# Securing Outsourced Personal Health Records on Cloud Using Encryption Techniques

Abhijeet Borade(✉) and Rashmi Agarwal

REVA Academy for Corporate Excellence, REVA University, Bengaluru, India
{abhijeet.cs02,rashmi.agarwal}@reva.edu.in

**Abstract.** Due to the greater flexibility and accessibility of data outsourcing environments such as cloud computing environments, several healthcare organizations have implemented electronic Personal Health Records (PHRs) to ensure that individual patients have such resilience and scalability. It allows users to manage their health information in a safe environment. However, PHRs contain highly sensitive information where security and privacy issues are major concerns. PHR owners should also be able to securely define their own access policies for offsite data. In addition to basic authentication capabilities, existing commercial cloud platforms typically offer symmetric or public key encryption as an optional feature to keep tenants' data confidential. However, such traditional encryption schemes are not suitable for data outsourcing environments due to the high key management overhead of symmetric encryption and the high maintenance costs of handling multiple copies of ciphertext for public key encryption solutions.

The output of this study is to design and development of a secure, fine-grained access control scheme with lightweight updates to outsourced PHR access policies. The proposed scheme is based on Cipher Text Policy Attribute-Based Encryption (CP-ABE) and Proxy Re-Encryption (PRE). Additionally, this study introduces a policy versioning technique that supports full traceability of policy changes using the Elgamal technique and a performance evaluation that demonstrates the efficiency of the proposed scheme.

**Keywords:** PHRs · Access control · CP-ABE · Policy update · Proxy re-encryption · Policy versioning · Performance evaluation

## 1 Introduction

Everyone is rapidly marching towards a new age wherein all will gather our information and execute higher cost estimation in a rough manner across the remotely operated servers, which is widely known as "Cloud".

The Fig. 1 shows the cloud computing model with reference to the various elements of it. Despite the cloud technologies having numerous benefits including but not limited to paying per utilization, providing distributed surrounding for computation, cost affordability, able to be very flexible, and many more, it still poses numerous privacy-related problems as the primary information would be available online with the risks

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2023
Published by Springer Nature Switzerland AG 2023. All Rights Reserved
S. Nandan Mohanty et al. (Eds.): ICISML 2022, LNICST 470, pp. 195–208, 2023.
https://doi.org/10.1007/978-3-031-35078-8_17

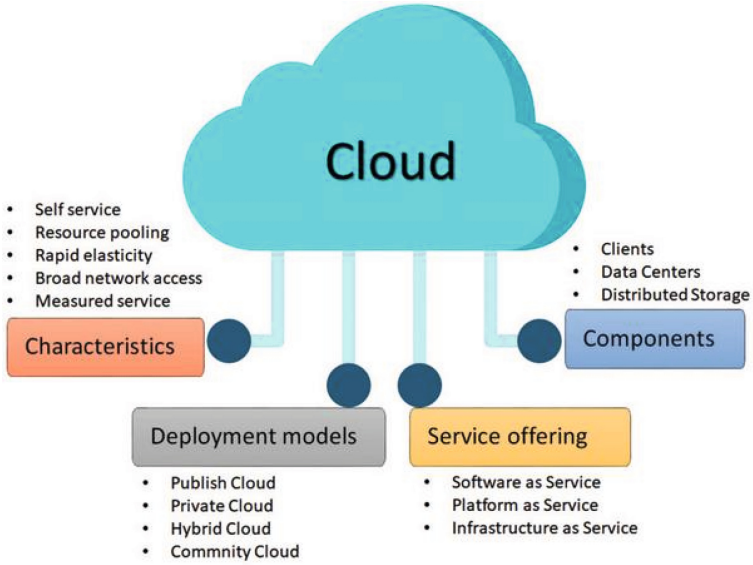


**Fig.1.** Typical model of cloud computing [1]

of being harmed by any unauthorized utilization by any anonymous users [2–6]. These cloud technologies indulging information sharing can often be outsourced because of the cost incurred for deployment and maintenance inconveniences. These outsourced servers should preferably be accessible 24 × 7 in order to impart unrestricted privilege to the services and information being shared. In the modern age, several firms and even many individuals desire to accumulate their precious information in outsourced cloud storage because of the potential to cut down the total cost for any project and the effective resource administration offered by several providers of these servers. While thinking about the aspect of security and privacy problems in the cloud, the owners of the information more commonly might protect their information with a few encryptions prior to outsourcing the third-party service providers.

Encryption of information is the most appropriate way of securing sensitive information from unauthenticated entry. Furthermore, we can say that encrypting information cannot alone adequately aid robust security command. The mechanism of access command is another security aspect that is usually needed. For sorting out this, Attribute-Based Encryption (ABE) [7] was widely deployed by several investigators. "One-to-Many" basis encryption schema along with enhanced access command was imparted by these methodologies. Thus, we can say that these methodologies had the abilities of both access command and encryption.

