I J C T A, 9(37) 2016, pp. 89-94

Code Certificate – A Verification Technique for Secure Data Transmission

S. Selvakumar[*] and M.R. Keerthi[**]

Abstract: Cloud Computing is one of the latest technology which consists of shared pool of configurable resources. It also allows users' to store their data, access and retrieve data. The data stored in public cloud can be viewed and accessed by everyone. At times the user can set privacy settings, such that only authorized user can access the data. In case of private cloud, the data stored by the user is accessible only to the data owner. In case of data storage, security and privacy issues are possible. So, in order to secure and protect data, various techniques and methodologies are proposed. This paper describes about the use of code verification and use of code certificate in order to perform secure and trusted sharing of data transmission.

Keywords: Cloud computing, Security, Privacy, Code Verification, Code Certificate, Data.

1. INTRODUCTION

Cloud computing is an emerging technology where the data are stored in the cloud storage service and its being fetched by the tenants or the customers where they enjoy the services offered in this blooming technology. In a nut shell public cloud can be accessed by every user, private cloud is used by pay as per usage for the organizations, hybrid cloud is the combination of both public and private cloud where the organization manages the data or the resources in the cloud storage service and provides them to the tenants or the customers. The main aim is to provide proper security to data that is stored by the user. As, security is the most important concern in the cloud computing, several algorithms, security mechanisms and other techniques are being implemented to enhance security.

The services offered and working mechanism for each cloud varies. **Public cloud** is a common cloud computing model whereby a service provider makes resources like software and data storage available over the Internet, a **private cloud** allows customers the benefits of cloud computing like self-service, automation, consolidation and metered usage but behind the safety of their firewall on their own virtual private network, a **hybrid cloud** is a cloud computing environment in which an organization provides and manages some resources in storage and has others providers externally. A **Dynamic hybrid cloud** is a model that supports truly dynamic and hybrid cloud environments by leveraging existing public and private cloud solutions. "*The goal is to provide a nonintrusive environment that could run anywhere, anytime in the most optimized way, leveraging existing public and private cloud environments.*"

The attributes of cloud are its use of internet-based services to support business process and rent IT-services on a utility-like basis rapid deployment, low startup costs/capital investments, costs based on usage or subscription, multi-tenant sharing of services/resources, on demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, measured service.

The data in the private cloud is managed by the **Third Party Auditor (TPA)**. The Third Party Auditor audits and maintains the data stored in the private cloud. The auditing or the verification is done in order to check the data integrity of the tenant or the customer. The Third Party Auditor performs auditing or verification in an efficient way such that there is no leakage of data.

[*] Department of CSE, SRM University

[**] M. Tech Computer Science and Engineering, SRM University

2. RELATED WORKS

In [1] the authors state that inside threats are possible still having advance firewall and security. The security issue occurs when external customers can store their data in cloud in which any employee in the cloud could manage the misuse of the data. The data stored in the cloud will exhibit a high level of availability. The data stored in the cloud can be accessible only to the user who owns the data. The authorization and authentication, password protecting are maintained for access control. If an attacker can get the control of the operating system then they control all the host operating system functions. To protect the host operating system from the attacker, the minimal operating system is chosen to be stripped for all unnecessary service.

In [2], the authors express that data should be backed up as well as appropriate level of data mirroring is implemented. Firewalls are implemented to prevent information which resides in the cloud from DDos and Dos attacks.

The authors in [3] focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, authors propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Juels et al. [4] described a formal "proof of retrievability" (POR) model for ensuring the remote data integrity. Their scheme combines spot-cheking and error-correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al.

Ateniese et al. [5] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags for auditing the data file, thus providing public verifiability. However, their scheme requires sufficient computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. [6] described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not address small data corruptions, leaving both the distributed scenario and data error recovery issue unexplored.

3. PROBLEM DESCRIPTION

There are several security issues that are faced by data owners. Security issues arises when there is no proper authentication and authorization mechanisms. By using cloud services, users can easily access their personal information and make it available to various services across the Internet. While users interact with a front-end service, this service might need to ensure that their identity is protected from other services with which it interacts.

In this paper, we will be discussing about certain challenges that occurs in cloud computing environment. They are authentication, identity management, access control and accounting.

Authentication is the process of confirming with the given attribute of an entity is true or not. Authentication is performed in order to verify the identity of the user. Verifying a person's identity is done in order to ensure secure access of confidential data and other resources.

Authentication is broadly classified into three types and its as follows. The first type of authentication is based on accepting the proof of identity, the second type of authentication is based on comparison of attributes of objects itself. At times attribute comparison may be vulnerable to forgery. In general, creating an indistinguishable object as an attribute for authentication requires expert knowledge. The third type of authentication relies on the documents and other external affirmations.

Authentication can be done based on certain factors referred to as **authentication factors**. These factors include knowledge factor, ownership factor and inherence factor. Authentication plays an vital role in securing data which is one of the prime challenge.

Identity Management is the next challenge in designing a cloud environment. It describes the management of individual principles and privileges within or across the enterprise boundaries in order to increase and maintain security. In other words identity management is the process of controlling information about the users. It includes the information that authenticates the identity of the user.

