International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Security and Privacy for Storage and Computation in Cloud Computing

K. Sharmila[1], V. Vinoth Kumar[2]

[1]ME-CSE, Kingston Engineering College, Vellore, India

[2]Assistant Professor -CSE, Kingston Engineering College, Vellore, India

Abstract: ***The Secure Data Sharing in Clouds (SeDaSC) methodology that provides:data confidentiality and integrity, access control, data sharing (forwarding) without using compute-intensive re-encryption, insider threat security, and forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations.***

Keywords: Confidentiality, Integrity, Forward-Backward Access Control, Thread Security, Asymmetric Key.

1. Introduction

Cloud computing is elastic, flexible, and on-demand storage and computing services for customers. The data are usually encrypted before storing to the cloud. The access control, key management, encryption, and decryption processes are handled by the customers to ensure data security. A single key shared between all groups members will result in the access of past data to a newly joining member. A separate key for every user is a cumbersome solution. The data must be separately encrypted for every user. The changes in the data require the decryption of all of the copies of the users and encryption again with the modified contents, a methodology named Secure Data Sharing in Clouds (SeDaSC).The SeDaSC methodology works with three entities as follows: Users, A cryptographic server (CS), Cloud.

2. Literature Survey

A body of literature has been conducted by several authors and a list of them is given below;

1. Security and Privacy Issues in Cloud Computing
Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. We discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment. We discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a briefpresentation on the future trends in cloud computing deployment.

2. A systematic literature review of cloud computing in e-health.
A systematic literature review requires a comprehensive and unbiased coverage of searchedliteratures. To maximize the coverage of our searched literatures, we started by identifying some of the most used alternative words/concepts and synonyms in the research questions. Weconducted first a manual search in the areas of related areas such as computer science. Since one of the most significant advantages of cloud computing is its huge data storage capacity, six papers proposed cloud-based frameworks. High accessibility, availability and reliability make cloud computing a better solution for interoperability problems. Papers in this category mostly applied cloud technology for secured data sharing, processing and management, and can be categorized based on three types of cloud platforms, namely, public cloud, private cloud and hybrid cloud.

3. An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art.
Cloud monitoring activity involves dynamically tracking the Quality of Service (QoS) parameters related to virtualized resources. Applications and resources configuration in cloud computing environment is quite challenging considering a large number of heterogeneous cloud resources. The fact that at each point of time, there will be a different and specific cloud service may be massively required. Cloud monitoring tools can assist a cloud providers or application developers in:

a) Keeping their resources and applications operating at peak efficiency.
b) Detecting variations in resource and application performance.
c) Accounting the Service Level Agreement (SLA) violations of certain QoS parameters.
d) Tracking the leave and join operations of cloud resources due to failures and other dynamic configuration changes.

4. An efficient certificateless encryption for secure data sharing in public clouds.
It explains a mediated certificate less encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Existing mCL-PKE schemes are either inefficient because of the use of expensive pairing

operations or vulnerable against partial decryption attacks. Our mCL-PKE scheme constructs a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon successful authorization, the cloud partially decrypts the encrypted data for the users. The confidentiality of the content and the keys is preserved with respect to the cloud, because the cloud cannot fully decrypt the information. An extension to the above approach is to improve the efficiency of encryption at the data owner.Our mCL-PKE scheme and the overall cloud based system, and evaluate its security and performance. Our results show that our schemes are efficient and practical.

5. Efficient and provably-secure group key management scheme using key derivation.

The rapid developments of the Internet in many commercial and network-based services, such as pay-TV and on-line games have become popular. To control access to these services for legal members only, a common way is to use a cryptographic key to protect the communication and disclose the key only to the group of legal members. The group key management (GKM) is for a group manager to maintain a common cryptographic (group) key for a dynamic group of legal members through a network channel. A GKM scheme can also be used to provide communication privacy and transmitted message integrity. In this paper, we first demonstrate a collusion attack against Chen, et al.'s concrete RSA-based GKM scheme. Then, we have an efficient and provably-secure GKM scheme using the key derivation method. Our GKM scheme has some attractive features. Firstly, the proposed scheme is very efficient since the key derivation method uses simple keyed hash plus XOR operations. Secondly, the proposed scheme have an efficient rekey mechanism for a member who may become off-line and miss group key updates in his off-line period. Finally, the proposed scheme can be proved secure based on the pseudorandom function family assumption and one-way property of a hash function.

6. Ensuring Data Storage Security in Cloud Computing.

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, Together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale.

7. Attribute Based Group Key Management.

Attribute based systems enable fine-grained access control among a group of users each identified by a set of attributes. Secure collaborative applications need such flexible attribute based systems for managing and distributing group keys. However, current group key management schemes are not well designed to manage group keys based on the attributes of the group members. In this paper, we propose novel key management schemes that allow users whose attributes satisfy a certain access control policy to derive the group key. Thus data must be encrypted with keys made available only to the members of the group. The management of these keys, which includes selecting, distributing, storing and updating keys, should directly and effectively support the attribute-based group dynamics and thus requires an attribute-based group key management (AB-GKM) scheme, by which group keys are assigned.

