JES Journal of Engineering Sciences

Vol 10, Issue 12, Dec /2019
ISSN NO:0377-9254

A New Approach For Secure Data Sharing in Clouds

[1]Ms N. Sushma (M.Tech) [2]Mr V.N.S Vijay Kumar M.Tech , Associative Professor

[1,2] Lenora College Of Engineering, Rampachodavaram, East Godavari, Andhra Pradesh, INDIA

[1]Sushma.Nanduri11@Gmail.Com [2]Vijaykumarlce@Gmail.Com

Abstract—Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) 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. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud.

1. INTRODUCTION

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers [1]. Organizations with a low budget can now utilize high computing and storage services without heavily investing in infrastructure and maintenance [2].[3]. However, the loss of control over data and computation raises many security concerns for organizations, thwarting the wide adaptability of the public cloud. The loss of control over data and the storage platform also motivates cloud customers to maintain the access control over data (individual data and the data shared among a group of users through the public cloud) [4]. Moreover, the privacy and confidentiality of the data is also recommended to be cared for by the customers [5]. The confidentiality management by a customer ensures that the cloud does not learn any information about the customer data. Cryptography is used as a typical tool to provide confidentiality and privacy services to the data

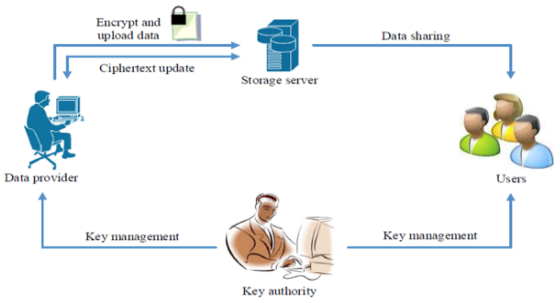

Figure: 1.Secure data sharing in cloud computing

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 [6]. However, when the data are to be shared among a group, the cryptographic services need to be flexible enough to handle different users, exercise the access control, and manage the keys in an effective manner to safeguard data confidentiality [7]. The data handling among a group has certain additional characteristics as opposed to two-party communication or the data handling belonging to a single user. The existing, departing, and newly joining group

members can prove to be an insider threat violating data confidentiality and privacy [7]. Insider threats can prove to be more devastating due to the fact that they are generally launched by trusted entities. Due to the fact that people trust insider entities, the research community focuses more on outsider attackers. Nevertheless, multiple security issues can arise due to different users in a group.

2. RELATED WORK

Incremental proxy re-encryption scheme for mobile cloud computing environment [7]

Due to the limited computational capability of mobile devices, the research organization and academia are working on computationally secure schemes that have capability for offloading the computational intensive data access operations on the cloud/trusted entity for execution. Most of the existing security schemes, such as proxy re-encryption, manager-based re-encryption, and cloud-based re-encryption, are based on El-Gamal cryptosystem for offloading the computational intensive data access operation on the cloud/trusted entity. However, the resource hungry pairingbased cryptographic operations, such as encryption and decryption, are executed using the limited computational power of mobile device. Similarly, if the data owner wants to modify the encrypted file uploaded on the cloud storage, after modification the data owner must encrypt and upload the entire file on the cloud storage without considering the altered portion(s) of the file. In this paper, they have proposed an incremental version of proxy re-encryption scheme for improving the file modification operation and compared with the original version of the proxy re-encryption scheme on the basis of turnaround time, energy consumption, CPU utilization, and memory consumption while executing the security operations on mobile device. The incremental version of proxy re-encryption scheme shows significant improvement in results while performing file modification operations using limited processing capability of mobile devices.

In this paper, they have proposed an incremental proxy re-encryption scheme and compared with the existing proxy re-encryption scheme on the basis of turnaround time, energy consumption, CPU utilization, and memory allocation on the mobile device.Due to the involvement of additional file segmentation, blocks concatenation, and cryptographic hash function, the proposed scheme provides confidential and integrity services to mobile users with slightly more time and marginally more energy consumption on the mobile device as compared to PReS. However, I-PReS shows improvement in results while performing the block(s) insertion, deletion, and modification operation(s) as compared to the PReS. The improvement in results depends on the number of block(s) that the data owner wants to update. They showed the result improvement of I-PReS in block(s) modification operation(s) as compared to PReS.

