modify user’s data or destroy it and even cloud server collude attacks. Cloud users are mostly worried about the security and reliability of their data in the cloud. Amazon’s S3 [1] is such a good example.
Existing work related to our proposed work can be found in the areas of integrity verification of remotely stored data and file encryption schemes in distributed systems and access control mechanisms over outsourced data. Ateniese et al. [4] designed a model based on PDP (Provable Data Possession) protocol which allows a client to verify the server’s data possession. In this scheme the client preprocesses the file and generates meta-data, stores it locally, and then outsource the file to the server. The server stores the file and starts respond to challenges issued by the client. Integrity verification is done through batch verification of Homomorphic hash functions.

3. OUR SYSTEM AND ASSUMPTIONS

3.1 System components and relations

3.1.1 Data owner

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

ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 373-378

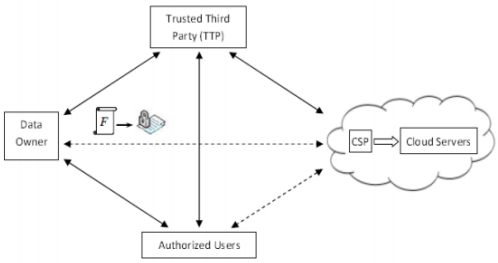

Fig 1: Cloud computing data storage system model

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 that 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.

3.2 Outsourcing and accessing

For confidentiality, the owner encrypts the data before sending to cloud servers. To access the data, the authorized user sends a data-access request to the CSP, and receives the data file in an encrypted form that can be decrypted using a secret key generated by the authorized user. 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 is an independent entity, and thus has no incentive to collude with any party. However, any possible leakage of data towards the TTP must be prevented to keep the outsourced data private. The TTP and the CSP are always online, while the owner is intermittently online. The authorized users are able to access the data file from the CSP even when the owner is offline.

3.3 Threat model

The CSP is untrusted, 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 defense

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

4. SECURITY ANALYSIS

4.1 Data confidentiality

The outsourced data are kept secret; the data owner creates an encrypted version of the data file F. The encryption of a file is done using a secret key K generated by owner, where K is accessed only by the data owner and the authorized users.

4.2 Detection of data integrity violation

Due to pre image and second-pre image resistance properties of the used cryptographic hash function h along with the non collusion incentive of the TTP, the data cannot be corrupted on cloud servers without being detected.

5. IMPLEMENTATION AND

EXPERIMENTAL EVALUATION

5.1 Implementation

We have implemented the proposed scheme on top of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3) [26] cloud platforms. Our implementation of the proposed scheme consists of four modules: OModule (owner module), CModule (CSP module), UModule (user module), and TModule (TTP module). OModule, which runs on the owner side, is a library to be used by the owner to perform the owner role in the setup and file preparation phase. Moreover, this library is used by the owner during the dynamic operations on the outsourced data. CModule is a library that runs on Amazon EC2 and is used by the CSP to store, update, and retrieve data from Amazon S3. UModule is a library to be run at the authorized users' side, and include functionalities that allow users to interact with the TTP and the CSP to retrieve and access the outsourced data. TModule is a library used by the TTP to perform the TTP role in the setup and file preparation phase. Moreover, the TTP uses this library during the dynamic operations and to determine the cheating party in the system.

5.2 Experimental Evaluation

Here we describe the experimental evaluation of the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with static data with only confidentiality requirement.

CSP computation overhead: As a response to the data access request, the CSP computes two signatures: σF and σT . Thus, the computation overhead on the CSP side due to data access is about 6.04 seconds and can be easily hidden in the transmission time of the data (1GB file and 2MB table).

Owner computation overhead: To experimentally evaluate the computation overhead on the owner side due to the dynamic operations, we have performed 100 different block operations (modify, insert, append, three times, each time with a different revocation percentage. In the first time, 5% of 100 dynamic operations are executed following revocations.

6. CONCLUSIONS

The cloud based storage scheme is proposed that allows owner to benefit from facilities offered by the CSP and enables indirect mutual trust between them. It enables 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/users or CSP).In this Paper, we have envisaged a 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. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a TTPA is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. The experimental results show that the proposed scheme is a robust model in terms of security.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[2] F. Sebe,´ 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.

[3] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[4] C. Erway, A. Kupc¸ ¨u,¨ C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Confer-ence on Computer and Communications Security, 2009, pp. 213–222.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in

Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[6] A. F. Barsoum and M. A. Hasan, "Provable possession and replication of data over cloud servers," Centre For Applied Cryp-tographic Research, Report 2010/32, 2010, http://www.cacr.math. uwaterloo.ca/techreports/2010/cacr2010-32.pdf.

[7] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: multiple-replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.

[8] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multi-ple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[9] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[10] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography, 2009.

[11] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT '08, 2008, pp. 90–107.

[13] 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.

[14] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proceedings of the Network and Distributed System Security Symposium, NDSS, 2003.

[15] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in NDSS, 2005.

[16] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123–134.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[18] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10, 2010, pp. 534–542.

[19] 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.

[20] K. E. Fu, "Group sharing and random access in cryptographic storage file systems," Master's thesis, MIT, Tech. Rep., 1999.

[21] 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.

[22] M. Backes, C. Cachin, and A. Oprea, "Secure key-updating for lazy revocation," in 11th European Symposium on Research in Computer Security, 2006, pp. 327–346.

[23] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Advances in Cryptology - CRYPTO, 2005, pp. 258–275.

[24] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, London, UK, 2001, pp. 514–532.

[25] P. S. L. M. Barrio and M. Naehrig, "IEEE P1363.3 submission: Pairing-friendly elliptic curves of prime order with embedding degree 12," New Jersey: IEEE Standards Association, 2006.

[26] Amazon Web Service, http://aws.amazon.com/.

[27] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in Proceedings of SAC 2005, volume 3897 of LNCS. Springer-Verlag, 2005, pp. 319–331.

[28] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable

data transfer," Cryptology ePrint Archive, Report 2006/150, 2006.

[29] D. Naor, M. Naor, and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '01. Springer-Verlag, 2001, pp. 41–62.

[30] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in EUROCRYPT, 1998, pp. 127–144.

[31] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proceedings of the 12th ACM Conference on Computer and Communications Security, ser. CCS '05. ACM, 2005, pp. 190–202.

[32] J. Fangs, Y. Chen, W.-S. Ku, and P. Liu, "Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms," in Proceedings of the 2010 39th International Conference on Parallel Processing, 2010, pp. 251–258.

[33] J. Fangs, Y. Chen, and D. H. Summerville, "A fair multi-party non-repudiation scheme for storage clouds," in 2011 International Conference on Collaboration Technologies and Systems, 2011, pp. 457– 465.