International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Survey of Traditional and Blockchain-based EHR system

Miss Falguni Pawar[1], Prof. Viresh Vanarote[2]

[1]T.E Computer Engineering, RMD School of Engineering, Warje, Pune-58, Maharashtra, India
[2]Asst. Prof. of Computer Engineering, RMD School of Engineering, Warje, Pune-58, Maharashtra, India

---

Abstract - *The gradual transformation of healthcare systems from paper-based records to electronic records has its own advantages like easy access to medical data, able to maintain effective clinical workflows, reduced medical costs, lowers medical errors, easy exchange of data between various stakeholders, but this transition also came with some unique challenges with respect to privacy, confidentiality, and security of medical information of the patients. These electronic health records of the patient are comprised of a wide variety of data, such as medical histories, demographics, medication, immunization status, laboratory test reports, and other sensitive patient information. The existing cryptographic and non-cryptographic approaches were used to address these challenges to some extent but not completely solve the problems. This paper discusses an overview of e-Health System, cryptographic and non-cryptographic approaches, their drawbacks, and a new electronic health record system using Blockchain technology which makes it difficult for the hackers to change, hack or cheat the system.*

Keywords: e-Health, Electronic Health Record(EHR), Cryptography, Cloud Computing, Encryption and Decryption

Motivation: The existing privacy-preserving mechanisms are not enough powerful to ensure foolproof security in the e-health cloud. Contrary to most beliefs, the main risk faced by health records hosted in cloud servers is internal attacks from people who have authorized credentials to access data within organizations, where database administrators or key managers are attackers, which is significantly worse than the external attacks. This paper aims to provide a proper understanding of concepts of privacy-preserving mechanisms and also reviews some of its drawbacks in e-healthcare environments that make electronic health records vulnerable to threats in the cloud arena. E-health data contains various sensitive and confidential information ranging from patient data to financial information including social security number, credit card details, whose leakage not only throws open sensitive patients' information and cause financial losses but also breaks the most fundamental right of a citizen in any country i.e. right to privacy. Even though we have made access to EHR easier for patients and healthcare professionals there are some issues like Data encryption, secure storage, authentication, access control, key management, efficient user revocation, etc. which are yet to be addressed and resolved.

1. Introduction

The digital technology of the 21st century has changed the complete picture of the healthcare system across the world. Transitioning to an e-health solution provides high efficiency and flexibility to healthcare services by providing a platform that allows the easy share of healthcare data among different stakeholders, convenient storage of medical information. Cloud computing allows the creation, storage, and retrieval of healthcare information by all healthcare providers, doctors, and patients. Third-party cloud services provide immense benefits in terms of cost-effective storage, access, processing, and updating of information but these huge databases are operated as a single ecosystem that can be accessed by different users from multiple locations, it is susceptible to intrusion and thus posing a threat to patient's data in the cloud. Therefore, having medical data on the third-party servers naturally increase these vulnerabilities.

Healthcare cyber threats is a major concern for two main reasons:

- In addition to the medical information of the patient it also has valuable financial data.
- Since there are very few people who do not see healthcare providers, nearly everyone's personal information is available in some form which makes it more vulnerable to identity theft.

After reviewing the numerous research paper about the privacy-preserving mechanism of e-health solutions we have identified the following tasks

1. Overview of the e-health system in the cloud
2. Cryptographic and Non-cryptographic approaches to protect e-health data and their drawbacks
3. Overview of blockchain technology
4. Patient-Centric EHR system using blockchain technology

