International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Basic Framework for Policy Updates for the Outsourced Exchange of Private Medical Records

V. Jayaganesh

Abstract: ***Since cloud computing and other data outsourcing settings offer high flexibility and accessibility, many healthcare providers se personal health records (PHRs) that are electronic to let patients manage their own health data in a scalable and robust environment. However, PHRs contain extremely sensitive data, thus security and privacy issues are crucial. PHR owners should be free to create their own flexible and safe access rules for their data that is outsourced. Beyond the fundamental authentication feature, most commercial cloud platforms offer tenants the option of symmetric or public key encryption to protect their data. But because symmetric encryption has a large key management overhead and requires a lot of upkeep, In this study, we develop a fine-grained, secure access control system for outsourced PHRs that incorporates updates to the policies in a lightweight manner. Our suggested solution (PRE) is based on proxy re-encryption and ciphertext policy attribute-based encryption (CP-ABE). To assist complete policy change tracing, we also offer a policy versioning approach. Ultimately, an assessment of performance was carried out to demonstrate the efficacy of the suggested approach.***

Keywords: Policy versioning, proxy re-encryption, PHRs, access control, CP-ABE, policy updating, and performance evaluation

1. Introduction

To provide unfettered access to share services and data, the outsourced server in a cloud system storage or other outsourced data sharing environment must always be up and running. Many business and individual increasing refer to store that the important data on external servers, such as cloud storage, because of the cost reductions and effective resource management can be offered by an cloud providers. Before sending their data, the majority of data owners encrypt it to a cloud server in order to protect privacy and security. The best way to stop unauthorized access to private data is to encrypt it. However, encryption is not enough to provide stringent security oversight. An system can control another often needed security perimeter.

The outsourced server in an outsourced shared data environment, such as a cloud storage system, needs to be reachable at all times to provide unlimited access to shared data and services. Many companies and individuals increasingly choose to store their critical data on external servers like cloud storage due to the cost savings and efficient resource management provided by cloud providers. To Data owners typically encrypt their data before outsourcing it to a cloud server in order to satisfy privacy and security concerns. The best defense against unwanted access to sensitive data is encryption. Nevertheless, encryption by itself cannot provide strict security control. Usually, as an extra security perimeter, an access control system is needed. attributes-based encryption (ABE)

2. Related Work

[1].In this research, Due to the great flexibility and accessibility of data outsourcing environments, such as the cloud computing environment, many healthcare providers adopt electronic personal health records (PHRs). In an environment that is both scalable and durable, this allows individual patients to control their own health data. Security and privacy issues are crucial, though, because PHRs contain such sensitive information. The freedom to establish their own safe and adaptable access guidelines for then we have outsourced data should also be granted to PHR owners. Commercial cloud systems that are already in place frequently include symmetric or public key encryption as an add-on feature to allow data confidentiality for their tenants, on top of the basic authentication feature. Nevertheless, because symmetric encryption has a large key management overhead and requires expensive maintenance.

[2]. In this research, As a result of the great accessibility and flexibility of data outsourcing environments, including cloud computing environments, Electronic personal health records (PHRs) have been used by numerous healthcare organizations. which allow patients to manage their own health data in a scalable and resilient setting. However, security and privacy concerns are the main cause for concern because PHRs hold extremely sensitive information. Owners of PHRs should also be able to safely and flexibly create their own access policies for the data that is outsourced. To enable data confidentiality for their tenants, current commercial cloud systems typically offer symmetric or public key encryption as an optional feature in addition to the fundamental authentication capability. The substantial key management burden of symmetric encryption, however, makes such conventional encryption techniques unsuitable for data outsourcing environments.

[3]. In this paper-In this study, we find a workable way to update CP-ABE access rules without needing the data owner to use a new encryption process. As far as sharing PHRs goes, the data owner, which may be a patient, has the freedom to selectively share their data with anyone they choose. We employ the CP-ABE technique to encrypt the symmetric key, which ensures efficient encryption and improved efficiency for updating policies and accessing data. We use symmetric encryption to encrypt data since it provides better encryption performance. The symmetric key is encrypted using the CP-ABE approach, thus the cost of altering the policy only affects the encrypted version of the key. It is therefore not required to re-encrypt every ciphertext. With this, the significantly reduced.

[4]. In this research, For unrestricted access to shared data and services in an outsourced data sharing environment, such a cloud storage system, the outsourced server must always be

up and running. Because cloud providers offer cost savings and effective resource management, many businesses and individuals now opt to store their important data on external servers like cloud storage. Data owners typically before outsourcing their data, they encrypt it. a cloud server in order to address privacy and security concerns. The best method for shielding private information from unwanted access is to encrypt it. However, strict security control cannot be supported by encryption alone. An additional security perimeter that is typically necessary is an access control system. Attribute-based encryption (ABE) [1] has been developed to address this issue.