Efficient and Provably-Secure Group Key Management Scheme Using Key Derivation [8]

With the rapid development of the Internet, 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, they first demonstrate a collusion attack against Chen, et al.'s concrete RSA-based GKM scheme. Then, proposed an efficient and provably-secure GKM scheme using the key derivation method. Their GKM scheme has some attractive features. Firstly, the proposed scheme are 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.

In this paper, they proposed an efficient and provably secure GKM scheme using key derivation the scheme is suitable in practical scenarios with frequent group key updates. They have an efficient rekey mechanism for a reconnected member who may miss group key updates in his off-line period. Compared with the RSA-based CTT scheme, our scheme is more practical under the same features and asymptotic performance.

3. FRAMEWORK

In this paper, we propose a methodology named Secure Data Sharing in Clouds (SeDaSC) that deals with the aforementioned security requirements of shared group data within the cloud.The SeDaSC methodology, which is proposed in this paper, securely shares the data among a group without using the El-Gamal cryptosystem, the BDH, and bilinear pairing.

FIGURE: 2. System Architecture

The SeDaSC methodology is based on symmetric cryptography without reencryption. The aforesaid properties avoid computationally intensive operations and make the SeDaSC methodology a lightweight methodology. Moreover, the forward and backward access control is ensured by only allowing user access to a portion of the key that prohibits insiders to launch individual or coordinated attacks on the data.

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. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations.

4. EXPERIMENTAL RESULTS

Now a day's all organizations are using cloud services to store their business data and this data outsource leads to data leakage by cloud servers or by insider threats (sharing data users in groups), cryptographic algorithms are used to protect data but this technique will not support Access Control mechanism (weather sharing users has only read or write or both permissions), departing users (users whose access removes out or backward users), new users (joining new members or future users).

To support above features author has describe technique in this paper where three applications are used.

Cloud Server: Responsible to store data owners file in encrypted format.

Cryptographic Server: Responsible to generate two different keys for each file, one key sent to all sharing users and one key kept by cryptographic server. Data owner upload file data then with generated keys part file will be encrypted, Whenever any user send request for file download then cryptographic server will obtains user key and check weather user holds valid key or not, if user hold valid key then cryptographic server will use its part key and another key from user to decrypt file, Decrypted file then sent to user. To check file integrity this server generated MAC code on file data, if cloud hold correct file data then same MAC code will be generated and file integrity will be preserved. Whenever any new user joins in group then key part will be share with newly joined member. Whenever any user departs then its

key will be removed out and he cannot request for old or future data.

Data Owner or Data Users: In this application data owner will upload data to cloud by sharing with other users with access control such as Read or Write or both permissions. If read permission then user can only download data, if write permission means he can download, update and reupload data. Any time data owner can add new member in group or remove any member from group.

With above concept sharing data in cloud storage will be secured. Amazon S3 will be used for file data storage in encrypted format.

