IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-14, May 2019 E-ISSN: 2347-2693

Security Enhancement Using pre-authentication and Proxy re-encryption

Sushma A[1*], Sonisha S[2], M S Soumya Sree[3], Pooja M.S[4], Deekshitha G H[5]

[1,2,3,4,5]Dept. of Information Science and Engineering , NCET, Bengaluru

Corresponding Author: sushma.ash20@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si14.459462 | Available online at: www.ijcseonline.org

***Abstract*—** Cloud computing on its own is a technology, arming many services with its resources on the internet, when we speak about big data context, as we have witnessed massive growth in the use of internet that indeed has increased the demand for greater storage capacities where now MB's and GB's are small talks in the fields of storage. When we talk about the cloud storage there are privacy and security concerns that we need to work upon for which as of in this paper we propose and use techniques such as pre-authentication, encryption and de- encryption policies. The pre-authentication and proxy re-encryption mechanisms combine the advantages of proxy conditional re-encryption multi-sharing mechanism It can simply be termed as privacy preserving approach to increase security of data on cloud.

***Keywords*—** *Privacy, pre-authentication, big data*

I. INTRODUCTION

Now-a-days, amongst the wide growth in fields of technology big data is a hot research topic. As witnessed due to increase in the number of internet users there is greater amount of data produced that indeed increases the need for storage. With the increase in data production, the users prefer to save their data on the cloud as it has considerable amount of services and storage, which helps the users to upload and access the data anywhere, and anytime. People use multiple gadgets, pictures, record music, upload and click download through the internet and multiple other operations that produces massive amount of data. As a result, demand for cloud storage has greatly increased and is growing constantly. When data is stored on the cloud the only concern users have is whether data uploaded is secured or not. The cloud users do not want others to sneak into their storage space without permission. Public key encryptions are generally used by data provides to encrypt data, thus protecting the privacy of the data, no one other than the users with the private key can access the data on the cloud. The users without the valid permissions cannot access the data. Since the cloud is to open for everyone and the services over wide the data uploaded onto the cloud needs to be encrypted to protect the privacy of the data.

The cipher text is decrypted using their keys and obtain the message they want using the decryption methodologies the privacy needed can be ensured.

There are many cryptographic techniques, methods proposed until now to satisfy privacy in big data storage.

The Public Key Encryption (PKE) technique cannot achieve privacy secure system due to its

Public key non-anonymous property; so, some personal information can be leaked. To overcome the problems and maintain privacy, anonymous encryption mechanisms have been used.

To resolve the cloud security issues great efforts have been made by research communities and identity-based encryption techniques have been proposed which are more anonymous.

By creating linkage between users and the cloud, cipher texts can be easily protected.

PHR's ensure data stores were not leaked out, which are amongst the problems discussed in this paper. However, there are many more aspects to be considered.

In the system that is proposed the technique called proxy re-encryption process is being used. Here we ensure privacy by applying a semi-trusted proxy, re-encryption. By, using the semi-trusted proxy systems data sharing can be done without any exposure to the third party during re-encryption process.

II. RELATED WORK

Privacy-Preserving Cipher text Multi- Sharing Control for Big Data Storage:

In this work the need of secure big data storage service is more desirable than ever to data. The basic requirement of the service is to guarantee the confidentiality of the data.

Moreover, the service should provide encrypted data sharing with specified people under specific conditions .The system uses a privacy- preserving cipher text multi-sharing mechanism to achieve the above security purposes. It combines the merits of proxy re- encryption with anonymous techniques in which the cipher text is securely and conditionally shared multiple times without leaking any knowledge of underlying message and the identity information of cipher text of senders/recipients. Security is one of the most important concern in any type of service for storage providers. Individuals and organizations can view, modify and update their data stored in the cloud through remote accessing in the system. As and when there is increase in number of individual users, the public and private organizations choose to upload their data in cloud force to keep the data more secure from being hacked. The data of an individual user should be kept confidential and it should be accessed only by the authenticated users. While providing security, the most important aspect to be considered is that before storing the data, the anonymity of the service providers is achieved. The data security features are commonly required to maintain secure processing, and these features are achieved by employing a new techniques such as cipher text multi sharing mechanism.

