ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Review Article

A SECURED CODE VERIFIED DATA MANIPULATION AND TRANSMISSION USING CLOUD

A.Tharma Jeyaseeli[a,b*], **S.Selvakumar**[a]
[a] Department of Computer Science, SRM University, Chennai, Tamil Nadu, India
[b] Department of Computer Science, SRM University, Chennai, Tamil Nadu, India
Email:jeyaanbuchelian93@gmail.com

Received on 10-11-2016 *Accepted on: 29-11-2016*

Abstract

A cloud computing is a large network of servers that are remote in nature on the internet that is useful in storing and managing the repository of data rather than in a personal computer or a local server. This technology has reduced the cost of computation, hosting of applications, storage and delivery will be reduced. Cloud computing is the approach that provides the cost benefits and it has the ability of transforming a data center to an environment which is alterable. Cloud computing is based on the idea of reusing the IT capabilities. Compared to distributive computing, grid computing, autonomic computing and utility computing the cloud computing is different in terms of its wide boundary across the organizations. The stored data in public cloud can be accessed and viewed by everyone. At times the user can set privacy settings, such that only authorized user can access the data.

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

1. Introduction

The computing of service is achieved through the internet with the help of cloud computing. The hardware and software that are maintained by the third party at inaccessible locations can be used by individuals and business enterprises. Some of the examples are online business applications, social networking sites and online file storage. The information can be accessed for anywhere if a network connection is available in that place. A number of resources are being provided in cloud computing that includes the storage space of data, power of computer processing, highly skilled corporate and consumer applications. A convenient network access is enabled to a repository of computing resources that can be supplied quickly and distributed with less management activity. A cloud computing is a combination of deployment models, essential characteristics and service models. Cloud computing characteristics includes self service when required, fast adaptability, broad network approach, resource pooling. Required self service means that the customers can demand and bewield their own resources. Broad network approach allows services to be proposed over the internet and networks that are private. Pooled resources means that customers withdraw from a repository of computing resources, mostly in distant data centers. Services can be either larger or smaller; and the use of a service is noted and customers are charged based on that. Cloud Computing is operating, set up or arranging and using the applications online. Online data repository, applications and infrastructure are provided here. The Cloud Computing makes a business application a grouped one and free or movable. The **Public Cloud** is where the systems and services are easily accessed by the public. Public cloud is less secured because of its transparency, e.g., e-mail. The **Private Cloud** is where the systems and services are accessed within an organization. It is highly secured because of its private nature. The **Community Cloud** is where the systems and services are accessed by group of organizations. The **Hybrid Cloud** is a combination of public and private cloud. The difficult activities are performed using private cloud where as the easy activities are performed using public cloud.

2. Related Work

In [1] the author states that more users store their data and application on the cloud because of the tremendous development in Cloud computing. Cloud security problems are the major reasons for the developments made in cloud computing. Certain characteristics are being maintained by the cloud computing and they includes virtualization, multi-user, scalability and so on. As a result of these new characteristics the traditional security technology cannot make the cloud a safe one. Therefore, most of the research is based on the cloud computing security. In order for the problem to be solved in data security in cloud computing a fully homomorphism encryption algorithm has been introduced, a new data security solution is proposed for the insecurity of the cloud computing and the concepts of this application is then built. This new security solution is useful in the retrieval and processing of the encrypted data and leads the broad to be an applicable one, the security of the transmitted data and the storage. In [2] the author states that the increased usage of cloud computing applications everywhere enhances the advent of cloud computing platform for users, the data exchange between the users, data storage and transmission as a security threat, a cloud computing security are the problems to be solved. In this paper, the state of encryption technology provides a solution for cloud computing data security for safe data transmission and security. In [3] the author describes that this paper establishes the relation between network coding and cloud storage. Secure cloud storage is a recent study whereas secure network coding is there for more than ten years. It shows how the construction of a secure cloud storage protocol with any random secure network coding protocol. This suggests an effective way of construction of different secure cloud storage protocols. It also denotes that it is secured highly using a definition which takes the real world uses of the cloud storage. The general construction proposes a secure cloud storage protocol with the help of recent secure network coding protocol. This protocol is a publicly verifiable and secured cloud storage protocol , whereas the previous work is not publicly verifiable and also security argument is only argued heuristically here(random oracle model). This also enhances the third-party public auditing, which has a growing attention nowadays.

3. Problem Description

Cloud computing has a vast number of challenges in different places which made it an emerging technology. Some of them are described as follows.

***Security and privacy*:** Security and privacy is considered as one of the biggest challenge in cloud computing. It is mostly used in preserving the privacy of the users and providing security. This is achieved by using the encryption techniques and secured hardware and applications.

Portability: The portability is also a challenge that deals with the movement of data from one cloud service provider to the other. A vendor lock-in should not occur at any case. But still it is unachievable because of the service providers who use different languages.

Interoperability: This challenge is about the working of an application from one platform in another platform. It is achieved with the help of web services but they are complicated.

Computing performance: For the delivery of an intensive application in a cloud usually a high bandwidth is needed and in case of avoiding that a low bandwidth is used but this does not reaches the expected computation level.