This ABE could be categorized into two namely:

1. KP-ABE – Key-Policy Attribute-Based Encryption.
2. CP-ABE – Ciphertext-Policy Attribute-Based Encryption [8].

In KP-ABE, the encryption was made by a couple of features, whereas the key of the user was related to the access policy. Now, coming to CP-ABE, the encryption of data was made by utilizing access policy and construction of the decryption key of the users was completed by utilizing the features. From the perspective of security implementation, CP-ABE was desired since the owner of the information could mention the policy on his/her without any restriction towards the encryption of information.

The benefits imparted by CP-ABE:

1. One of the major benefits that's given by CP-ABE was cluster key administration [8].
2. It would lessen the overhead in the interactions and gave rise to enhanced information access command.
3. The most notable in it was segregating of abstract features from real-time keys.
4. Rather than developing encryption of the type "one-to-one", it gave rise to encryption of the type "one-to-many". This makes it to be a favorable tool to sort out the issue of protected and enhanced distributed access command over information and its sharing.

Despite CP-ABE having several benefits, it also tends to have a few limitations, which will be discussed below:

1. It incorporated high-cost incurring overheads indulging re-generation of key, re-encryption of ciphertext, and re-distribution of the key once the policy update or feature revocation takes place.
2. Both policy update and revocation processes need to be carried out with utmost care since the chance for propagation consequences towards decryption of both user and ciphertext was higher.
3. In particular, the cost incurred for both the interaction and estimation associated with the update of the key was higher whenever the count of users was larger in numbers.
4. The cost expended for both the re-encryption of information and the update of policy was an unnecessary burden for the owner of that information, whereas the cost expended for interactions were found to be related with the counts of ciphertexts to be re-uploaded and downloaded to and for from the information outsourcing surrounding. These kinds of overheads were found to result in ineffective execution for practical information sharing situation.
5. Furthermore, there was a possibility for the unavailability of encryptors once there's requirement of update in access policy.

Based on the realized limitations, there exist the scope for improvement in the outsourced cloud surrounding. In particular, the health sector related outsourcing has even more scope for improvements. These scopes for improvement are discussed below:

1. A better access administering methodology is needed indeed for handling PHRs records by containing lesser weight for the update of policy in several authority information outsourcing surroundings.

2. A need for devising a policy versioning approach exist to permit re-construction of every earlier policy version and excellent recording of every update event, thereby comprehensive investigation is possible anytime.
3. There exists requirement for deploying parallel programming for the sake of parallelizing every crypto process in the system of PRE-Proxy Re-Encryption.
4. Finally, there is a stringent need for the performance and security perspective investigation to differentiate the effectiveness of any devised schema.

## 2 Literature Review

The Identity-Based Encryption (IBE) method known as Fuzzy Identity-Based Encryption was introduced [7]. An identity was seen as a collection of descriptive qualities in Fuzzy IBE. The fuzzy IBE scheme can decode the ciphertext in which the private key of identity $\omega$ was encrypted with identity $\omega_0$ only if identities $\omega$ and $\omega_0$ are close to each other, as determined by the "Set Overlap" distance metric. Will be Since biometric IDs always contain some noise when scanned, a fuzzy IBE scheme can be used to enable encryption using the biometric input as the ID. This is possible because a Fuzzy IBE scheme has the error-tolerance quality that makes it possible to employ biometric identities. It was also demonstrated that Fuzzy-IBE may be applied in a scenario known as "attribute-based encryption." There are two fuzzy IBE scheme constructions discussed in this study. The structures may be seen as an Identity-Based Encryption of a message beneath various aspects that make up a (fuzzy) identity. Both error-tolerant and protected against collusion attacks, IBE techniques were efficient. In addition, no random oracles are employed in the fundamental design.

The Selective-ID security model's ability to protect schemes from the attack was demonstrated. A user shouldn't have access to data in some distributed systems unless they have a specific set of credentials or other qualifications. The only way to enforce these rules now is to use a trusted server to store the data and handle access control. The data's privacy will be jeopardized, though, if any server used to store it is hacked. A system called CP-ABE was proposed in this work for implementing complicated access control on encrypted data [9]. Even if the storage server is unreliable, encrypted data may be kept private by employing the suggested procedures, and our solutions are also safe from collusion assaults. Our system uses attributes to describe user credentials and the party encrypting the data chooses a policy of who can decrypt it, whereas previous ABE systems used attributes to written data and incorporated the policy into the user's key. As a result, the techniques were conceptually more similar to conventional access control techniques like Role-Based Access Control. An implementation of the system was also offered, and it provides performance metrics.

