Secured Cloud Based Health Care Framework with Blockchain

Gowthamani R¹, Sasi Kala Rani K¹, G Renugadevi¹, Prithvi Kannah K¹, Suriya Prakash D¹
¹Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India
Email: gowthamanir@skcet.ac.in,18eucs523@skcet.ac.in

Abstract. PHRs are a new patient-centric model of health information exchange that is often outsourced and processed by third parties such as cloud providers. Third-party servers and unauthorised parties can have access to personal health information, causing widespread privacy concerns. Encrypting PHRs before outsourcing is a promising way to keep patients in charge of their PHRs. However, issues like privacy risks, scalability in key management, versatile access, and successful user revocation have remained the most important roadblocks to achieving fine-grained, cryptographically enforced data access control. We use attribute-based encryption (ABE) techniques to encrypt each patient's PHR file in order to achieve fine-grained and scalable data access control for PHRs. We concentrate on the multiple data owner situation, and separate users in the PHR scheme into multiple protection domains, which significantly reduces key management complexity for owners and users. Using multi-authority ABE, a high standard of patient privacy is maintained at the same time. Our framework also allows for dynamic changes to access policies or file attributes, as well as powerful emergency break-glass control and on-demand user/attribute revocation. The security, scalability, and efficiency of the system are demonstrated via comprehensive analytical and experimental results.

Keywords: Blockchain; Cloud Computing; Attribute Based Encryption;

1. Introduction

Cloud-assisted mobile health monitoring, which employs existing mobile communications and cloud computing technologies to provide feedback decision support, has been lauded as a game-changing approach for improving healthcare quality while lowering costs. Unfortunately, it also puts clients' privacy and tracking service providers' intellectual property at risk, potentially deterring widespread adoption of health technology. Furthermore, the outsourcing decryption strategy, and a newly proposed key private proxy re-encryption have been modified to move the technical complexity of the involved parties to the cloud without jeopardizing the privacy of the client or the intellectual property of the service provider. Finally, the feasibility of our proposed design is shown by our protection and performance review. PHRs are a new patient-centric model of health information exchange that is often outsourced and processed by third parties such as cloud providers. Third-party servers and unauthorised parties can have access to personal health information, causing widespread privacy concerns. Encrypting PHRs before outsourcing is a promising way to keep patients' access to their personal health records. However, the most significant roadblocks to achieving fine-grained, cryptographically enforced data access control have remained issues like privacy threats, scalability in key management, versatile access, and efficient user revocation.
1.1 Objective

We use Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR code, resulting in fine-grained and scalable data access control for PHRs. We concentrate on the multiple data owner situation, and split users in the PHR scheme into multiple protection domains, which significantly reduces the key management complexity for owners and users. Using multi-authority ABE, a high level of patient privacy is ensured at the same time. Our system also allows for dynamic changes to access policies or file attributes, as well as powerful Emergency break-glass control and on-demand user/attribute revocation. Our proposed scheme's security, scalability, and efficiency are demonstrated via comprehensive analytical and experimental results.

Streamlined procedures, better administration and monitoring, superior patient treatment, tight cost control, and increased sustainability are all advantages of using a health care system. It is designed and built to provide real imaginative benefits to hospitals and is strong, versatile, and simple to use. It is, moreover, backed by dependable and consistent support.

The database, object-oriented, and networking techniques are used in the ‘Healthcare System' project. As there are many places where we hold records in databases, we use MY SQL software, which is one of the best and most user-friendly software for doing so. The front-end software for this project is JAVA, which is an Object Oriented Programming language that connects to MY SQL.

2. Existing System

Owing to the high cost of building and maintaining specialised data centres, many PHR facilities are outsourced to or run by third-party service providers, such as Microsoft Health Vault. While having universal PHR capabilities is exciting, there are many security and privacy concerns. Its widespread adoption will be limited as a result of this. The main question is whether patients can fully control how their private health information (PHI) is transmitted.

2.1 Disadvantages

Unauthorized parties and third-party servers can have access to personal health information, raising widespread privacy concerns. An employee of the Department of Veterans Affairs, for example, stole a database containing 26.5 million military veterans' sensitive PHI, including their social security numbers and medical conditions, and took the data home without their permission. They frequently assume that the system can only use one Trusted Authority (TA). This not only results in a load bottleneck, but it also raises the issue of key escrow, as the TA has access to all encrypted data, making the inevitable disclosure of personal information a possibility.

3. Proposed System

Encrypting PHRs before outsourcing is a promising approach to maintain patients' access to their own PHRs. We propose a new patient-centric architecture and a collection of data access control protocols in this paper for PHRs stored on semi-trusted servers. To secure each patient's PHR file, we use attribute based encryption (ABE) techniques. Achieve fine-grained and scalable data access control for PHRs.

