A patient Centric Framework using Anonymous Authentication with Multi-authority Access Control for Personal Health Record

Mrs. Sabana Sali[1], Mr. Prasannakumaran K.S[2]
[1]M.Tech Student, Cyber Forensics and Information Security,
College of Engineering, Kallooppara. Pathanamthitta, Kerala, India
[2]Assistant Professor, Department of Computer Science and Engineering
College of Engineering Kallooppara, Kerala, India [1]

Abstract

Confidentiality is something that every person desires in their daily lives. At some point in their life, everyone will visit a hospital. Patients can visit many hospitals, and each time they do, they must submit personal information with hospital officials, and each hospital has its own registration technique. No hospital ever shares a patient's personal information with another hospital. There is a potential that hospital databases may be hacked, allowing access to all of a person's medical records, which could be utilized in social engineering. Nobody wants to share their personal information, especially their medical histories, with others. This system offers a secure means to keep one's personal health information private, and it can only be accessed with the patient's permission.

Keywords- AES Encryption, Cryptography, Personal Health Record, AWS, CP-ABE

1. INTRODUCTION

E-medical record systems are critical to the digital transformation of healthcare because they allow patients to generate, maintain, and control their personal health records (PHRs) over the internet. Nowadays most medical record services are outsourced to a third-party, such as the public cloud, to reduce local computation and communication overhead. Using cloud technology, a PHR keeps a patient's health information secured and allows doctors and patients to access it from anywhere at any time. PHR has become a backbone of every hospital since it allows them to quickly handle patient data once they arrive at the facility, as well as provide confidentiality and security of the patients' medical records. However, numerous cryptographic technologies can be used to provide security of data, such as encrypting data before uploading it to a third-party service like AWS.

Each patient is assigned a unique ID that can be used at any time when they visit various hospitals. It gives a better approach for patients to provide their information without having to share it every time. It is an OTP-based system which is more secure because data can only be seen with the data owner's consent. Medical malpractice can be avoided in a positive way in this case since doctors cannot decline a prescription after a patient visits them because the report is uploaded to the cloud as soon as it is prepared and no additional changes can be made.

2. LITERATURE SURVEY

Jinyuan Sun, Student Member, IEEE, and Yuguang Fang, Fellow IEEE introduced a paper "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems"[1], which states that in an Electronic Health Record (EHR) system, cross-organization or cross-domain collaboration occurs from time to time for necessary and high-quality patient treatment. Because cross-domain cooperation unavoidably involves exchanging and sharing relevant patient data that is deemed highly private and sensitive, a careful design of

delegation mechanism must be in place as a building block. A cooperating partner's access rights are restricted and authorization is granted using the delegation method. Patients will not embrace the EHR system until correct use and disclosure of their health data is ensured, which is difficult to achieve without cross-domain authentication and fine-grained access control. Furthermore, the granted rights should be revocable at any time during the collaboration. In this research, they present a secure EHR system based on cryptographic constructions that allows for secure sharing of critical patient data while preserving patient data privacy during collaboration. The EHR system also includes advanced mechanisms for fine-grained access control and on-demand revocation, which are upgrades to the delegation mechanism's basic access control and the basic revocation mechanism's, respectively. The suggested EHR system is shown to achieve particular goals in the cross-domain delegation scenario of interest.

The personal health record system allows patients to learn more about their health indicators at any time, but because the resources are stored in a semi-trusted cloud service provider, Fatiha Mrabti and Rachid Ben Abbou introduced a paper “Efficient Secure and Privacy Preserving Data Access Control Scheme for Multi-Authority Personal Health Record Systems in Cloud Computing”,[2] which states that While the personal health record system allows patients to learn more about their health indicators at any time, it is critical to maintain data confidentiality while providing granular, scalable, and flexible access control because the resources are stored in a semi-trusted cloud service provider. As a result, a number of methods have been presented. They present a multi-authority attribute-based encryption method with semi-outsourced decryption in this work, which can provide a scalable and secure data sharing scheme with a low computational overhead.

