**A Secure Framework for Record Exchange Between Medical Institutions**

G. Senthil Kumar¹, S. Anuja¹, M.R. Sudha¹*, Anuj¹ and Ajay.D¹

¹ Department of Software Engineering, SRM Institute of Science & Technology, Chennai 603203, India.
¹* Department of Computer Applications, Faculty of Science and Humanities, SRMIST, Chennai 603203, India.

Abstract: The Personal Health Record (PHR) is a framework of health information exchange. In the digital age, hospitals and medical institutions are moving to an online platform to store the medical record of patients because physical storage has become quite labor-intensive, expensive and also very inconvenient in terms of maintenance and retrieval while online storage overcomes those obstacles. But there are still numerous privacy concerns as confidential health information may be accessed by unauthorized people. Storage of medical records and other patients related information on third party servers may be vulnerable to breaches as third-party servers usually do not possess a lot of security. To assure the patient's authority over to their PHRs, this method is used, to encrypt the PHRs before storing on a server and that data is linked with the blockchain. In this paper, we propose a model and mechanism for control of data access to Personal Health Records stored on the cloud. To achieve efficient data access control for Personal Health Records, we use AES and SHA algorithm as an approach to encrypt each PHR file. The analysis and results exhibit the security and efficiency of our proposed scheme.

**Keywords:** Cloud data; encryption; hashing; proxy re-encryption.

1. **INTRODUCTION**

Cloud storage is an emerging technology in a world where everything is turning digital. Cloud is defined as a group of servers that are accessed over the internet, the database and the software that runs it. These servers act as data centers and are placed throughout the world and eliminate the need and use of physical storage space. Thus, the cloud is used for data storage purposes across various domains and industries.

There are four different types of cloud servers i.e. Private, Hybrid, community and Public. Private cloud servers are those that host all our computing infrastructure in-house and are not shared. The security level and control are the highest while using a private network. A hybrid cloud uses a blend of private and public clouds, depending on their use. Community clouds are shared among organizations that have a common goal. Lastly, public clouds are those that are maintained by a third-party organization and the computing infrastructure is situated at the company’s premises.
However, the cost of setting up a personal in-house cloud server is high and not every individual or organization can afford to pay for it as it requires a very sizeable investment and huge outlays. Apart from the above, storing information on an in-house server also requires efficient training and highly skilled staff for maintenance and recovery of the said cloud server and the data that is stored on it. Organizations usually rent out third-party servers wherein they completely trust third-party servers to store, maintain and handle their sensitive information. While these third-party servers are very cost-effective and do not require the hiring organization to maintain them, they do not have complete control over their stored data. They would also require more investment as and when storage space runs out which could prove to be a financial burden in the long run. Also, third-party cloud storages are vulnerable to both internal and external threats such as an internal leak, unauthorized access and more which may lead to unforeseen breaches such as theft, loss, and leakage resulting in the loss of confidential information such as medical, personal and financial data that is stored on them and shared on an untrusted cloud leading to privacy transgression.

Several methods have been utilized to ensure the confidentiality of the Personal Health Records stored on cloud servers. Those approaches make sure, integrity, confidentiality, accountability and authenticity. Integrity makes sure that the data is not modified, whether during transit or while cloud storage whereas confidentiality ensures that the personal health record is hidden from unauthorized users. Authenticity makes sure that the personal health record is accessed by authorized users only, whereas accountability calls attention to the fact that agreed-upon procedures should be complied with [1].

In this paper, we propose a system that uses a semi-trusted proxy server with SHA and AES algorithms for key generation and encryption of data. The system also proposes a mechanism for access to Personal Health Records in a cloud system. It also enables the patient to have authority over granting access to those files which can then viewed, added or modified by agents with an access [2].

A semi-trusted proxy server (so-called because it cannot be completely trusted) is a hybrid type of a cloud server that combines attribute-based encryption with proxy re-encryption to render data confidentiality and fine-grained access control while storing encrypted information on the cloud. This semi-trusted proxy server would encrypt the data files at the server end and only store the files on the cloud [3]. After encryption each data attribute is stored in a blockchain. With the use of the blockchain, encrypted data can be converted into a hash code using cryptographic technologies and generate a key value. This way even if there is a breach the files would still be encrypted and there would not be a loss of sensitive or critical information.