In EHR systems, hospitals, devices, and patients can upload health records and obtain and view them at any given instance. To preserve the patient's privacy these types of systems, Patient Controlled Encryption (PCE) is used as a means to secure and privately store the patient's medical records. This means that the patient can selectively share records with healthcare providers and doctors. The PHR is organized in a hierarchical structure, where a key is assigned to every level in the hierarchy. The patient stores a secret key, from which a tree of subkeys is obtained. The user passes out sub keys selectively for decryption restricting access to only certain portions of his record. For selective search of portions of the records, the Patient is given the power to create and allot trapdoors. Patient Controlled Encryption system stops the unauthorized users from accessing the patient's data by healthcare providers and data storage providers.

Sometimes, a patient can unknowingly allow access to a corresponding class without the knowledge of the type of file. The complexity in key management is high due to all the low-level categories involved, that requires different decryption keys for each category.

To translate an encryption under A's identity into another system under B's identity, an identity based Proxy-re-encryption system is deployed. This translation is done without seeing the plaintext with the encryption keys or proxy keys are used. A simple extension to an identity based encryption scheme gave birth to the PRE rendition of it. It is a two prong system, an algorithm for the generation of encryption keys for assignment to the proxy is the first part. The second prong is for re-encryption and here the ciphertexts are given re-encryption keys by the proxy and their identity is re-made into another one. The re-encryption keys are generated by the delegator with the aid of his IBE secret key; this is the trademark of a non interactive system. The IBE master secret key isn't a requirement. It prevents ciphertext attacks a well but a detailed Pre-Authentication mechanism has not been investigated.

Jakobsson developed a quorum-based protocol where the proxy is divided into sub-components, each controlling a share of the re-encryption key; here, the keys of the delegator are safe as long as the proxies are honest. A similar approach was considered by Zhou, Mars, Schneider and Redz .

III. PROPOSED SYSTEM

A. SYSTEM MODEL AND DEFINITION

A. System Overview

Firstly, the system is mainly for multi receivers to share data from cloud conditionally, and data privacy preserving. Our system can apply to situations when the data is extremely large. The user's data uploaded onto the cloud, needs to be encrypted in order to prevent the data from being exposed to the attacks .

The proxy server, a semi-trust party is used for re-encrypting the cipher text. The receivers who want to retrieve their data have their own key for the decryption process. Our system lets the receivers to retrieve their desired data from the cloud.

This system not only provides re-encryption operation, but also ensures the authentication between data providers and receivers are maintained without leaking of data. We adopt the authentication technique based on attributes; it enhances the security to resist tracing attacks. With the two techniques, this system would meet the flexibility and privacy preserving demands in cloud storage. Data providers use portable devices such as smart phones, and other gadgets in order to upload data, and then the data collected is encrypted and transmitted to the cloud centers. The cloud centre verifies the data providers attributes. The providers will get their credentials which represent the attributes. Each provider can use the pseudonyms allocated before to verify his attribute anonymously and communicate with others without any data loss. Similar to the providers, data receivers can prove their qualifications without privacy exposure. After the authentication and re-encryption process, users can start sharing data with each other.

B. SYSTEM DEFINITION AND ADVANTAGES

The system proposed serves all the required attributes of secure virtual storage environment must contain, the system ensures privacy preserving by implementing pre-authentication, encryption and proxy re-encryption techniques with the help of key generation processes.

Advantages

- Firstly the system proposed has concept of highly secure privacy of keys.
- The security mechanisms used provides a combined advantage of proxy re-encrypted multi- sharing mechanism with attribute-based authentication process.
- The system achieves attribute authentication before re-encryption, ensuring security of both attributes and the data.
- Receivers with permission to access the data can use their keys to decrypt the cipher text, but others are restricted from the access, so the data provider's privacy is well protected.

C. SECURITY FRAME

In this system, we ensure the security against several attacks, including selective conditions like Chosen Chipper- text Attack (CCA), selective identity CCA and collusion attacks, and ensuring that cipher texts, re-encryption keys and the attributes of the users are kept anonymous and safe.

Only if the authorization chain has no corrupted identities, unauthorized accesses the data access is allowed, else the access from the process is declined. Thus the anonymity of the attributes and cipher texts is well maintained, we give the definition for the system's security frame.