The PU-ABE encryption method, which supports effective access policy updates, was a novel variation of key policy attribute-based encryption. It records properties for access policies that are added and removed. There were several ways that PU-ABE contributes. First, it examines the encryption-related policies, which may be altered without re-encrypting data or necessitating secret key exchange between the cloud server and the data owners. Then, PU-ABE guarantees that outsourced data will be kept private and

will be subjected to precise access controls. And finally, there were minimal communication and storage costs since the ciphertexts got by the end user were of a fixed size and irrespective of the number of characteristics used in the access policy.

This article [10] explores the evolution of systems that can store large amounts of data and handle a high rate of user access requests. When creating a safe large data storage service, one of the most important privacy factors to be taken into consideration is the anonymity of the service users. Additionally, the service must be capable of offering realistic and fine-grained encrypted data sharing, allowing a data owner to permit the sharing of ciphertext of data among others under certain predefined circumstances. To accomplish the aforementioned qualities, the research effort firstly presented a privacy-preserving ciphertext multi-sharing technique. A ciphertext may be safely and conditionally exchanged several times using this method, which combines the advantages of proxy re-encryption and anonymity without compromising the confidentiality of the underlying message or the senders' or receivers' identities. The study also demonstrates that the new primitive was protected in the standard model against chosen-ciphertext attacks.

Granular and simple access control for mobile cloud environments was supported by the Lightweight Collaborative Ciphertext Policy Attribute Role-Based Encryption (LW-C-CP-ARBE) system. In order to lower the cost of data re-encryption and decryption for mobile users, the CP-ABE technique was implemented as fundamental cryptographic access control. Because of this, there is little overhead while performing cryptographic operations on end-user hardware. The development of a secure access policy sharing, and re-encryption protocol allowed users with write privileges to change the data and ask the proxy to re-encrypt it. In order to show how effective and useful our system is, the evaluation and experiments were provided last [11].

With the help of Attribute-Based Proxy Re-Encryption (ABPRE), a semi-trust proxy can change the ciphers governed by one access policy to the ciphers governed by another access policy without disclosing details about the underlying communication. Such a foundation enables fine-grained and secure cloud exchanges of encrypted data. A re-encryption key in a key policy variant is associated with an access tree that identifies the categories of ciphertext that can be re-encrypted. Only two efforts to implement KP-ABPRE have been undertaken, one of which satisfies Repayable Chosen Ciphertext Security (RCCA security), and the other of which asserts to be Chosen Ciphertext Secure (CCA secure). The results of the investigation indicate that both systems were open to RCCA and CCA attacks, respectively. In this study, a selective CCA secure KP-ABPRE method was further proposed. The suggested method becomes the first KP-ABPRE technique to fulfill the selective CCA security because the attacks on two currently used RCCA secure and CCA secure schemes were proven in the literature. The planned structure was demonstrated to satisfy collusion resistance. Additionally, based on the Bilinear Diffie-Hellman exponent assumption, the suggested system was shown to be collusion resistant and selective CCA secure in the random oracle model.

An effective technique for updating access policies that use small size ciphertext was suggested in the research paper [12] This scheme's KP-ABE foundation restricts data owners' capacity to define their own access policies. A useful policy update and file update in the context of CP-ABE were proposed in the scientific study. Using the key update that the data owner generated, the ciphertext components are modified. The researchers suggested a ciphertext update approach to manage policy updates in the cloud server in two separate studies [12, 13]. In the form of a Linear Secret Sharing System (LSSS), they provided algorithms for adding and deleting characteristics in the AND, OR, and threshold gate of the ABE policy after examining the policy updating cost [10]. Using the encryption method of the fundamental CP-ABE scheme, Yuan published a policy update algorithm [14] that was based on the matrix update algorithm [18] then it was suggested to perform a multi-keyword search across CP-ABE with dynamic policy updates. This method updates the policy using the existing policy's encryption data without selecting a new secret value.

## 3 Proposed Methodology

The technique suggested in this paper is developed based on PRE and CP-ABE. A mechanism for policy versioning is also shown to provide complete traceability of policy changes.

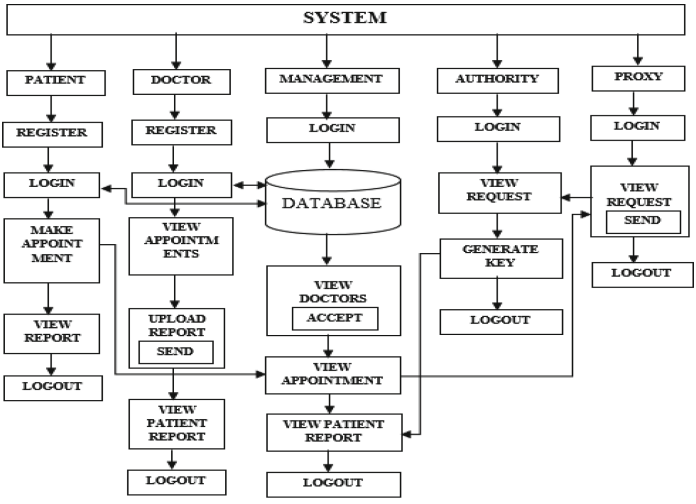


**Fig. 2.** Block Diagram of the Proposed Methodology

The Fig. 2 depicts the block diagram of the proposed methodology.