2. Literature Survey

[1] A systematic and complete review of security and privacy-preserving challenges in e-health solutions indicates various privacy-preserving approaches to ensure the privacy and security of electronic health records (EHRs) in the cloud. **[2]** In this paper, Authors have investigated privacy in eHealth as a communication problem, since future eHealth

systems will be highly distributed and require interoperability of many sub-systems. In addition, they have also research privacy needs for others than patients.
[3] Cloud computing is a recent and fast-growing area of development in healthcare. Thus, the objective of this scoping review was to identify the current state and hot topics in cloud computing in healthcare **[4]** This survey aims to encompass the state-of-the-art privacy-preserving approaches (cryptographic and noncryptographic approaches) employed in the e-Health clouds. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted. **[5]** Authors show how new primitives in attribute-based cryptography can be used to build a secure and privacy-preserving EHR system that enables patients to share their data among stakeholders in a flexible, dynamic, and scalable manner.
[6] This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data to access control to untrusted cloud servers without disclosing the underlying data contents. **[7]** This article explains why RBAC is receiving renewed attention as a method of security administration and review, describes a framework of four reference models developed to better understand RBAC **[8]** The paper describes the ABAC model in terms of its authorization architecture and policy formulation and makes a detailed comparison between ABAC and traditional role-based models, which clearly show the advantages of ABAC.
[9] This paper describes seven different access control mechanisms used in cloud computing platforms for different purposes. **[10]** The researchers utilized the Texas State University Library to gain access to three online databases: PubMed (MEDLINE), CINAHL, and ProQuest Nursing and Allied Health Source. These sources were used to conduct searches on literature concerning the security of electronic health records containing several inclusion and exclusion criteria. Researchers collected and analyzed 25 journals and reviews discussing the security of electronic health records, 20 of which mentioned specific security methods and techniques.

3. Overview of traditional e-health system in the cloud

Before we move on explaining e-Health system lets understand some cloud computing characteristics:

On-demand self-service: All the resources stored in the Cloud can be provisioned without human interaction from the service provider. In other words, a Health Insurance company can provide additional computing resources as needed without going through the cloud service provider.

Broad Network Access: All the resources in the Cloud are available over the network and can be accessed by diverse customer platforms from anywhere in the world. For e.g, any patient's medical record can be accessed or shared to the Insurer or doctor easily when required.

Multi-tenancy: Cloud computing resources are designed to support a multi-tenant model. Multi-tenancy in the cloud is nothing but allowing multiple customers to share the servers or the same physical infrastructure while maintaining privacy and security over their information. It's similar to people living in an apartment building, sharing the same building resources but they still have their own apartments and privacy within that building.

Elasticity and scalability: The cloud is flexible and configurable. Clients feel that resources are unlimited. Cloud resources can be rapidly adjusted to accommodate specific demands for business. It offers the flexibility to scale up or down depending on your specific business needs.

Measured service: Cloud Service Provider uses different metrics for usage but the detailed report will be generated for every customer.

An overview of e-health architecture is depicted in Fig 1.

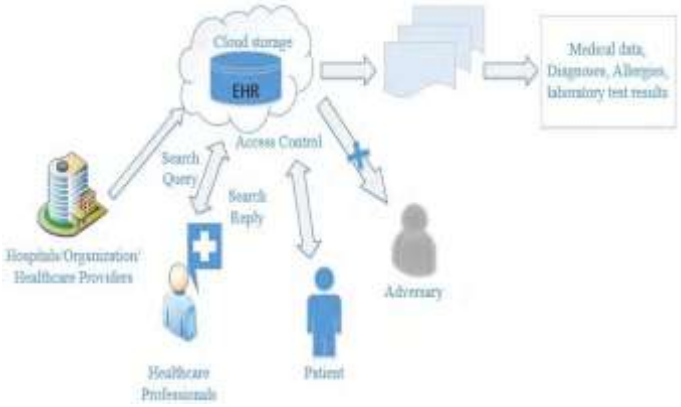

Fig 1. Architecture of electronic health data in cloud.