“Luan Ibraimi, Muhammad Asim, Milan Petko vic “ introduced a paper “Secure Management of Personal Health Records by Applying Attribute-Based Encryption”[3] which states that The confidentiality of personal health records is a major problem when patients use commercial Web-based systems to store their health data. Traditional access control systems have a number of drawbacks when it comes to enforcing access control requirements and maintaining data confidentiality. The data must be stored on a central server that is protected by an access control mechanism, and the data owner loses control of the data once it is transferred to the server. As a result, these systems fail to meet the needs of data outsourcing scenarios in which the third party storing the data should not have access to the plain data and cannot be trusted to enforce access regulations. They introduce a new ciphertext-policy attribute-based encryption (CP-ABE) technique for enforcing patient/organizational access control regulations in this study.

3. PROPOSED SYSTEM

The proposed system is a PHRs system that uses a secure sharing framework based on multiple authority attribute-based encryption. The attribute used here is the unique ID which is generated for each patients. There are different modules in which the central authority will add corresponding details and finally a unique ID is generated for the patient. The user's identity and attributes are hidden under this scheme.
The doctor's reports are transferred to the cloud, where they are encrypted with the patient's unique ID as the key. To avoid cloud servers from meddling with cipher text or misleading end users, an anonymous authentication based on attribute-based signature is proposed. The patient's Personal Health Record is protected at various levels of security. To encrypt the report generated by the doctor, an AES Encryption is employed. There is a feature that allows doctors and patients to chat, and messages are encrypted using the RSA algorithm.
The OTP-based method adds an extra layer of security since if the report needs to be viewed by a doctor, the OTP, which only the patient knows, must be disclosed to the doctor.

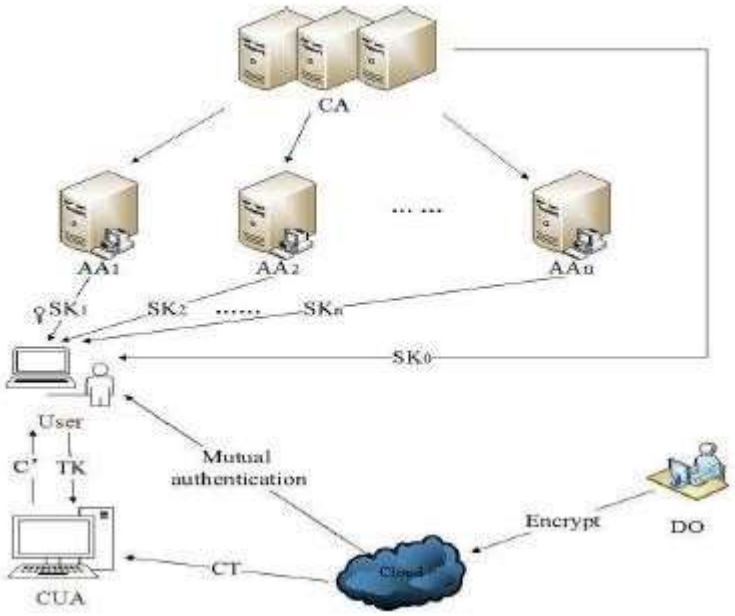

Fig 1: System model

4. MODULES

There are eight modules in the proposed system.

Admin is the top authority in the system. A country's states can be added by the administrator. Various state administrators can be assigned to various states around the country. Admin can also look up information about state administration, such as the number of registration points and registered hospitals. Some residents have made requests for them to be accepted, which the admin can also manage.

The next level is **State Admin**. State admin can create districts under each state and oversees all district admin tasks. He can also see the registration stations and hospitals that have been registered. State administrators can see some complaints filed by district administrators. The hospitals must be registered in the system, which the state administration either accepts or rejects.

State Admin oversees **District Admin**. A district's Taluk and village are managed by the district administrator. He has the ability to add and see registration points. He approves the citizen's request for a card. If a conflict arises between the district administrator and the registration point, he can file a complaint with the state administrator.