The Fig. 3 represents the architecture of the proposed methodology This paper finds a way to effectively change CP-ABE access control without requiring new encryption schemes on the part of the data owner. The idea that the PHR is shared. Patients who own their data can choose to share it with certain others. Symmetric encryption is used to

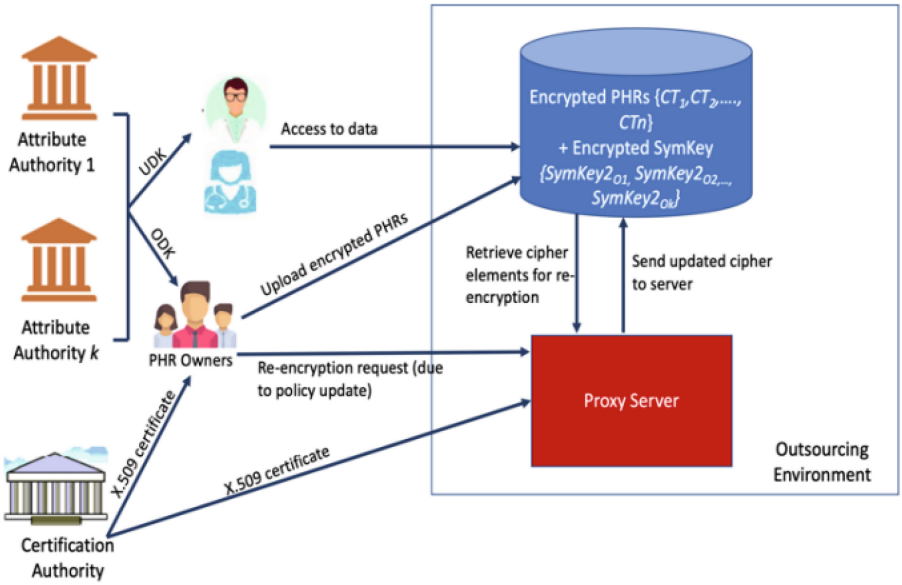


**Fig. 3.** Architecture of the Proposed Methodology

encrypt data as it offers good cryptographic performance. Symmetric keys are encrypted using CP-ABE technology to provide effective encryption and enhanced performance of data access and policy updates. Because CP-ABE technology is used to encrypt symmetric keys, the policy update cost only affects encrypted symmetric keys. So, there is no need to re-encrypt all ciphertexts. This greatly reduces the computational effort on the proxy side. Technically, the PRE protocol is designed to manage ciphertext re-encryption, which represents a significant cost for policy updates. Its advantages are accuracy is good, low complexity, high computation, and no need for skilled persons.

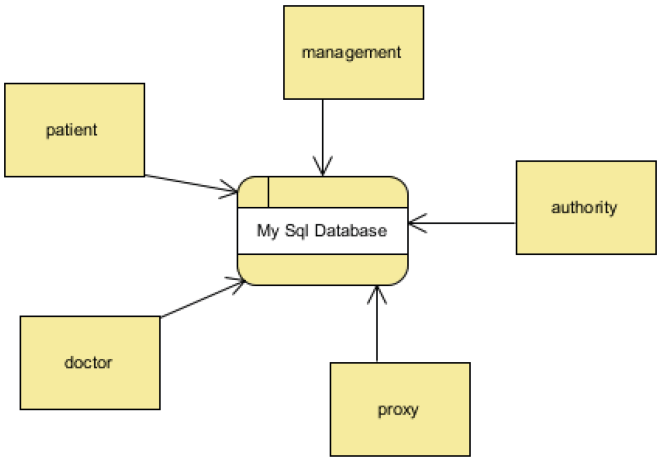


**Fig. 4.** Data Flow Diagram representation of Level-0

In Fig. 4, the level-0 DFD representation is shown, here all the modules such as patient, doctor, hospital management, authority and proxy server are capable of transmitting the data to My SQL Database.