EHR or EMR in the cloud involves all the health data information including demographics, medical histories, medications, laboratory reports, radiology images, billing information, and any additional sensitive patient information. The cloud offers great service to both healthcare providers and patients alike in terms of cost-effective storage, processing, and updating of information with enhanced efficiency and quality. Since all this data is stored in multiple servers, it can be easily accessible by users from various locations on demand, however, they equally expose patient privacy, via improper authorization and misuse of EHR data. Therefore security and privacy are considered to be critical requirements when sharing or accessing patient data between several stakeholders (Doctors, Insurance companies, Labs, etc).

4. e-Health Security Issue

The use of the cloud computing paradigm in healthcare facilitates the sharing and integration of medical records. However, the cloud computing paradigm offers several benefits; it also poses privacy and security threats to health data. Below are some of the major security issues of the traditional EHR system in the cloud.

Confidentiality: Confidentiality is the act of ensuring that patient's health data are kept completely undisclosed to unauthorized entities. Due to the increased number of parties, devices, stakeholders, and applications involved, there is an increase in data compromise threats.

Integrity: Integrity ensures the health data captured by a system or provided to any authorized entity are accurate and consistent with the intended information and have not been altered in any way while transferring data. There is a lack of assurance of reliability from the cloud service provider

Availability: For any healthcare cloud system to serve its purpose, the information must be available all the time on demand. The availability of medical data in critical situations even when there is a security breach is important. High-availability systems should prevent service disruptions due to power outages, hardware failures, system upgrades, and denial-of-service attacks. Medical data might not be available on time because of a lack of geo replications of the databases.

Ownership of data: In general, the owner is defined as the creator of the information. Patients can allow or deny the sharing of their information with other stakeholders. To implement patient data sharing in a healthcare system, the patient may grant rights to users based on a role or attributes held by the respective user to share specific healthcare data with that user.

Authenticity: Authenticity ensures that the entity requesting access is authentic. The Cloud provider job is to ensure that only the authorized and authentic authority should have access to sensitive health data.

5. Overview of Blockchain Technology

Blockchain is a system of recording information in a way that makes it difficult or impossible to alter, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains several transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash. This means if one blocks in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to alter the information in the block, they would have to change every block in the chain, across all of the distributed versions of the chain.

Specifically, Blockchain has three parts:

1. Hash of the Block: A hash is a string of numbers and letters, produced by hash functions. A hash function is a mathematical function that takes a variable number of characters and converts it into a string with a fixed number of characters. Even a small change in a string creates a completely new hash. In other words, once a block is created its hash will be calculated, and changing something inside the block will cause the hash to change. Hash will be very useful in detecting any changes done by hackers.
2. Hash of the previous block: It's the calculated hash of the previous block. All blocks are connected using the hash of the previous block. This effectively creates a chain of blocks which makes it more secure
3. Data in the Block: The data stored in the Block depends on the type of blockchain. E.g. In our case, the data will be lab results of the patient, claim forms, doctors' prescription, etc. with the timestamps and other details.

How Blockchain Works?

Four things must happen for a block to be added to the blockchain

1. A transaction must occur. E.g. In our case releasing the Lab reports of the patient by lab assistant will be considered as a transaction. A block can group potentially thousands of transactions.
2. That transaction must be verified. There is someone in charge of vetting new data entries. In the blockchain, every transaction will be verified by the network of computers. When reports of the patient are out, that network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the patient, including the transaction's time, and participants.
3. That transaction must be stored in a block. After your transaction has been verified as accurate, it is ready to be added in the block. All the details about the transaction are all stored in a block.
4. That block must be given a hash. Once all of a block's transactions have been verified, the hash will be calculated for that block, also block is given the hash of the previous block.

6. EHR system using blockchain technology

In the previous section, we have explained all the fundamentals of blockchain technology, Now let's see how that is used in the EHR system.
Fig 2 shows the novel architecture of the blockchain-based EHR system introduced in 2019 by researchers of RMIT University, Australia. Four main components of this architecture are explained below:

User Application: It allows users to build an initial transaction with some system-generated data (timestamp). Users can be doctors, lab assistants, insurers, etc. Different User Interface is given to different users.