It also includes information that describes information and actions and also the management of descriptive information about the user. Identity management is also considered to be an important factor as it restricts the user for accessing the data stored in the cloud.

Access Control is the process of restricting the user's accessing limit. Only authorized users are allowed to access the data stored in the cloud. Access control policies can be defined based on user's security criteria. Authentication and access control are often combined into a single operation. Access controls are defined based on certain policies that are defined by user. **Accounting** is the process of accounting the actions that takes place during transaction of data. It helps in maintaining the data owner, to identify the users who access, or use the data.

Secure service management deals with management of security services that are necessary for the user. The service integrator provides a platform that lets independent service providers and interwork services and cooperatively provide additional services that meet customers' protection requirements.

Privacy and data protection deals with the process of providing privacy for user data. Several privacy policies are defined in order to maintain security for the user data. Many organizations aren't comfortable storing their data and applications on systems that reside outside of their data centres. Privacy-protection mechanisms must be embedded in all security solutions.

4. SYSTEM MODEL

Authentication and Identity Management is done by using cloud services, users can easily access their personal information and make it available to various services across the Internet. An identity management (IDM) mechanism can help authenticate users and services based on credentials and characteristics.

Access Control and Accounting demand fine-grained access control policies in cloud environment. In particular, access control services should be flexible enough to capture dynamic, context, or attribute- or credential-based access requirements and to enforce the principle of least privilege. Such access control services might need to integrate privacy-protection requirements expressed through complex rules.

Secure service management is based on customers' security protection which is a necessary one, because security is the highest concern of all the users' of application.

Privacy and data protection is the process of defining necessary privacy policy for protecting data. Users' are more concerned about their data stored in the cloud.

4.1. System Architecture

There are several techniques to ensure secure transfer of data between public and private cloud. To make sure that the data transmitted is secure, several methodologies, algorithms and encryption standards are performed. One among them is the use of **code certificate.**

a) **Code Certificate Generation:** Code Certificate is not same as digital certificate. To create a code certificate it requires *p* number of hexa-decimal based random numbers (*q* size). It makes a group among the random numbers and generates the code certificate.

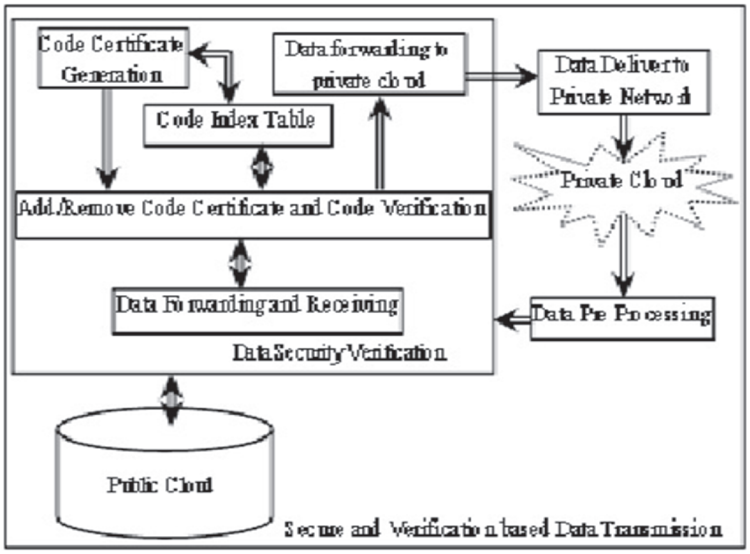
Code Certificate Generation
Data forwarding to private cloud
Data Deliver to Private Network
Code Index Table
Private Cloud
Add/Remove Code Certificate and Code Verification
Data Forwarding and Receiving
Data Pre Processing
Data Security Verification
Public Cloud
Secure and Verification based Data Transmission

Figure 1: System Architecture

b) **Index Table:** During the transmission the code certificate is required to binding the input message as well as to remove the code certificate when the message is received. Code Index Table is used to easy way maintain those code certificate and its sequence according with its index.

c) **Data Forwarding:** The original input message is delivered to the private cloud after the validation is over. Before the message to be delivered, all the code certificates are removed from those received message from the public cloud.

d) **Add/Remove:** Add/Remove Code Certificate and Code Verification is the main component of this system. It adds the code certificate based on the sequence of the code index in the input message which is received from the private cloud. It removes the code certificate based on the sequence of the code index in the output message which is received from the public cloud before transmit to the users. To add more security on the message we use digital signature on it.

e) **Data Transmission:** Data Transmission includes data forwarding and receiving and this acts like a interface between the public and the private cloud. All the communications are done through this module for secure and verification based data transmission .That is this makes the connection between the public and the private cloud.

In order to make secure data transmission between public and private cloud code certificate is used. For each code certificate that is generated a reference value is generated and this is stored in index table. This makes the transmission of data more secure.