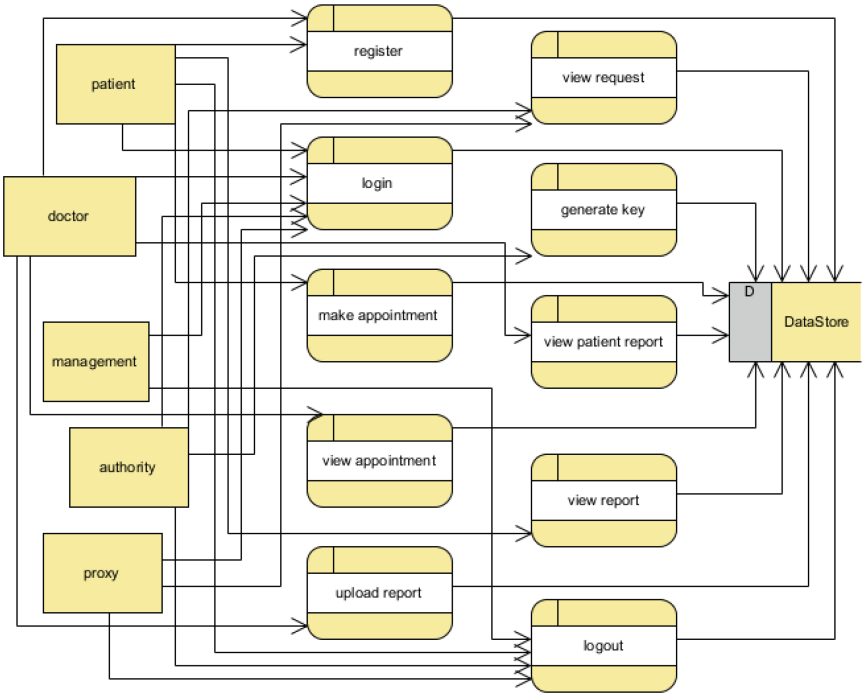


**Fig. 5.** Level-1 DFD Representation

In Fig. 5, the level-1 DFD representation is shown, here all the modules such as patient, doctor, hospital management, authority, and proxy server separately transmit the data to a certain set of suitable operations like register, login, view, generate, upload, and logout after that the corresponding the responses are transmitted to the datastore block.

In Fig. 6, the level-2 DFD diagram is shown, here all the modules such as patient, doctor, hospital management, authority, and proxy server separately transmit the data to a certain set of suitable operations like register, login, view, generate, upload and logout. After that, the corresponding response coming from the entire block consisting of all these operations is transmitted to the datastore block and receives some data from the datastore block.

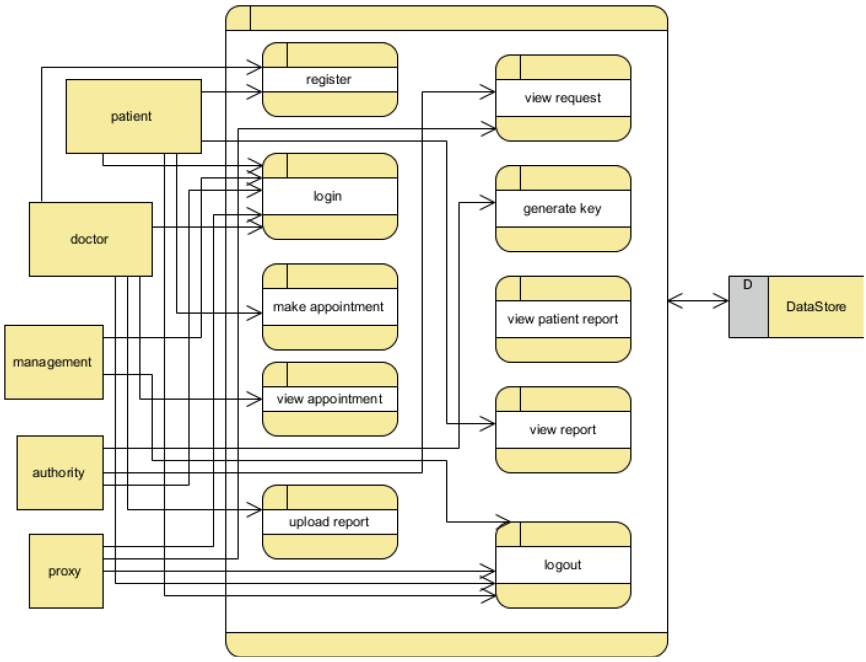


**Fig. 6.** Level-2 DFD Representation

## 4 Software Design

Unified Modeling Language (UML) is a regulated general-purpose modeling language in the field of object-based software engineering. Rules are maintained and generated by the Object Management Group. The UMLs are aimed to be a usual language for generating models of object-based computer software. It consists of two main elements: a Meta-model and a notation.

In Fig. 7, a use case representation is a form of behavior representation that is elucidated by and generated from a Use-case investigation. It exists to show a pictorial schema of the capability given by a system.

Figure 8 shows a class representation is a kind of static arrangement representation, which reports the arrangement of a system by presenting the classes, attributes, processes, and associations between the classes in the system. This representation shows the class that comprises data.