3. Experimental Analysis

To determine whether our recommended approach is effective, we put up a proxy server system simulation to mimic an outsourcing scenario. To simulate the system, the cp-abe tools and the Java Pairing-Based Cryptography library are utilized (JPBC). The Intel (R) Xeon (R)- CPU E5620, clocked at 2.40GHz, was utilized for the test. We gauge the efficacy of our system by contrasting the encryption, decryption, and re-encryption timings of our suggested re-encryption procedure carried out by PRE with multi-thread processing and without PRE. JPBC was utilized to replicate the cryptographic architecture of scheme [5] so that it could be compared with our system. To evaluate the computational efficiency of encryption and decryption, we adjust several policy-related aspects in the simulation. Even though our method requires two encryption steps, the second encryption stage uses the key encryption of CP-symmetric ABE. Because of the relatively small 128-bit symmetric key size, the encryption and decryption timings are not greatly affected by the total processing time. This exemplifies the benefits of our proposed cryptography methods..

4. Proposed Modelling

To our proposal states that PHR owners upload patient profiles and treatment records, among other encrypted data files, to a cloud server. If a user possesses the required abilities (a decryption key that complies with the access control policy), they, like doctors, can access the shared file. Attribute authorities provide PHR owners and users with a set of characteristics in the form of a user decryption key, as shown in . Our design enables many authorities to offer the characteristics to users. For example, a patient may obtain keys from multiple institutions, including medical facilities or insurance companies. in an environment where outsourcing typical The cryptographic methods we offer are based on an extension of the original in our scheme. CP-ABE . There are two encryption components in our system build. Data is first encrypted using symmetric AES encryption. Second, CP- ABE is used to encrypt the symmetric key.

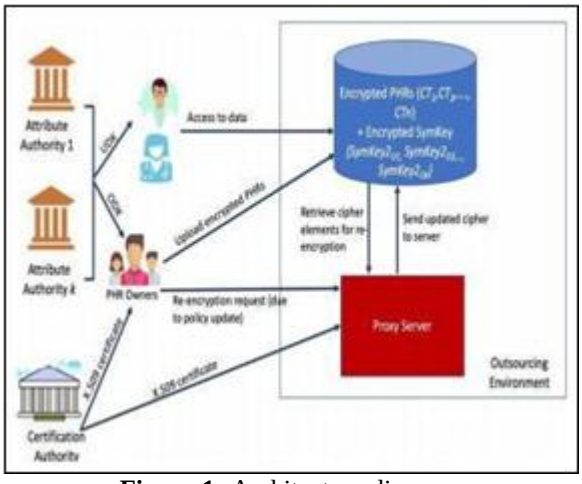

Figure 1: Architecture diagram

5. Module Description

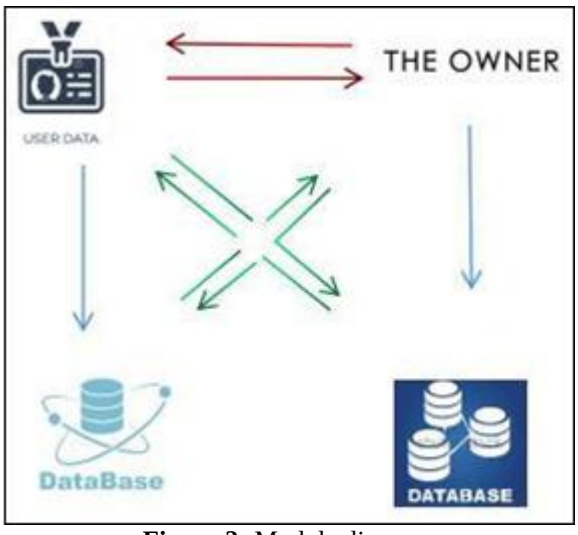

Figure 2: Module diagram

1) Data Owner
2) Data user
3) Database

1) Data Owner
Enter the account details while registering. Cloud can authorize the account after registration. The account owner cannot log in without authorization. The owner may submit a health record linked to their medical records in an encrypted fashion. Examine the uploaded files and Control the data Examine the request and respond to user.

2) Data User
Enter your basic details when creating an account. Cloud can authorize the account once it has been registered. The owner cannot access the account without authorization. Examine every submitted file and submit a request for a specific piece of data. Following receipt of the data owner's response, the certificate authority can distribute the file keys. Get the file here.

3) Database
The account that is using the proper password and username See each uploaded file View the requests and responses that have been downloaded. Give others access to the key See

every file that has been downloaded. the account that is using the proper password and username See and approve all users. See every file that has been uploaded. See every file that has been downloaded. Files that have been downloaded and uploaded are graphed.

6. Results and Discussions

In this section, we compare the functionality of our scheme with the schemes of Li et al. [5] and Ying et al. [16]. To simplify the expression of computing cost for each scheme, we define the following notations.G0: Exponentiation operation in group G0; let pbe the element size in the G1, G2, Zp G1: Group Exponentiation, Rd = Random decryption of the ciphertext or messageNc is the number of characteristics linked to the encrypted key or ciphertext. Our plan provides cheaper communication costs for policy updates as compared to [5,]. This is so that the new access control policy, which only accepts attributes that belong to Zip, and the random element will be sent to the proxy server exclusively. Communication expenses are incurred in [5] for the update key generation and matrix mapping element with a new access policy to be sent for cipher text updating.