Reliability and availability: It is necessary for a service to be reliable and available i.e. it must be available to all users who are authorized.

Authentication: Nowadays one of the major threats to security is the authentication of unauthorized users. In order to avoid that the users are asked for some details and if the given detail matches with the already existing details then they are provided with authentication.

4. System Model

Authenticity and Selfhood Management is done with the help of the cloud services where the users are allowed to easily access or use their data and they can also share it with the public if they wish. Authorized users are identified with the help of identity management process.

Accounting and Controlling of Access describes about the easy access of data and services i.e. it must be flexible so that it is easy to obtain all the requirements of the users.

Security management deals with the security provided in a service. This plays a vital role in a private environment where the user's private data are maintained in a highly secured way.

Data safety and security is where the data is protected and safeguarded and is kept in the data repository in a highly secured manner i.e. the privacy of the user is maintained here.

Data Manipulation or consumption is the process of using the data provided in the cloud. The user when needed can upload or download any files from the cloud using the secret code. The files include audio, video files, images, documents, etc.

4.1. System Architecture:

A number of techniques are used for the safe transmission of data from a public cloud to a private cloud. One of the effective methods is the code certificate generation where a code is generated for security purpose.

Generation of a passcode i.e. a code certificate: Code Certificate is much unsimilar from a digital certificate. A 'p' number of hexa-decimal random numbers of size 'q' are used to create a code certificate. It is generated randomly by grouping method.

Database Index:

When a data or message is to be transmitted the code binds with it when it is encrypted and is also removed when decrypted at the receiver end. Database Index is used for maintaining those code certificates along with its sequence according to the index.

Data Dispatching:

Once the validation is over the message is sent to the private cloud. Before the delivery of the message to the user the code certificates are removed from the message from public cloud.

Adding and Removal of code certificate:

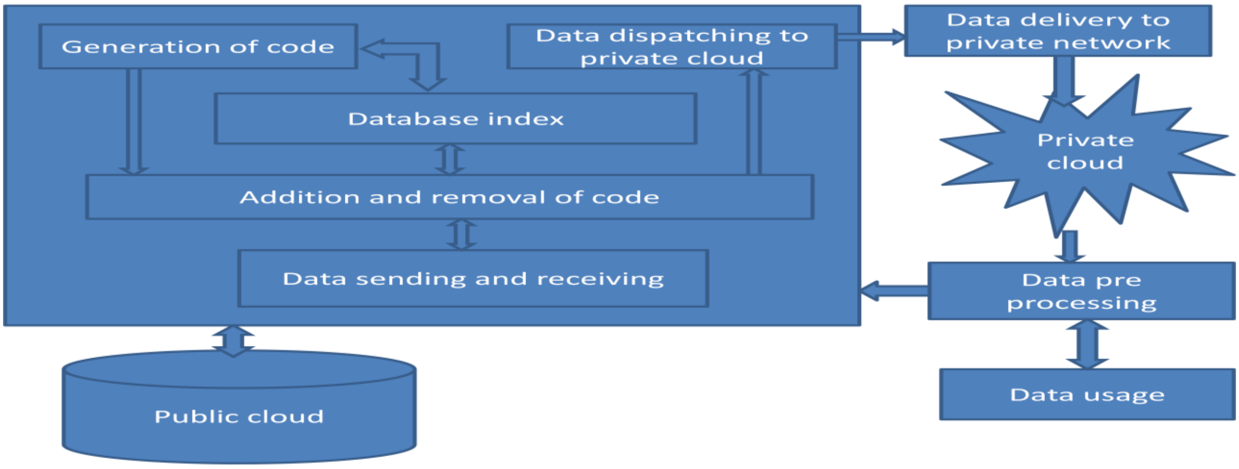
The addition and removal of codes from the message is the concept of this component. Codes are added to the message according to the sequence keys that are generated. The code certificate is removed depending on the sequence of the code index available in the output messages that are sent from the public cloud. In order to tighten the security digital signatures are used.

Data Remission:

Data Remission includes the sending and receiving of data and it acts as a bridge between the public and the private cloud. Communication is done with the help of this module between the service providers. It establishes connection between the private and public cloud. The transmission of data becomes an effective one with the help of the code certificates.

Data Manipulation/Consumption:

Data manipulation or consumption is a component where the user obtains a secured environment (i.e.) the private data are secured and maintained confidentially and the user can anytime download or upload data in a secured way.


Generation of code
Data dispatching to private cloud
Data delivery to private network
Database index
Private cloud
Addition and removal of code
Data sending and receiving
Data pre processing
Public cloud
Data usage

5. Conclusion

The safeguarded transmission of data which may be a document or an image or an audio file or a video file is done effectively with the help of the code certificates. Similarly the user can consume the data available to the user and the user can manipulate it with the help of authentication process. Only authenticated users who are provided with a particular detail which includes user name and password are allowed for the consumption or usage of data. A normal user can view only the page whereas an authenticated user can move forward with the help of authentication process and can use the data. The users have the options for viewing the data using it and downloading it when needed .This consumption of data is achieved only after the code verification process either.

6. 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, June2013.
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.