3.1 Block Chain

A blockchain is a decentralised, distributed public ledger that serves as a shared, coordinated database for cryptocurrency transactions. Although blockchains are basically shared databases, the data does not have a single owner. Users determine the data is added to the blockchain by cooperation, thus ensuring that identical copies of the data are obtained and automatically modified. In any environment, e-hospital produces a large amount of complex and rich data, ranging from sensitive patient-identifiable information to operational analytics. Because of the broad distribution and appropriate actions involved in sharing these Vote-related data, they continue to be vulnerable to data breaches. To address this problem,
blockchain technologies have been proposed. Verified users gain access to blockchain systems after being given permission. This gives them the freedom to exchange relevant data with other confirmed users, ensuring accountability, scalability, and performance. Although this innovation has shown promise in a variety of fields, there are a range of hurdles to tackle before it can be successfully applied in an E-hospital. Since vote-related data is plentiful and comes from a variety of sources, data aggregation and linking has the ability to yield useful population-level insight. The need for methods to safeguard access control to confidential patient data is a key concern with the increased convergence of Vote data sources. Furthermore, as the amount of Vote- and lifestyle-related data increases as a result of, for example, mobile apps and wearable devices, blockchain technology can be used by patients, providers, and researchers to allow novel consent and access mechanisms. Blockchains can be used to monitor access to confidential data since they use cryptographic methods to authenticate and validate users.

3.2 Advantages

The organization's work was well-organized and well-planned. The data had been properly preserved in data stores, which assist in both retrieval and storage of information.

- Accuracy: The proposed method has a higher degree of accuracy. All operations would be conducted correctly, and any information obtained from the centre would be reliable.
- Reliability: Due to Attribute Encryption, the proposed system has a high degree of reliability. The improved device reliability can be due to the fact that data is now properly stored.
- No Redundancy: Under the proposed framework, every attempt must be made to ensure that no information is duplicated anywhere, whether in storage or elsewhere. This will ensure effective storage space usage and data continuity.
- Immediate retrieval of information: The proposed system's main purpose is to allow for fast and efficient retrieval of data. Any type of information may be accessed at any time by the user.
- Immediate information storage: - In a manual system, it can be difficult to store a large volume of data.
- Easy to Use: - The system should be simple to use and built in such a way that it can be developed in a short amount of time while remaining within the user's budget.

4. Module description

4.1 Patient Registration

The patient is the focus of our proposed system most important entity. The patient's main responsibilities are as follows: A new patient would need to fill out paperwork submit a request for authentication from a trusted authority in order a obtain an variety of identification (ID), after which He or she may be in a position to do so. access the services provided by the framework Produces and saves the patient's medical file (PHR) to the cloud server. By defining a access policy that can be used (attribute-based) to encrypt prior to distribution of data.

4.2 Interaction with Providers of healthcare

Individuals who support others organised services in health care to all members of a community are known as healthcare providers. Health practitioners and specialists, physicians, nurses, pharmacists, surgeons, medical technicians, laboratory workers, and other employees could be among the healthcare providers. For specific purposes, each of these individuals needs access to a portion of the patient records. The following are the responsibilities of every healthcare provider: To gain access to specific parts of the patient's record, Obtain an identification number (ID) from a reliable source. Make a submit a submission for the secret key along with the parameters.
4.3 Key Generation

The following functions are performed by a trustworthy authority (TU), such as the Ministry of Health or some other government department: Ensure that all users who are involved with the system are authenticated. Create key elements for healthcare providers and patients make public the cryptographic processes parameters require.

4.4 Cloud Based HER

The proposed framework's backbone is an Cloud-based EHR for e-government. E-government is a form of electronic government. programme (Yesser) in Saudi Arabia has been established, and government cloud computing is one of the company's programmes and goods. The following the cloud services are included in the proposed cloud-based e-government EHR: The first service has two main components: a computing tools and a data repository The very first is service is in charge of storing encrypted electronic health records that can only be accessed by authenticated healthcare professionals that have been given access based on their qualifications. The second service is in charge of creating access policies, effectively handling keys, and other programming tasks. As a third provider, the web-based platform is hosted. The web-based platform that is being built should be a protected online environment website that stockholders can access from anywhere, at any time, using an Internet connection, and on any device.

4.5 Distribution of Information

The central authority that can be trusted cannot due to the need to encrypt the EHR separately for each consumer to the size of the database and the fact that it contains several users with different access privileges. Encrypting the EHR once and then disseminating the encryption is more effective. to a large number of attribute authorities (AAs) based on their functions.