2. RELATED WORKS

Attribute-based proxy re-encryption scheme (ABPRE) is a modern Cryptic scheme that expands the conventional proxy re-encryption technique to the attribute-based equivalent and hence permits a user with consigning capability in an access control environment [4]. Entities, recognized by attributes, can candidly assign a proxy that can re-encrypt a ciphertext associated with certain access policies to some other ciphertext with a slightly different access policy. Proxy re-encryption was proposed to allow a user to assign a proxy capable of translating the ciphertexts. This is well embedded into traditional cryptosystems together with identification-based and public key settings. All advantages of the Proxy re-encryption scheme can be included in the access control environment. The security model of the Attribute-based proxy re-encryption scheme was elucidated for the very first time and the scheme proved selective-structure chosen plaintext secure and master key secure in the standard model. The focal point of healthcare has moved from paternalistic to a patient-centric approach. The patient is educated about their health information, in this approach. They are inclined towards understanding, following instructions and asking more intuitive
questions. Allowing patients to control access to their records will motivate them to more involved in their healthcare. This will reinforce the patient-provider relationship and intensify the efficacy of healthcare management. They were provided with a concrete instantiation of the said system. A simulation result for it was also given. The mechanism proposed in this paper does not only target PHR but can also be used in other areas such as data sharing or secure vehicular communication.

Cloud computing reinforces collaborative and mobile services and applications. Reduced cost area flexibility, high automation, and increased storage are some advantages offered by it. Delivery of services by healthcare can be improved by the help of cloud computing. In this paper, the service and categories models of cloud computing, its, diverse applications, technological intellect in healthcare and medical services, and biometrics-based authentication for information security were presented. It also presented issues related to blockades to applications, privacy, concerns about security, etc.

Cloud computing is an upcoming paradigm in which resources are provided as services over the internet. It is quite likely that the data that is stored in third-party clouds is not as secure as the one that is stored in-house [5]. To overcome this hurdle existing solutions usually apply different cryptographic methods to encrypt data and keep it confidential. But with this comes a huge computational overhead as the owner is responsible for the distribution of keys and management of data if he desires fine-grained access control and thus cannot be scaled well [6]. This is overcome by defining the access policy and delegating the computational tasks involved in the untrusted cloud servers without actually disclosing the data content.

A new strategy is suggested, together with a Diffie-Hellman key distribution scheme and asymmetric cryptosystem. The security of both systems depends upon the fact that calculating discrete logarithms over limited fields is exhausting. This paper described a symmetric cryptographic system and a signature strategy based on the fact that calculating discrete logarithms is hard over finite fields. Although the system is tough to crack, the drawback of the key distribution scheme used i.e. Diffie-Hellman makes it susceptible to the man in the middle attack and it can be possible that the key generated and used for the symmetric cryptosystem is not completely random [7]. If the estimated time for calculating discrete logarithms and integer factors so far remains the same, then, the size of the ciphertext for the same security level as RSA system will be twice, and similarly, the size of the public key file will also be double which is not feasible as performance and storage will be taking a hit since larger size requires more time to decrypt. Due to its countless advantages cloud computing is recently impacting people’s way of living life and working standard. However, the protection of cloud computing is forever a blockade for its worldwide applications and concern of various likely cloud customers. To ease customers to see the security affairs of cloud computing and bestow some efforts to enhance the security level of cloud computing, they surveyed the pre-existing security paradigm of cloud computing and gathered the main security concerns of cloud computing attaining from various organizations [8]. And then gave the few security tactics from the point of view of security and operation and incident response to mitigate the traditional security problems of cloud computing. Cloud computing is a form of computing model that allows anyone from anywhere to access a remote server that has a dynamic set of hardware that is provided hastily and on-demand that requires the least amount of involvement and control. However, the superiority of cloud computing is obstructed by the means of protection to a substantial extent. To contribute an attempt in enhancing the safety of cloud computing, they examined the principle current safety fashions of cloud computing and summed up the primary safety issues of cloud computing from specific organizations. Finally, they gave some safety strategies towards these common protection troubles of cloud computing. In the future, they can accomplish these security techniques with management and the future era. Cloud technology has brought a lot of transformations to data storage for both individuals and organizations. Cloud offers
flexibility for data storage, access, and recovery, but it is not immune to the security challenges associated with other ETs. There have been concerns about data integrity and privacy of cloud customers. Service attack, spoofing identity, and unauthorized access to data. These attacks are often orchestrated by insiders and outsiders and can compromise the confidentiality and integrity of cloud data. Most educational institutions are digitalizing their data which are ultimately moved to the cloud to be managed by a third party. Considering the sacred nature of educational data, the study examines the implications of cloud security challenges on education. The study established that cloud computing has become a force in education but some security challenges associated with it remain a major source of concern to users. Cloud security issues obstruct the successful implementation of cloud technology in education, and they compromise the privacy and confidentiality of cloud users. Many educational institutions have migrated to the cloud to facilitate their activities. However, the increasing security issues in the cloud are capable of discouraging educational institutions from adopting the technology. Consequently, there is a need to strengthen cloud security system to eliminate cloud threats. This will enable customers to maximize the potential benefits of cloud technology. Cloud technology will play an important role in the future of education but stakeholders must find a way to tackle the associated security risks to optimize its benefits. Storing private on a third-party server has financial and maintenance advantages but it also has serious disadvantages. The data stored on untrusted third-party servers are prone to breaches and data leakages due to disclosure of data by the service providers or external unauthorized entities. A solution to this would be to enhance the privacy of a semi-trusted proxy server by redefining its control policies and using a proxy re-encryption mechanism. The issue left behind by this proposed solution is that it contains inconsistencies and authorization conflict.

