International Journal of Research in Engineering, Science and Management
Volume 5, Issue 3, March 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

A Lightweight Policy Update Scheme for Outsourced Personal Health Records Sharing

R. Priyadarshini[1], P. Harshitha[2*], R. Manasa[3], P. James Prasad[4], M. Jeshwanth[5]
[1]*Associate Professor, Department of Computer Science and Engineering, Siddartha Institute of Science and Technology, Puttur, India*
[2,3,4,5]*Student, Department of Computer Science and Engineering, Siddartha Institute of Science and Technology, Puttur, India*

***Abstract*: With high adaptability and openness of information re-appropriating climate, for example, distributed computing, a few medical care suppliers execute electronic individual well-being records (PHRs) to empower individual patients to deal with their well-being information in such a strong and versatile way. Nonetheless, PHRs contain profoundly delicate data about which security and protection issues are the basic concern. Moreover, PHR proprietors ought to be proficient to deftly and safely characterize their entrance strategy for their rethought information. Notwithstanding the fundamental verification includes, existing business cloud stages typically give symmetric or public key encryption as a discretionary component to help information secrecy for their inhabitants. Be that as it may, such customary encryption plans are not reasonable for information rethinking climate due to high key administration, the upward of symmetric encryption, and high upkeep cost for taking care of different duplicates of ciphertext for public-key encryption arrangement. In this paper, we plan and foster a safe and fine-grained admittance control plot with a lightweight access strategy update for rethought PHRs. Our proposed conspiracy depends on the ciphertext strategy, property-based encryption (CP-ABE), and intermediary re-encryption (PRE). What's more, we acquaint an approach forming method with help the full detectability of strategy changes. At long last, we led the presentation assessment to show the proficiency of the proposed conspiracy.**

***Keywords*: CP-ABE, PHR, PRE.**

1. Introduction

Accessing the health records whenever it is necessary is possible when the health records are stored in a server connected to the internet. Instead of carrying a health record as a hard copy when it is necessary, it is better to access it when it is needed via the internet. Cloud Computing is a technology that helps to store and access health records using the internet.

Cloud Computing uses encrypted algorithms to ensure the security of the health records stored in it. The Ciphertext-Attribute Based Encryption and Proxy-Re-Encryption are used to provide security to the health records.

The project has 4 modules- PHR Owner, PHR User, Cloud Server, Proxy Server. The PHR Owner uploads the file to the server connected to the internet using an encrypted key. Before uploading the files the PHR owner has to register with basic information and Cloud Server provides authorization to the Data Owner.

The PHR User has to register with basic information, the PHR owner has to authorize the PHR user then he can log in to his/her account to see all the PHR owners and files uploaded by them. PHR User has to send a request to the PHR owner of the respective file he wants to access. The PHR owner requests the Proxy server to re-encrypt the encrypted file he uploaded with the requested policy. The Proxy Server re-encrypts the encrypted file the PHR owner uploaded with the policy requested by the PHR owner. Then the PHR owner accepts the request sent by the PHR user. Then the user can download the requested file.

2. Modules

A. PHR Owner

The PHR owner registers with the basic information in the cloud server before uploading the files in the encrypted format. To upload files in the encrypted format CP-ABE algorithm is used. The PHR owner re-encrypts the already encrypted file according to the policy he/she requested using a Proxy server. The PHR owner accepts the request sent by the PHR user to make the PHR user access the file he/she requested.

B. PHR User

The PHR user registers in the cloud server with the basic information. Then the PHR user can request the PHR owner to access the file required.

C. Cloud Server

Cloud server authorizes both PHR owners and PHR users by taking their basic information during the registration. The Cloud server contains the health records in the form of image files in the encrypted format. When these files need to be re-encrypted according to the policy requested by the PHR owner, the Proxy server accesses the files in the cloud server to re-encrypt them and store them back in the cloud server.

D. Proxy Server

The Proxy server re-encrypts the already encrypted files stored in the cloud server according to the policy requested by the PHR owner. The proxy server fetches the files from the cloud server and re-encrypts them using the policy requested by the PHR owner and stores them back in the cloud server.

*Corresponding author: paladugu.harshitha2000@gmail.com

3. Algorithms

A. Ciphertext policy Attribute Based Encryption (CPABE)

The ciphertext is depicted with a bunch of properties while the private keys are related with an entrance structure indicating which ciphertext the clients can decode. As a double methodology, Ciphertext strategy ABE (CPABE) doles out properties to private keys and appends an entrance strategy ciphertext so just clients holding the arrangement of qualities fulfilling the entrance strategy can decode the ciphertext.