8. Efficient Provably-Secure Hierarchical Key Assignment Schemes.

A hierarchical key assignment scheme is a method to assign some private information and encryption keys to a set of classes in a partially ordered hierarchy, in such a way that the private information of a higher class can be used to derive the keys of all classes lower downin the hierarchy. A hierarchical key assignment scheme is a method to assign an encryption key and some private information to each class in the system. The encryption key will be used by each class to protect its data by means of a symmetric cryptosystem, whereas, the private information will be used by each class to compute the keys assigned to all classes lower down in the hierarchy. This assignment is carried out by a Trusted Authority.

9. Provably Secure Group Key Management Approach Based upon Hyper-sphere.

Secure group communication systems have become increasingly important for many emerging network applications. Robust group key management approach is indispensable to a secure group communication system. Motivated by the theory of hyper-sphere, this paper presents a new group key management approach with a group controller GC. The distance from any point on the hyper-sphere to the central point of the hyper-sphere is identical. Inspired by this principle, a secure group key management scheme is designed. The most significant advantages of the proposed approach are the reduction of user storage, user computation, and the amount of update information while re-keying.

10. An Efficient and Secure Multicast Key Management Scheme based on Star Topology.

The proposed scheme preserves the forward secrecy and backward secrecy in multicast group key management and therefore, is more secure. In addition, it also eliminates the rekeying process whenever a member joins/ leaves a group. Group key management plays an important role in group communication. A common group key is required for individual users in the group for secure multicast communication. Group key has to be updated frequently whenever a member joins and leaves in order to provide forward and backward secrecy. It is difficult to obtain the private key d from publicly available parameter, similar to the difficulty of factoring the largeintegers as in RSA algorithm. Therefore, the security of theproposed scheme depends on RSA cryptosystem.

3. Conclusion and Future Enhancement

SeDaSC methodology is a cloud storage security scheme for group data. The proposed methodology provides data confidentiality, secure data sharing without Re-encryption, access control for malicious insiders, and forward and backward access control. In the future, the proposed methodology can be extended by limiting the trust level in the CS. This will further enhance the system to cope with insider threats. Moreover, the response of the methodology with varying key sizes can be evaluated.

4. Acknowledgement

I would like to take this opportunity to express my profound gratitude and deep regard to my guide, *Prof.V.Vinothkumar, Kingston Engineering College*, for his exemplary guidance, valuable feedback and constant encouragement in completing this paper. His valuable suggestions were of immense help in getting this work done. Working under his, was an extremely knowledgeable experience. Also, I would like to extend my sincere gratitude to my parentsfor their constant support and encouragement in completing this paper.

References

[1] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 1431–1441, Jul. 2014.
[2] K. Alhamazani*et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*, DOI: 10.1007/s00607-014-0398-5, 2014, to be published.
[3] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Gen. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul. 2013.
[4] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inf. Sci.*, vol. 258, pp. 371–386, Feb. 2014.
[5] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.
[6] D. Chen *et al.*, "Fast and scalable multi-way analysis of massive neural data," *IEEE Trans. Comput.*, DOI: 10.1109/TC.2013.2295806, 2014, to be published.
[7] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band, "Incremental proxy re-encryption scheme for mobile cloud computing environment," *J. Supercomput.*, vol. 68, no. 2, pp. 624–651, May 2014.
[8] Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in *Proc. IEEE 11th Int. Conf.TrustCom*, 2012, pp. 295–302.
[9] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificate less proxy re-encryption scheme for secure data sharing with public cloud," in *Proc.7th ACM Symp. Inf. ,Comput. Commun. Security*, 2012, pp. 87–88.
[10] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in *Proc. 6th USENIX Security Symp. Focusing Appl. Cryptography*, 1996, p. 8.
[11] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–2119, Sep. 2013.
[12] Y. Chen, J. D. Tygar, andW. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in *Proc. IEEE INFOCOM*,pp. 1952–1960.
[13] K. Alhamazani*et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*,DOI: 10.1007/s00607-014-0398-5, 2014, to be published.

Author Profile

K. Sharmila is a Post-graduate student in the Computer Science Department, Kingston Engineering College, and Vellore, India. She received M.S degree in 2012 from Sathyabama University, Chennai, India. Her research interests are Cloud Computing, data mining and data structure.

V. Vinoth Kumar Assistant Professor, Department of Computer Science, Kingston Engineering College. He received his B. Tech degree in 2010 from SBC Engineering college in Arni .He then completed his M.tech in 2012 at Dr. M. G. R University in chennai. He has received Gold medal for outstanding academic performance in post graduate information technology. His area of interest includes Networks Security, Wireless Networks, Network simulation, Sensor Networks and Cloud Computing. He has done 2 publications and he has attended 6 workshop.