3. SECURE FRAMEWORK FOR RECORD EXCHANGE

In the current cloud environment, personal health records of the patients are stored in a local server that provides flexible access for both professional users such as doctors, surgeons as well as personal users like friends and family, but this flexibility makes the system susceptible to theft and attacks and the confidentiality of the records is at risk [9]. We propose a platform that gives the access right of the personal health records in the hands of the rightful patient. We also use a separate server to just store the encrypted data, while the key generation takes place in a separate server [10]. AES along with the SHA algorithm is used to secure the data. In this system, the data are the patient records which are first hashed with SHA and then the hashed data is further encrypted with AES this provides both encryption and authentication. When the doctor enters and submits the patient data into the system, the server generates the hashed value and then the hashed value is used as input for the AES algorithm to encrypt and that data is finally stored into the cloud server with is separate from the proxy re-encryption server. A random key is generated every time any user requests to access the private data, the data is decrypted with the key which is used to grant access, this key is in the form of OTP if it matches, the user can view the data, else the permission is denied. Figure 1 shows the architecture diagram of the proposed system.
3.1 Access granting process:
Any user who wants to access the records put in the ID and submit it to request access, an OTP is sent to the patient’s mobile number this OTP is used to grant access to any user including the patient itself to view the record and update it.

3.2 Encryption:
When the doctor saves the patient data, the system generates the key and encrypts the data using AES and then the data is finally saved into the cloud-hosted database. The database has only the data in an encrypted format, no key or any other sensitive information is saved in the cloud database.

3.3 Key Generation:
Whenever encryption or decryption is done a key is required to perform those actions and this module is responsible for that it generates a random key which is SHA hashed so that the key is secure and this key is used for authenticating the user.

3.4 Data Access:
This is responsible for the interaction with the data present in the database. This data is partially the personal health records of the patients and partially is the hospital’s doctors and dean information like personal details, contact details, login information, etc.

3.4.1 Key Generation:
First the keygenerator class is used to associate it with AES. Then a random key is generated and key size is specified. Finally the new secure key is generated by using the “generateKey()” method, which is shown in figure 2.
3.4.2 Hashing:
First, the key is converted to UTF-8 format, then a message digest is set for SHA-1, then the UTF-8 converted key is converted to a digest and finally secretKey is set to output the AES, which is shown in figure 3.

```java
generateKey();
}
```

**Figure 2 - Key generation**

3.4.3 Encryption:
The secret key and string to encrypt is passed in the function. The function then creates the initialisation vector i.e. random key that is prepended to each encrypted string. Then finally output format is set to UTF-8 and input is of hex code in base64 format. This will return encrypted string, as shown in figure 4.

```java
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
```

**Figure 3 - Hashing**

3.4.4 Decryption:
The secret key and string to decrypt are passed in the function. The function then creates the initialization vector i.e. bytes size (round key). Then finally output and input format is of hex code and base64 format. This will return the decrypted string, as shown in figure 5.

```java
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
```