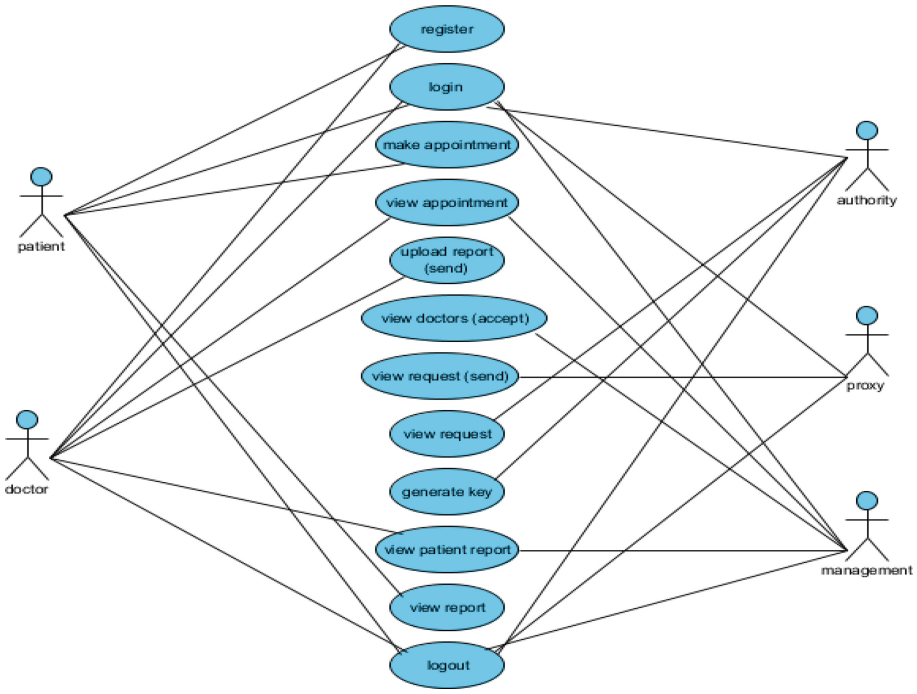


**Fig. 7.** Use Case Representation

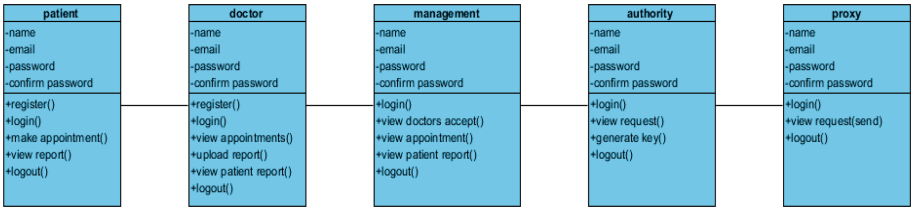


**Fig. 8.** Class Representation

The Fig. 9 depicts a sequence representation is another type of communication representation presenting the way in which operations processes operate with each other and the way of their arrangement. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