5. CONCLUSION

Thus the use of code certificate in this system architecture ensures secure and trusted transmission of data between public and private cloud based on code verification. The code generator generates the code certificates where random set of numbers are generated in it. The code certificate must match with the code index table with which the verification process is performed. The user can only generate the code certificates corresponding to the data accessed which ensures data integrity. The data from the public cloud transferred to the private cloud, consists of the code certificate along with it for verification. When the data is being stored in the private cloud the code certificates are being removed denoting that the data is being securely transferred if not then security issue arises. From the private cloud the data is being preprocessed to the data security verification.

During the retrieval of data, the user has to submit the code certificate value, which should match with the code certificate attached to the data. If it matches, then the data owner will be able to retrieve data and view it. Even though the security is maintained, there are still possibilities for attacks to takes place as cloud computing is an emerging technology and it has its own pros and cons.

References

1. Eystein Mathisen (2011) "*Security challenges & solutions in cloud computing*" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST), Daejeon, Korea.
2. Gurudatt Kulkarni & Jayant Gambhir, Tejswini Patil, Amruta Dongare (2012) "*A security aspect in cloud computing*" 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS).
3. Cong Wang, Qian Wang, and Kui Ren AND Wenjing Lou Ensuring Data Storage Security in Cloud Computing
4. A. Juels and J. Burton S. Kaliski, "*PORs: Proofs of Retrievability for Large Files*," *Proc. of CCS '07*, pp. 584–597, 2007.
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "*Provable Data Possession at Untrusted Stores*," *Proc. Of CCS '07*, pp. 598–609, 2007.
6. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "*Scalable and Efficient Provable Data Possession*," *Proc. of SecureComm '08*, pp. 1–10, 2008.
7. Varadharajan. V & Tupakula. U, '*Security as a Service Model for Cloud Environment*', IEEE Transactions on Network and Service Management, Vol. 11, No. 1, pp. 60-75, 2014.
8. C. Wang, S.S.M. Chow, Q. Wang, K. Ren & W. Lou, '*Privacy-Preserving Public Auditing for Secure Cloud Storage*', IEEE Transactions on Computers, Vol. 62, No. 2, pp. 362-375, 2013.
9. A. Juels and J. Burton, S. Kaliski, "*PORs: Proofs of Retrievability for Large Files*," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, 2007.
10. M.A. Shah, R. Swaminathan, and M. Baker, "*Privacy-Preserving Audit and Extraction of Digital Contents*," Cryptology ePrint Archive, Report 2008/186, 2008.
11. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "*MR-PDP: Multiple- Replica Provable Data Possession*," *Proc. of ICDCS '08*, pp. 411–420, 2008.
12. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage,
13. Arockiam Lawrence, Amalraj Irudayasamy, Enhanced Algorithm for Data Privacy Preservation using Data Anonymization with Low Information Loss in Public cloud, International Journal of Intelligent Computing Research (IJICR), Volume 5, Issues 3/4, Sep/Dec 2014.
14. N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "*LT Codes-Based Secure and Reliable Cloud Storage Service*," Proc. IEEE INFOCOM, 2012.
15. B. Wang, B. Li, and H. Li, "*Certificateless Public Auditing for Data Integrity in the Cloud*," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013.
16. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "*Remote Data Checking for Network Coding-Based Distributed Storage Systems*," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.
17. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "*Privacy-Preserving Public Auditing for Secure Cloud Storage*," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362-375, Feb. 2013.
18. B. Wang, B. Li, and H. Li, "*Public Auditing for Shared Data with Efficient User Revocation in the Cloud*," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.
19. B. Wang, H. Li, and M. Li, "*Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics*," Proc. IEEE Int'l Conf. Comm. (ICC'13), pp. 539-543, 2013.
20. D. Boneh, X. Boyen, and H. Shacham, "*Short Group Signatures*," Proc. 24th Ann. Int'l Cryptology Conf. (CRYPTO'04), pp. 41-55, 2004.

21. B. Wang, B. Li, and H. Li, "*Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud*," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS'12), pp. 507-525, June 2012.

22. B. Wang, B. Li, and H. Li, "*Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud*," IEEE Trans. Services Computing, 20 Dec. 2013, DOI: 10.1109/TSC.2013.2295611.

23. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "*Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.

24. E. Brickell, J. Camenisch, and L. Chen, "*Direct Anonymous Attestation*," Proc. 11th ACM Conf. Computer and Comm. Security (CCS'04), pp. 132-145, 2004.

25. D. Boneh, B. Lynn, and H. Shacham, "*Short Signatures from the Weil Pairing*," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001.

26. D. Cash, A. Kupcu, and D. Wichs, "*Dynamic Proofs of Retrievability via Oblivious RAM*," Proc. 32nd Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 279-295, 2013.

27. X. Liu, Y. Zhang, B. Wang, and J. Yan, "*Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud*," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 6, pp. 1182-1191, June 2013.

28. S. Yu, C. Wang, K. Ren, and W. Lou, "*Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing*," Proc. IEEE INFOCOM, pp. 534-542, 2010.

29. A. Juels and B.S. Kaliski, "*PORs: Proofs of Retrievability for Large Files*," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 584-597, 2007.

30. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "*Scalable and Efficient Provable Data Possession*," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm'08), 2008.