5. Algorithm

5.1 Algorithm Steps:

- [1] Organizing (K). A protection parameter, K, is fed into the device set-up process It creates a public key (PK) as well as a master key (MK).
- [2] Create Attribute Authority is a command that allows you to create an attribute with a specific authority (PK, AA). With the AA request as input, this algorithm is run by the GA (central authority). It generates a functional identifier for the AA, Aid, as well as a collection of attributes, Sid, and a hidden authority key, SKAid, for the AA. The Ministry of Health classifies AAs based on their functions, then assigns attributes to users of those functions.
- [3] Attribute Key Generator is a class that generates keys for attributes (PK, SKAid, Sid). The Help domain authority is in charge of executing this algorithm. It accepts the PK and the domain authority's hidden key, SK Aid, as well as a set of attributes, Sid, as inputs. It returns the user SKUj's attribute hidden keys.
- [4] Encrypt your data (PK, M, P, PKU). The PK, a message (M), and an access policy are all inputs to the encrypt algorithm (P).
- [5] Decrypt (PK, CT, P, SKUj, SKA). The decrypt algorithm takes the PK, which is a ciphertext code, as input. takes the PK, which is a ciphertext code, as input. CT, the same control P used in encryption, SKUj, the hidden user key, and SKA, a list of secret attribute keys. If the attributes are adequate to satisfy the P, the CT message will be decrypted; otherwise, the output will be null.

Due to the complexity of the EHR database and the fact that it includes many users with differing access rights, it is not feasible. The trusted central authority cannot encrypt the EHR separately for each user due to the size of the database and the fact that it includes many users with different access privileges. [6-12] Since the EHR database is very broad and includes many users with different access rights, it is not appropriate The EHR must be encrypted separately for each user by a trusted central
authority. It's more productive to encrypt the EHR once and then disperse the encryption through a variety of attribute authorities (AAs) based on their roles.

6. Result

Proposed result shows that patient data can be transferred to concern person in secured way

![Figure 1. Data Processing](image1)

Details of patient along with doctor details shown in Figure 1.

![Figure 2. Patient Records](image2)

Only allowed doctors only can access concern patient data shown in Figure 2.

![Figure 3. Patient Data](image3)

It includes a user's biographical details shown in Figure 3.
We can see the verified user information as well as others shown in Figure 4.

7. Conclusion

By enforcing access control policies using hierarchical multi-authority CP-ABE, we propose a robust cloud-based EHR architecture that ensures the security and privacy of medical data stored in the cloud. The proposed framework allows for comprehensive electronic health record (EHR) integration, interoperability, and sharing among healthcare providers, patients, and practitioners. The system's attribute domain authority is in control of a separate attribute domain and is self-contained. In addition, there is no computational overhead for the government authority, and multifactor applicant authentication has been developed and checked.

References:

[1] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, Internet of Things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015

[2] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, Deep learning for IoT big data and streaming analytics: A survey, IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.

[3] J. Men, G. Xu, Z. Han, Z. Sun, X. Zhou, W. Lian, and X. Cheng, Finding sands in the eyes: Vulnerabilities discovery in IoT with EUFuzzer on human machine interface, IEEE Access, vol. 7, pp. 103751–103759, 2019.

[4] A. Moraru, M. Pesko, M. Porcius, C. Fortuna, and D. Mladenic, Using machine learning on sensor data, J. Comput. Inf. Technol., vol. 18, no. 4, pp. 341–347, 2010.

[5] E. Borgia, The Internet of Things vision: Key features, applications and open issues, Comput. Commun., vol. 54, pp. 1–31, Dec. 2014.

[6] Masrom, Maslin, and Ailar Rahimli. A Review of Cloud Computing Technology Solution for Healthcare System. Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.

[7] S. D., & H. A. (2019). AODV Route Discovery and Route Maintenance in MANETs. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). doi:10.1109/icaccs.2019.8728456

[8] H. Anandakumar and K. Umamaheswari, An Efficient Optimized Handover in Cognitive Radio Networks using Cooperative Spectrum Sensing, Intelligent Automation & Soft Computing, pp. 1–8, Sep. 2017. doi:10.1080/10798587.2017.1364931
[9] N. Jouppi, C. Young, N. Patil, and D. Patterson. Motivation for and evaluation of the first tensor processing unit. IEEE Micro, 38(3):10–19, May 2018.

[10] Álvaro López García, Enol Fernández-del Castillo, Pablo Orviz Fernández, Isabel Campos Plasencia, and Jesús Marco de Lucas. Resource provisioning in Science Clouds: Requirements and challenges. Software: Practice and Experience, 48(3):486–498, 2018.

[11] Enol Fernández-del Castillo, Diego Scardaci, and Álvaro López García. The EGI Federated Cloud e-Infrastructure. Procedia Computer Science, 68:196–205, 2015.

[12] Miguel Caballer, Sahdev Zala, Álvaro López García, Germán Moltó, Pablo Orviz Fernández, and Mathieu Velten. Orchestrating Complex Application Architectures in Heterogeneous Clouds. Journal of Grid Computing, 16(1):3–18, mar 2018.