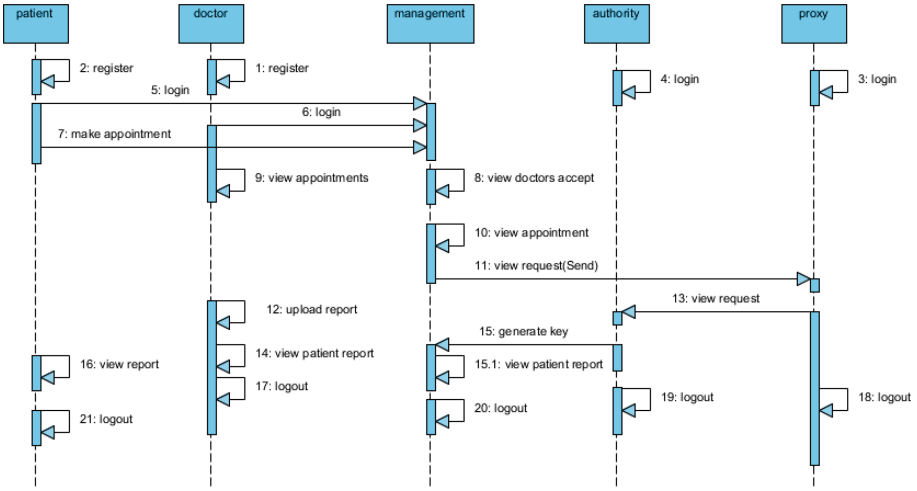


**Fig. 9.** Sequence Representation

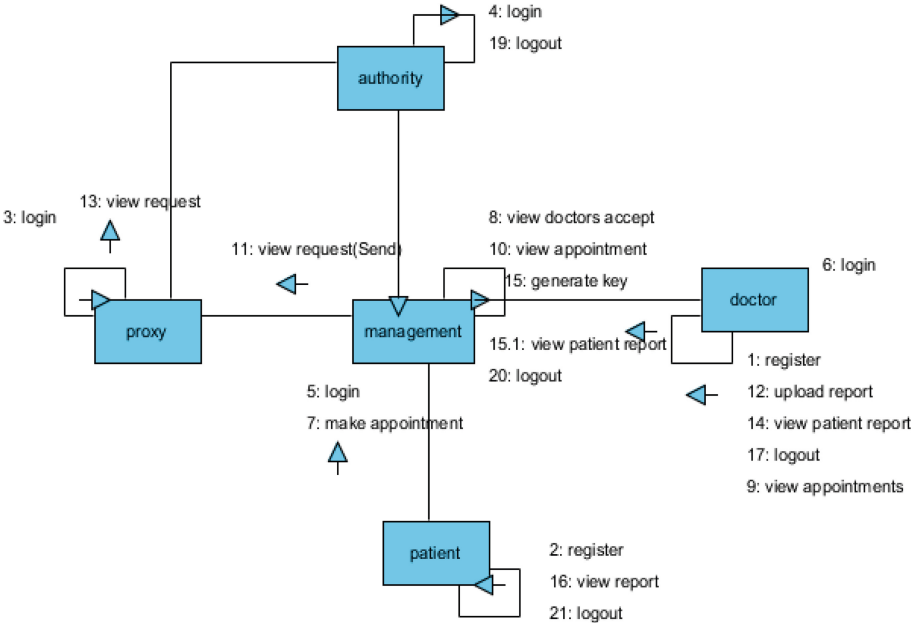


**Fig. 10.** Collaboration Representation

Figure 10 shows the collaboration representation, the call order of the operation is indicated with the help of a few counting processes as indicated below. The count depicts the way in which the operations are called one by one. In this work, we have considered the identical order administration system to make the collaboration representation. The calls of the operation are identical to the order representation. However, there lies one

uniqueness between the two- The sequence representation would not report the entity arrangement, whereas the collaboration representation reports the entity arrangement.

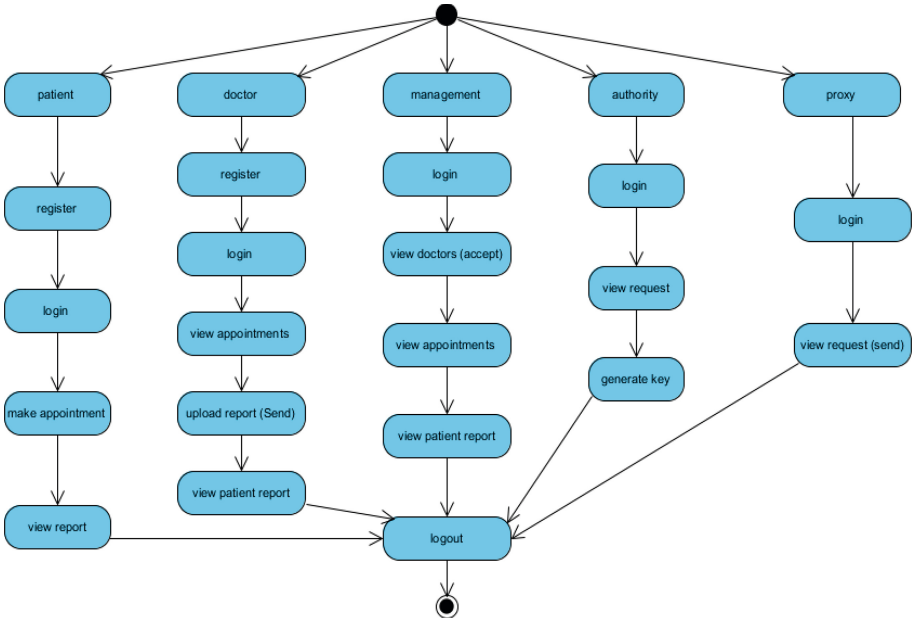


**Fig. 11.** Activity Representation

In Fig. 11, the activity representations are seen and pictorial indications of functionalities of step-by-step actions and activities by supporting concurrency, iteration, and choice. In the UML, representations of activity could be utilized to show the commercial and processing stepwise functionalities of elements contained in a system. This representation exhibits the entire control flow.

## 5 Testing and Validation

**Table 1.** Test cases.

| Input | Output | Result |
|---|---|---|
| Input text files | File upload or not | Success |

The Table 1 represents the test cases for the performance estimation of the project.