Blockchain Handshaker: It is the heart of the whole architecture which is connected to User application, Public Blockchain Network, and Cloud Databases. It is responsible for generating blockchain transactions, validating the transaction, sending that validated transaction to the cloud.

Public Blockchain Network: The public blockchain network comprises blockchain nodes, distributed ledger, and smart contracts. Blockchain nodes receive transactions and validate based on smart contracts. If a transaction is found as valid, data are converted to blocks and added in the distributed ledger.

Cloud: It is used for hosting the EHR management system and storing health records. EHR management system is responsible for storing validated transaction data in the cloud.

Fig 2. Blockchain based EHR architecture.

Working: User application sends an initial transaction that contains patient health data inserted by a user (doctors, lab assistants, insurers, etc.). Then Initial Transaction is sent to Blockchain Handshaker (BH) for communicating with the public blockchain network. BH generates a blockchain transaction. Another component of BH, transaction validator (TV), sends Blockchain Transaction to a public blockchain network for validation. Further, the public blockchain network validates transactions using smart contracts and mines to add transaction data into the blockchain. The public blockchain network sends a validation acknowledgment to BH at the end of validation. BH sends the validated transaction to the cloud for further processing. Finally, the cloud stores data in the cloud database at the end of processing.

If Public Blockchain Network ensures which transaction is faulty. So even if a hacker tries to alter the information it will be instantly tracked.

7. Conclusion

Security is one of the main problems that hinder the fast adoption of cloud computing technology in the healthcare industry. Patient's data in the traditional EHR system is more vulnerable even when using complex data encryption techniques. In this paper, we have discussed the overview of the traditional EHR system, the security issues of that system, and finally explained the tamper-proof Blockchain-based EHR system. Future work can be using artificial intelligence to generate dynamic smart-contracts using the handshaker to address cross-domain diversities.

8. References

[1] Chenthara, Shekha & Ahmed, Khandakar & Wang, Hua & Whittaker, Frank. (2019). Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2919982.

[2] N. Dong, H. Jonker, and J. Pang, ‘‘Challenges in e-health: From enabling to enforcing privacy,’’ in *Proc. Int. Symp. Found. Health Inform. Eng. Syst.* Berlin, Germany: Springer, 2011, pp. 195–206.

[3] L. Griebel, H.-U. Prokosch, and F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, ‘‘A scoping review of cloud computing in healthcare,’’ *BMC Med. Inform. Decis. Making*, vol. 15, no. 1, p. 17, Mar. 2015.

[4] A. Abbas and S. U. Khan, ‘‘A review on the state-of-the-art privacy-preserving approaches in the e-health clouds,’’ *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1431–1441, Apr. 2014. [Online].

[5] S. Narayan, M. Gagné, and R. Safavi-Naini, ‘‘Privacy-preserving EHR system using attribute-based infrastructure,’’ in *Proc. ACM Workshop Cloud Comput. Secure Workshop*, Oct. 2010, pp. 47–52.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[7] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, ‘‘Role-based access control models,’’ *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[8] E. Yuan and J. Tong, ''Attributed based access control (ABAC) for Web services,'' in *Proc. IEEE Int. Conf. Web Services*, Jul. 2005, p. 569.

[9] R. Charanya and M. Aramudhan, ''Survey on access control issues in cloud computing,'' in *Proc. Int. Conf. Emerg. Trends Eng., Technol. Sci. (ICETETS)*, pp. 1–4, Feb. 2016.

[10] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, ''Security techniques for the electronic health records,'' *J. Med. Syst.*, vol. 41, no. 8, p. 127, Aug. 2017.

[11] Rahman, Mohammad & Khalil, Ibrahim & Chamikara, M.A.P. & Bouras, Abdelaziz & Yi, Xun. (2019). A Novel Architecture for Tamper Proof Electronic Health Record Management System using Blockchain Wrapper. 97-105. 10.1145/3327960.3332392.