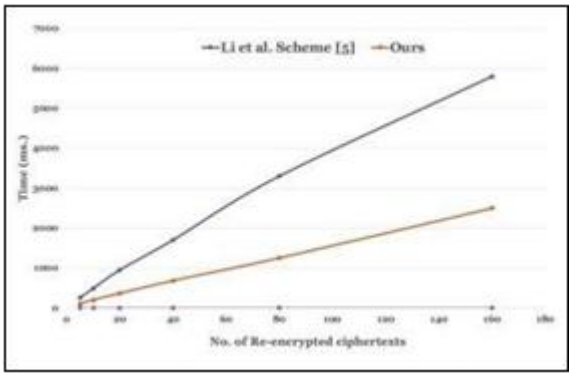

Figure 3: Graph

To calculate the cost of the policy change, we examine the cost of proxy re-encryption, update key generation, and ciphertext update expenses. Figure 5 displays the results of the Li et al. scheme, our recommended approach, and the policy update time (ms). Processing time is estimated using an increasing number of ciphertexts that require re-encryption. We incorporated the five attributes into the simulation. We re-encrypted files with an average size of 20 KB using the 5-attributes strategy.

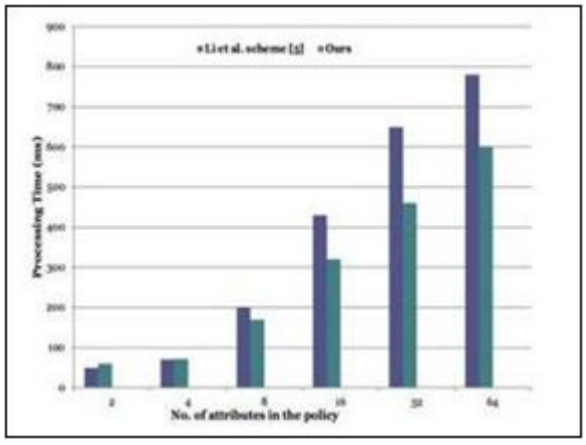

Figure 4: Results analysis

7. Future Enhancement

This offers a transparent access control for the file storage system and manages policy updates as a result. Furthermore, in order to facilitate the effective reconstruction of past policies for thorough auditing, we suggested the policy versioning technique. In conclusion, we showcased the file re-encryption performance. The outcomes demonstrated that the multi-thread processing-based re-encryption method performed better than the one without one. In subsequent work, we will conduct in-depth tests to evaluate the cloud-based proxy in an actual cloud environment using a bigger amount of data and access policies.

8. Conclusion

In the work, A method for updating policies that utilizes proxy re-encryption and policy outsourcing has been introduced. The expense of updating policies is entirely transferred to the outsourced server by our way. Furthermore, multi-thread processing is included in the re-encryption process for increased scalability and enhanced system performance. For the trial, we developed a GUI tool to implement adjustments to the CP-ABE policies. Owners of data can upload encrypted files and policies to our external storage using our system. In order to reencrypt data, administrators or data owners do not need to contact with an external server or extract policies from a local database. With our web-based solution, policies can be changed whenever and from anywhere. Transparent access control is therefore made possible by the file storage system and policy update management.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Cipher text-Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.
[2] S. Fugkeaw and H.Sato, ‘‘Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing, ’’ J. High Perform. Comput. Netw., vol. 9, no. 4, pp. 299–309, 2016.
[3] Y.Kawai, ‘‘Outsourcing there encryption key generation: Flexible ciphertex t-policy attribute-based proxy re- encryption, ’’ in Proc. Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), Beijing, China, 2015, pp. 301–315.
[4] H. Wang, Huiwen Wang, Huihui Wang, J. Li, Shulan Wang, Yuan Li, H. Wang, Huiwen Wang, Huihui Wang Scheme in Cloud Computing with Policy and File Updates, " IEEE Transactions on Industrial Informatics, Vol. 15 (2), pp. 6500-6509, 2019.
[5] K.Liang, W.Susilo, and J.K.Liu, Privacy-preserving ciphertext sharing strategy for massive data storage, IEEE Trans. Inf. August 2015, (8), pp.1578-1589.
[6] Y. Kawai, In: International Conference on Information Security Practice and Experience, ISPEC 2015, Beijing, China, 2015.
[7] Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing, Int. Journal High Performance and Computing Networking, Inderscience, Vol. 9 (4), pp. 299–309, 2016.

[8] X.Liang, Z.Cao, H. Lin, and J.Shao, ‘‘Attribute based proxy re-encryption with delegating capabilities, ’’ in Proc. 4th Int. Symp. Inf., Comput., Com-mun. Secur. (ASIACCS), 2009, pp. 276–286
[9] A. Sahai, B. Waters, “Fuzzy Identity-Based Encryption”, In Proc. of the 24th Annual International Conference on Theory and Applications of Cryptographic Technique (EUROCRYPT 2005), May, LNCS, 2015.
[10] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext policy Attribute based Encryption, IEEE Symposium of Security and privacy, Oakland, CA, USA, May 20-23, Los Alamitos, 2007.