**Table 2.** Test Cases Model Building.

| S. No | Test cases | Input | Expected Output | Actual Output | Pass/Fail |
|---|---|---|---|---|---|
| 1 | Read data | File data | Data read successfully | Data read success | P |
| 2 | Performing Encryption on file data | Encryption has to perform on file data | Encryption should be performed on file data | Encryption successfully completed | P |
| 3 | Generating Key pair | Key has to generate | Key will generate | Key Generated successfully | P |
| 4 | Cipher text | File data Encrypted data will Decrypt | Data should be decrypt | Data decrypted successfully | P |

The Table 2 depicts the test cases that is used for model building to estimate the performance of the project.

## 6 Conclusions and Future Work

Currently prevailing commercial cloud mode platforms gave rise to the public key or symmetric encryption as an add-on for aiding the confidentiality level of the information pertaining to the users. Also, to sort out realized issues in the past, ABE [7] were widely deployed by several investigators as conveyed earlier. "One-to-Many" basis encryption schema along with enhanced access command was imparted by such similar methodologies. Thus, these methodologies had the abilities of both access command and encryption. Owing to which, as a contour effort and redressing the earlier issues, this paper has successfully devised a schema of update for policy based on proxy re-encryption and policy outsourcing operation. It entirely unloaded the cost incurred for the update for policy that is to be carried out in the server that's outsourced. The re-encryption that has devised is found to aid the bigger scalability and enhanced the overall entity performance. Furthermore, the patient can successfully be able to decrypt the data using the key and also the doctors and the hospital can be empowered to view the patient data for any kind of emergency purposes.

The major contributions of this paper are (a) A better access administering methodology for handling PHRs by having lesser weight for the update of policy in several authority information outsourcing surroundings. (b) A devising a policy versioning approach to permit re-construction of every earlier policy version and excellent recording of every update event for carrying out the comprehensive investigation in the time as per the choice. (c) This paper made use of parallel programming for the sake of parallelizing every crypto process in the system of PRE. Finally, (d) it executed a comprehensive performance and security perspective investigation to differentiate the effectiveness of any devised schema.

After performing experimentation, used Graphical User Interface (GUI) tool during the implementation of update for policy in CP-ABE. By using the web-oriented tool,

the updates pertaining to the policies are made possible anywhere and anytime. Thus, at the onset, proposed devised methodology provided a clear access command for the policy update administration and file storage entity. Furthermore, the screenshots are taken and presented to show how every module like a patient, doctor, management of the hospital, proxy server, and authority along with its authority levels are organized after the successful implementation of this application. In this result analysis of this study presents the output screenshot to demonstrate the manner in which the application operates in order to secure the PHRs in the outsourced cloud surrounding, which served as a flexible tool for patients, doctors, and anyone in the medical care system.

In the future, we hope to use the Elgamal algorithm to conduct large-scale experiments to test cloud-oriented proxies with more information and larger access policies in real cloud environments.

## References

1. Le, D.N., Seth, B., Dalal, S.: A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach. J. Cyber Secur. Mobility **7**, 379–408 (2018)
2. Pundkar, S.N., Shekokar, N.: Cloud computing security in multi-clouds using Shamir's secret sharing scheme. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (2016)
3. Sareen, S., Sood, S.K., Gupta, S.K.: Towards the design of a secure data outsourcing using fragmentation and secret sharing scheme. Inf. Secur. J. Global Perspect. **25**, 39–53 (2016)
4. Jain, A., Soni, B.K.: Secure modern healthcare system based on internet of things and secret sharing of IoT healthcare data. Int. J. Adv. Networking Appl. **8**, 3283 (2016)
5. Hossain, M.A., Hossain, M.B., Uddin, M.S., Imtiaz, S.M.: Performance analysis of different cryptography algorithms. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **6** (2016)
6. Gupta, P., Koushal, V., Narayan, C., Anand, A.: Building genetic database at medical institutes: implement patient cost audit and improve biomedical research. Ann. Neurosci. **24**, 3-4 (2017)
7. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy (SP 2007) (2007)
8. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
9. Cheung, L., Cooley, J.A., Khazan, R., Newport, C.:Collusion-resistant group key management using attribute-based encryption. Cryptology ePrint Archive (2005)
10. Belguith, S., Kaaniche, N., Russello, G.: PU-ABE: lightweight attribute-based encryption supporting access policy update for cloud assisted IoT. In: IEEE 11th International Conference on Cloud Computing (CLOUD) (2018)
11. Liang, K., Susilo, W., Liu, J.K.: Privacy-preserving ciphertext multi-sharing control for big data storage. IEEE Trans. Inf. Forensics Secur. **10**, 1578–1589 (2015)
12. Fugkeaw, S., Sato, H.: Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing. Int. J. High Perform. Comput. Network. **9**, 299–309 (2016)
13. Liang, X., Cao, Z., Lin, H., Shao, J.:Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (2009)
14. Yuan, W.: Dynamic policy update for ciphertext-policy attribute-based encryption (2016)