IV. SYSTEM CONSTRUCTION

We present a briefing of what the entire system is composed of, it comprises of various operations carried out in order to provide high security cloud services. This system is constructed using multiple methodologies like key generation, encryption, re-encryption, pre-authentication and decryption that build the system. Firstly, the parameters are setup and the secret keys are generated. Then the data is encrypted into cipher text as the data is chosen to be uploaded onto the cloud.

Then the generation of the re-encryption keys is carried on. After which, the attributes of the data receivers are verified to avoid unauthorized accesses, and only receivers with specific attributes have access to the re-encryption keys and cipher texts. Finally, the decryption of the re-encrypted cipher texts is carried out and the data is retrieved by the valid users.

Security of Pre-Authentication

Here in this system to ensure security of attributes, users use qualified attributes for the verification process.

Unless leaking the original data or attributes happens directly, we ensure that the adversaries cannot obtain the private information.

This system aims to achieve the anonymous nature of attributes, to remove linkages between attributes and identities. The pre-authentication scheme used applies random commitments of attributes, such that adversaries are unable find the link between attributes and identities.

The commitments produced from same attributes are independent, they prevents the adversaries from getting attributes from specific users to avoid data leakage. The pre-authentication scheme can resist tracing attacks. The adversary cannot use a fake identity in the system. Otherwise, he is not able to pass the verification.

Thus our scheme is tracing attack-secure. The pre-authentication technique verifies the user's attributes before data communication, which means both data providers and the receivers can authenticate the attributes of the both side.

Thus the system protects user's privacy and avoids data loss. So the authentication of both data provider's and the receiver's attributes protect their privacy.

V. CONCLUSION

Here in this paper we understand the requirement for security in data sharing, we propose a system that is CCA secure in data sharing. We use the techniques such as pre-authentication and proxy re-encryption in this system that ensures that only users with authorized attributes are allowed to obtain the data, and provides security for the private attributes. Hence the pre-authentication and re- encryption techniques add on greatly in improving the security purposes of the cloud services.

REFERENCES

[1] X. Liu, X. Xie, K. Li, B. Xiao, J. Wu, H. Qi, and D. Lu, "Fast tracking the population of key tags in large-scale anonymous rfidsystems,"IEEE/ACM Transactions on Networking, vol. 25, no. 1, pp. 278–291,2017.

[2] H. J. Benaloh, M. Chase and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records" ACM Cloud Computing Security Workshop, pp. 103114, 2009.

[3] M.Green and G.Ateniese, "Identity based proxy re-encryption" Applied Cryptography and Network Security, vol. 4521, pp. 288-306, 2007.

[4] K. Wang, J. Mi, C. Xu, Q. Zhu, L. Shu, and D. J. Deng, "Real-time load reduction in multimedia big data for mobile Internet,"ACM Transactions on Multimedia Computing, Communications and Applications, vol. 12, no. 5s, Article 76, Oct 2016.

[5] Joseph K. Liu, Kaitai Liang, Willy Susilo, "Privacy- Preserving Ciphertext Multi-Sharing Control for Big Data Storage", August 2015 · IEEE Transactions on Information Forensics and Security.
[6] K. Wang, Y. Shao, L. Shu, Y. Zhang, and C. Zhu, "Mobile big data fault-tolerant processing for ehealth networks," IEEE Network, vol. 30, no. 1, pp. 1–7, Jan 2017.
[7] W. S. K. Liang and J. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," IEEE Transaction on Information Forensics and Security, vol. 10, no. 8, Aug 2015.
[8] P. L. J. Shao and Y. Zhou, "Achieving key privacy without losing 972CCA security in proxy re- encryption," J. Syst. Softw., vol. 85, no. 3, 973pp. 655– 665, 2011.
[9] W. S. K. Liang and J. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," IEEE Trans. Inform. ForensicsSecurity, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.
[10] P. Druschel and A. Rowstron,PAST: A Large- Scale, Persistent Peer-to-Peer Storage Utility, Proc.Eighth Workshop Hot Topics in Operating System, 2001, pp. 75-80.
[11] Markus Jakobsson, On quorum controlled asymmetric proxy re-encryption, In Proceedings of Public Key Cryptography, pages 112-121, 1999.
[12] Lidong Zhou, Michael A. Marsh, Fred B. Schneider, and Anna Redz, Distributed blinding for ElGamal re- encryption,Cornell Computer Science Department, 2004.