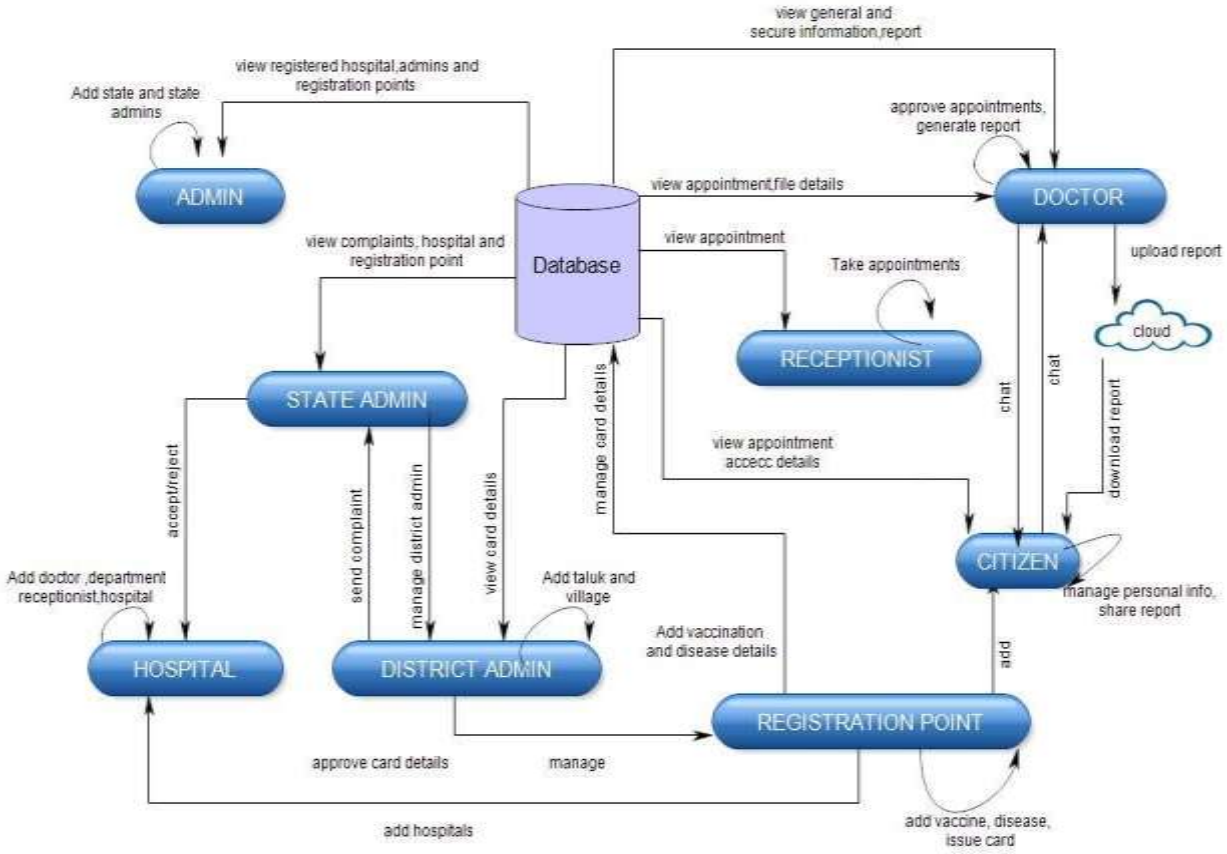

Fig 2: System Architecture

Next comes Registration **point**. This is where patients are being added. Once a citizen has been added, it must be approved by either the administrator or the district administrator. After each citizen's application is approved, a unique card ID is generated for them. When a citizen visits a different hospital, he can utilize this card ID. The registration point can additionally include information about the patient's vaccinations and diseases.

Another module is the **Hospital**. Different hospitals exist in a country, including both private and public hospitals. Hospitals can either register for themselves or be added by the registration point. Once the hospital has been listed, it must be approved by either the administrator or the state administrator. After the hospital has been approved, different departments, doctors under different departments and receptionist can be added.