B. Proxy Re-Encryption

Proxy re-encryption (PRE) plans are cryptosystems that permit outsiders (intermediaries) to modify a ciphertext that has been scrambled for one party, so it could be decoded by another client. On the off chance that User B demands the intermediary server for the re-encryption interaction to get the document transferred on the haze hub by client A. In the re-encryption process, the intermediary server changes the main level ciphertext of client A (CA ∈ C1) to the second level ciphertext of client B (CB ∈ C2) and picks a new nonce. The intermediary first checks the entrance control list on the off chance that client B approaches privileges to the transferred document, the intermediary server re-encodes that record and connected Nonce esteem with the record, and afterward permits client B to download it.

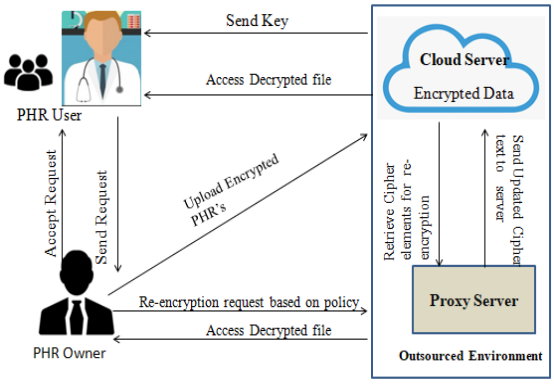

Fig. 1. System architecture

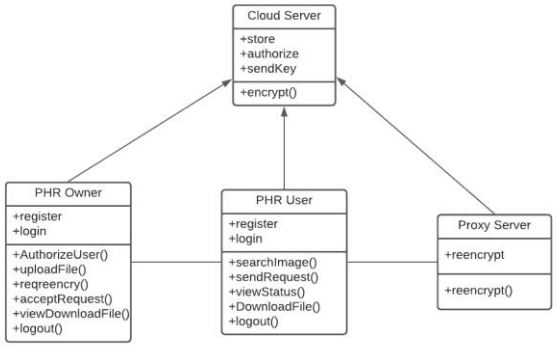

Fig. 2. Class diagram

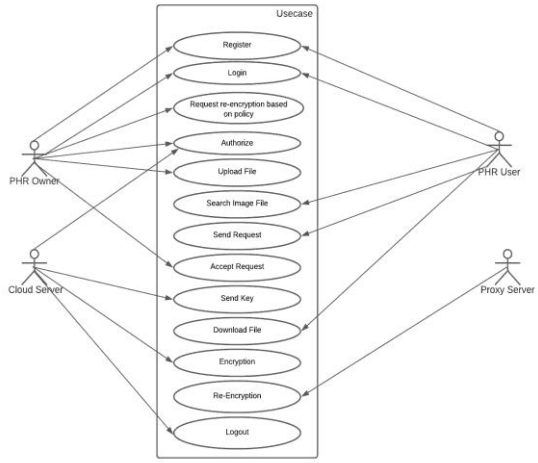

Fig. 3. Use case diagram

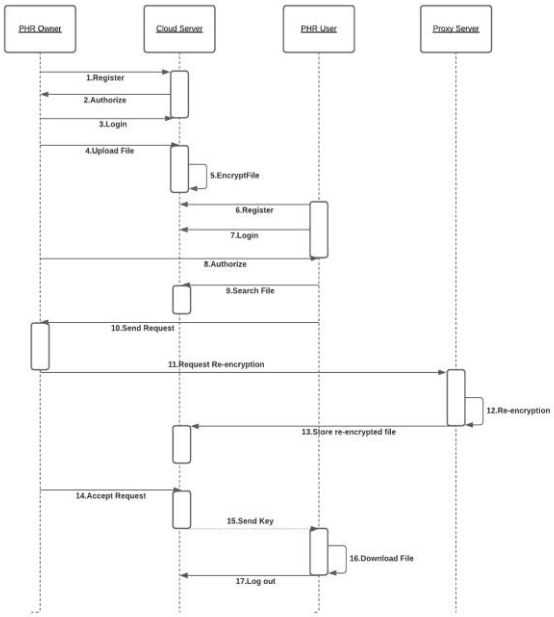

Fig. 4. Sequence diagram

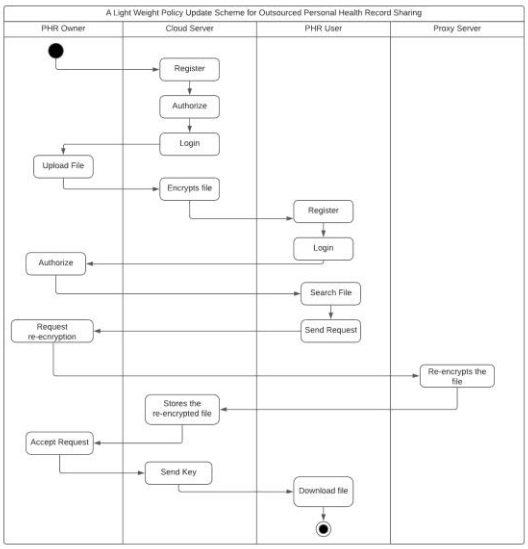

Fig. 5. Activity diagram

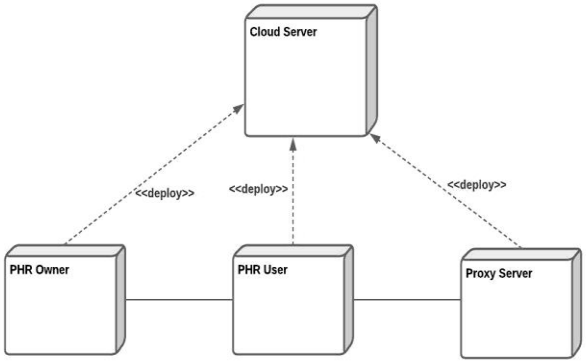

Fig. 6. Deployment diagram

4. Conclusion

The policy update scheme is based on the policy outsourcing and proxy re-encryption method. Our scheme fully offloads policy update costs to be done in the outsourced server. Also, the re-encryption process encapsulates the multi-thread processing to support high scalability and improves the overall performance of the system. For the experiment, a GUI tool for CPABE policy update implementation. PHR owners can upload files and policies in an encrypted format to the outsourced storage through our system. Administrators or data owners do not need to retrieve policies from the local database and interact with the outsourced server for the re-encryption process. With our web-based tool, policies can be updated anytime and anywhere. As a result, this provides transparent access control for the file storage system and policy update management. In addition, we proposed the policy versioning technique to enable efficient reconstruction of historical policies for rigorous auditing.