**Figure 4 - Encryption**

**Figure 5 - Decryption**
We propose a secure platform where medical institutions can securely share patient records. This system consists of an online platform that is used to access and store information. The platform is built using HTML, CSS, and JSP as front-end languages and SQL as a back-end language. The proposed platform aims to store data on the server securely in an encrypted manner with the use of a combination of Advanced Encryption Standard Algorithm and Simple Hash Algorithm to apply two layers of security to the said data. AES is one of the fastest and most secure algorithms in use today. Other proposed systems use only one algorithm and not two or more. Our system uses a combination of both where SHA is known to be irreversible and AES is used as an industry standard when it comes to encryption as it is fast, robust and reliable. While previously proposed methods saved the data locally, our system stores only the encrypted data on a cloud and hence in cases of the breach only the encrypted file will be exposed and not the plaintext as it requires a key to be decrypted. As a result, the data remains secure. AES 128 is super-fast and efficient. Either 192 or 256 bits are used for heavy-duty encryption but can be slow when compared to the 128-bit but the delay is negligible and the performance in terms of security makes up for it. SHA is impossible to reverse without using brute force which is infeasible. Hence it can be said that SHA is used for authentication and AES is used for encryption.

4. RESULTS AND ANALYSIS

| Modules                  | Execution Time (ms) |
|--------------------------|----------------------|
| AC Validation            | 698                  |
| ACG                      | 0.08                 |
| Server Starting          | 4180                 |
| Hospital registration – 80kb | 1478                |
| Doctor registration – 16kb | 1190                |
| Patient registration – 32kb+16kb | 1073               |

Figure 6 - Analysis of encryption time with fixed-size data
Figure 7 - Key generation.

Figure 8 - Encryption time for fixed-size data

Figure 9 - Decryption time for fixed-size data
In figure 6 and figure 7, 8, 9, AC Validation represents data decryption and authentication. Since our patient records are of consistent size the encryption and decryption process take close to a second to finish the process and is much predictable which is what a system needs and our system achieves it successfully. The related data is shown in Figures 6, 7, 8 and 9.

5. CONCLUSION

In the current scenario most, medical institutions are using third-party servers which are not exactly secure and are prone to breaches and data theft whereas moving to a privately owned cloud server is financially expensive and most medical institutions can afford to get one. Apart from the financial constraints there are other complexities such as maintenance and scalability with which low-end medical institutions cannot deal with. We propose a system that uses a semi-trusted proxy server that encrypts data beforehand using AES and SHA encryption and authentication algorithms and stores them on a cloud server which can be accessed through the platform with the authorization of the patient. This would result in a more secure and reliable record exchange mechanism which gives the patient the right to grant authorization for viewing their medical records.

REFERENCES

[1] M. Ali, A. Abbas, U. Khan and S. U. Khan, “SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud”, pp-02, July 2018.
[2] Man Ho Aua, Tsz Hon Yuenb, Joseph K. Liu, Willy Susilod, Xinyi Huange, Yang Xiangf, Zoe L. Jiangg. “A General Framework for Secure Sharing of Personal Health Records in Cloud System”, 2017.
[3] Amal Alsubaih, Alaaeldin Hafez. “Privacy Preserving Model in Semi-Trusted Cloud Environment”, 2013.
[4] X. Liang, Zhenfu Cao, Huang Lin, and Jun Shao, “Attribute Based Proxy Re-encryption with Delegating Capabilities”, 1985.
[5] Omoyiola Bayo Olushola, “Strategies for Securing Cloud Services”, 2019.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable and fine-grained data access control in cloud Computing”, 2010.
[7] Taher elgamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, 1985.
[8] Edeh Michael Onyema, Nwafor Chika Eucheria, Ugwugbo Ann Nneka, Rockson Kwasi Afriyie, OgbonnayaUchenna Nwoye, “Cloud security challenges: implication on education”, 2020.
[9] Lidong Wang, “Medical Applications and Healthcare Based on Cloud Computing”, 2013.
[10] Man Ho Aua, Tsz Hon Yuenb, Joseph K. Liu, Willy Susilod, Xinyi Huange, Yang Xiangf, Zoe L. Jiangg. “A General Framework for Secure Sharing of Personal Health Records in Cloud System”, 2017.