The **Receptionist** module can schedule appointments for a variety of patients who come to the hospital with this one-of-a-kind card. She can also see information about the appointment, such as todays and previous appointments.

The **Doctor** is the following module. The doctor can see the appointments made for the patient by the receptionist and create a report for the patient after consulting that patient. This document is encrypted and stored in the cloud. Additionally, the doctor has access to the patient's previous report which is the report generated by another doctor. There are two different forms of data. General information can be accessed by the doctor immediately, whereas secure information can only be viewed by entering the OTP sent to the patient's email address. The doctor has access to the shared files and can provide feedback on them.

The **Citizen** is the final one in the modules. He can check the status of his appointment and get his own report following the doctor's consultation. There is an option for the doctor and the patient to converse. He

can edit or add information to his profile, as well as see who has accessed or attempted to access his data. The patient has the option of disclosing the information to several doctors.

5. CONCLUSION & FUTURE SCOPE

The suggested system is a PHRs system that uses a secure sharing framework based on multiauthority attribute-based encryption. The user's identity and attributes are hidden under this scheme, and only the trusted central authority is aware of them. An anonymous authentication based on attribute-based signature is proposed to prevent cloud servers from interfering with cipher text or fooling end users. During the entire access-control operation, only authorised users have access to and receive messages. This system has a lot of potential in the future. If effectively executed, it can save a lot of time and ensure that the patient receives proper treatment in an emergency scenario.

REFERENCES

[1] L. Tbraimi, M. Asim, M. Petkovi, "Secure management of personal health records by applying attribute-based encryption, In Proceeding of the International Workshop on Wearable Micro and Nano Technologies for Personalized Health(pHealth)," in Oslo, Norway, Jun.2009, pp.71–74.

[2] J. Akinyele, M. Pagano, M. D. Green, "Securing electronic medical records using attributebased encryption on mobile devices," in Proceeding of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Oct.2011, pp.75–86.

[3] S. Narayan, M. Gagn_e, R. Safavi-Naini, "Privacy preserving HER system using attributebased infrastructure," in proceeding of the ACM Cloud Computing Security Workshop, Chicago, Oct.2010, pp.47–52.

[4J. Lai, R. H. Deng, Y. Li, "Fully secure ciphertext-policy hiding CPABE," in Proceedings of the International Conference on Information Security Practice and Experience, Jun.2011, pp.24– 39.

[5] J. Sun, Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," in IEEE Trans.Parallel Distrib.Syst., Jun.2009, pp.754–764.

[6] M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," in IEEE Trans.Parallel Distrib.Syst., 2013, pp.131– 143.

[7] X. Liang, M. Barua, R. Lu, "HealthShare: Achieving secure and privacy preserving health information sharing through health social networks," in Comput.Commun., 2012, pp.1910–1920.

.

[8] R. Lu, X. Lin, X. Shen, "SPOC: A secure and privacy-preserving oppotunistic computing framework for mobile-healthcare emergency," in IEEE Trans.Parallel Distrib.Syst., 2013, pp.614–624.

[9] X. Zhou, J. Liu, Q. Wu, "Privacy preservation for outsourced medical data with flexible access control," in IEEE Access., Jun.2018, pp.14827– 14841.

[10] S. Jiang, X. Zhu, and L. Wang, "EPPS:Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks," in Sensors., 2015, pp.22419–22438.

[11] S. Zhang, P. Chen and J. Wang, "Online/Offline Attribute Based Signature," in Ninth International Conference on Broadband and Wireless Computing, Communication and Applications.IEEE, 2014, pp.566–571.

[12] S. Ruj, M. Stojmenovic, A Nayak. "Decentralized access control with anonymous authentication of data stored in cloud," in IEEE Transactions on Paralell and Distributed Systems, Feb.2014, pp.384–394.

[13] X. Li, J. Jiang and Y. Chen, "Fully decentralized authentication and revocation scheme in data sharing systems," in 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018, pp.680–686.