References

[1] M. Mambo and E. Okamoto, Proxy cryptosystems: Delegation of the power to decrypt ciphertexts, IEICE Transactions, E80-A (1): pp.54-63,1997.

[2] Liang, W. Susilo, J. K. Liu, Privacy preserving ciphertext sharing mechanism for big data storage, IEEE Trans. Inf. Forensics Security, Vol. 10, pp. 1578-1589, August 2015.

[3] S. Fugkeaw, H. Sato, 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.

[4] Y. Kawai, Outsourcing the re-encryption key generation: Flexible ciphertext-policy attribute-based proxy re-encryption, in: International Conference of Information Security Practice and Experience, ISPEC 2015, Beijing, China, 2015.

[5] X. Liang, Z. Cao, H. Lin, J. Shao, Attribute based proxy re-encryption with delegating capabilities, In Proc. of ASIACCS, ACM, pp. 276–286, 2009

[6] Lyes Touati, Yacine Challal "Instantaneous Proxy-Based Key Update for CP-ABE", In Proc. Of Local Network Conference (LNC 2016), Dubai, December, IEEE, 2016.

[7] K. Yang, X. Jia, K. Ren, R. Xie, L. Huang, Enabling efficient access control with dynamic policy updating for big data in the cloud, in: Proceedings of IEEE Conference on Computer Communications, (INFOCOM'14), IEEE, 2014.

[8] K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

[9] S. Fugkeaw and H. Sato, Scalable and secure access control policy update for outsourced big data, Future Generation Computer Systems, Vol. 19, pp. 364-373. 2018.

[10] L. Cheung and C. Newport, "Provably ciphertext policy ABE," In Proc. of ACM Conference on Computer and Communication Security (CCS 2007), Virginia, USA, October, ACM, 2007.

[11] W. Yuan, Dynamic policy update for ciphertext-policy attribute-based encryption, IACR Cryptology, vol. 2016. pp. 457-468, 2016.

[12] U. S. Varri, S. K. Pasupuleti, and K. V. Kadambari, Key-Escrow Free Attribute-Based Multi-Keyword Search with Dynamic Policy Update in Cloud Computing, In Proc. of IEEE/ACM International Symposium on Cluster, Cloud, and Internet.