FIGURE:3. Home Screen

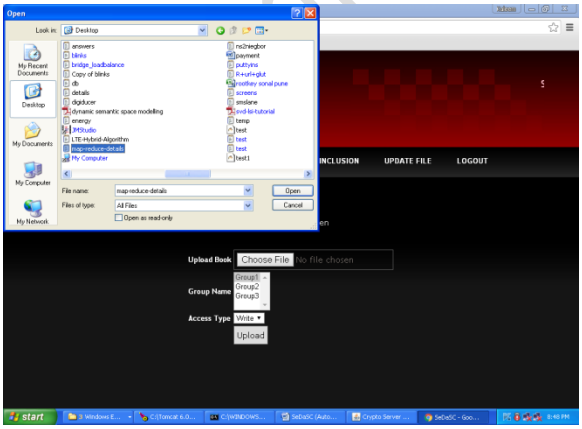

FIGURE:4. File Uploading Screen

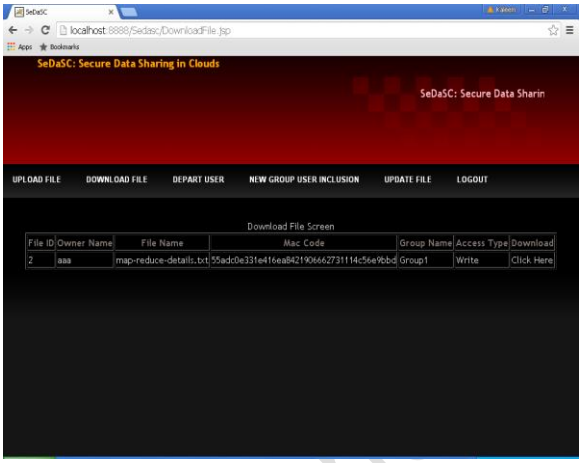

FIGURE:5. File Downloading Screen

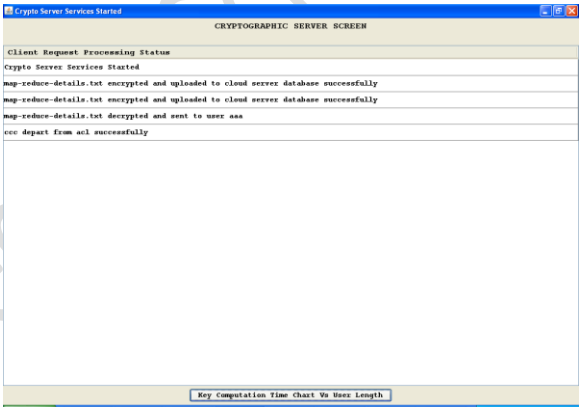

FIGURE:6. Cryptographic Server Screen

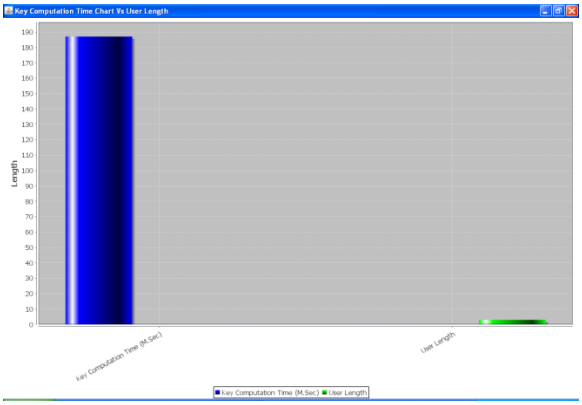

FIGURE:7. Key Computation Time Chart Vs User LengthScreen

5. CONCLUSION

We proposed the SeDaSC methodology, which is a cloud storage security scheme for group data. The proposed methodology provides data confidentiality, secure data sharing without reencryption, access control for malicious insiders, and forward and backward access control.The working of SeDaSC was formally analyzed using HLPNs, the SMT-Lib, and a Z3 solver. The performance of the SeDaSC methodology was evaluated based on the time consumption during the key generation, file upload, and file download operations. The results revealed that the SeDaSC methodology can be practically used in the cloud for secure data sharing among the group.

6. FUTURE SCOPE

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.

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 certificateless proxy reencryption 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.

Student Details:

Ms N.SUSHMA is a student of LENORA college of engineering, Rampachodavaram. Presently She is pursuing her M.Tech [Computer Science & Engineering] from this college and she received his B.Tech from Rajamahendri Institute of Engineering and Technology , Rajamandry, affiliated to JNT University, Kakinada in the year 2017.Her area of interest includes Data Ware Housing and Data Mining and its objectives including Object Oriented Programming Languages, all current trends and techniques in ComputerScience.

Vol 10, Issue 12, Dec /2019
ISSN NO:0377-9254

GUIDE DETAILS:

Mr V.N.S VIJAY KUMAR, is working as Associative Professor, Department of Computer Science & Engineering, Lenora college of engineering, Rampachodavaram, ijaykumarlce@gmail.com He has a total teaching experience of 10 years..His area of Interest includes Computer Networks, Data Warehouse and Data Mining, information security, flavours of Unix Operating systems and other advances in computer Applications.