e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

SECURITY AND PRIVACY OF ELECTRONIC HEALTH RECORDS SHARING USING HYPERLEDGER FABRIC

Vishnuvardhan Komuravelly*1, M. Ramchander*2

*1Student MCA IV Sem, Department of MCA, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.

*2Assistant Professor, Department of MCA, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.

DOI : https://www.doi.org/10.56726/IRJMETS29499

ABSTRACT

Electronic medical records and patient data sharing are critical and considered as core issues in health care. How to store patient's information securely, how to access the information and how to ensure the privacy of patients when sharing medical data among several health service providers or agents are critical considerations. To handle those crucial considerations, a blockchain-based technology called Hyperledger Fabric will be useful. Hyperledger Fabric is a permissioned blockchain technology that provides a way to secure the interactions among a group of identified participants. In this paper, we will show how the implementation of Hyperledger Fabric to store, manage and maintain electronic medical records can ensure the security and the privacy of patient data.

I. INTRODUCTION

An electronic health record (EHR) is a digital record containing different details regarding a patient's medical history, physical examinations, treatment, etc. Electronic health records (EHRs) provide opportunities to enhance patient care, embed performance measures in clinical practice, and facilitate clinical research to improve the identification and recruitment of eligible patients and healthcare providers in clinical research. Many healthcare providers provide patients with the ability to use online portals to access their EHR for checking their information and to communicate with physicians. Additionally, physicians and healthcare providers are implementing EHRs to increase access to health care, to improve the quality of care and to decrease costs. EHRs facilitate the sharing of patient information among different healthcare agents and can increase efficiency in the delivery of health care. Patients typically have data stored in a variety of locations where they receive care. Over a lifetime, much data accumulates at a variety of different healthcare providers. EHRs give those health providers the ability to coordinate health care among them and to have access to the most recent data. Moreover, EHRs can reduce costly redundant tests that are ordered because one provider does not have access to the clinical information stored at another provider's location. In addition, accumulated data are extremely valuable to health researchers, medical institutions and local health authorities since these data could be used to keep track of disease progress, improve patients care quality and monitor public health. Despite the benefits that EHRs provide, some issues need to be considered when implementing EHRs. Most of these issues are concentrated on two factors: privacy and security. Data sharing among EHRs systems has raised some security concerns because healthcare data is potentially accessible by a variety of users, which could lead to exposure of privacy. Once such data are available electronically, it opens the door for hackers and other malicious attackers to access the records. Controlling access to health data in EHRs is a considerable aspect for protecting data confidentiality but it is not sufficient. Additional security steps are essential to secure patient's information.

SCOPE

To overcome the issues of privacy and security associated with implementing EHRs, we may adopt a technology that can address those issues and allow patients to control their own data. Hyperledger Fabric is a permissioned blockchain-based technology that can be used for this purpose. It allows all participant nodes to share information securely without the need to trust someone to control all transactions on the network. Every transaction is recorded cryptographically after other participants validate it. The recorded transactions cannot

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

be deleted, altered or tampered with. Hyperledger Fabric features will be suitable to construct an integrated health records management platform with high level of privacy and confidentiality.

PURPOSE OF PROJECT

Once such data are available electronically, it opens the door for hackers and other malicious attackers to access the records. Controlling access to health data in EHRs is a considerable aspect for protecting data confidentiality but it is not sufficient. Additional security steps are essential to secure patient's information. Patients have the right to have their medical information stored securely and cannot be accessed by those who do not have the authority. Also, patient's medical information must be stored in a manner that prevents tampering and alteration. Sharing patient's data among different parties, such as hospitals, insurance companies and government agencies, adds another dimension to ensuring privacy of patients. Patients are usually very cautious about sharing their personal information and even more when it concerns their personal health information. Most EHRs do not grant patients the ability to authorize and revoke access to their information.

II. PROJECT ARCHITECTURE

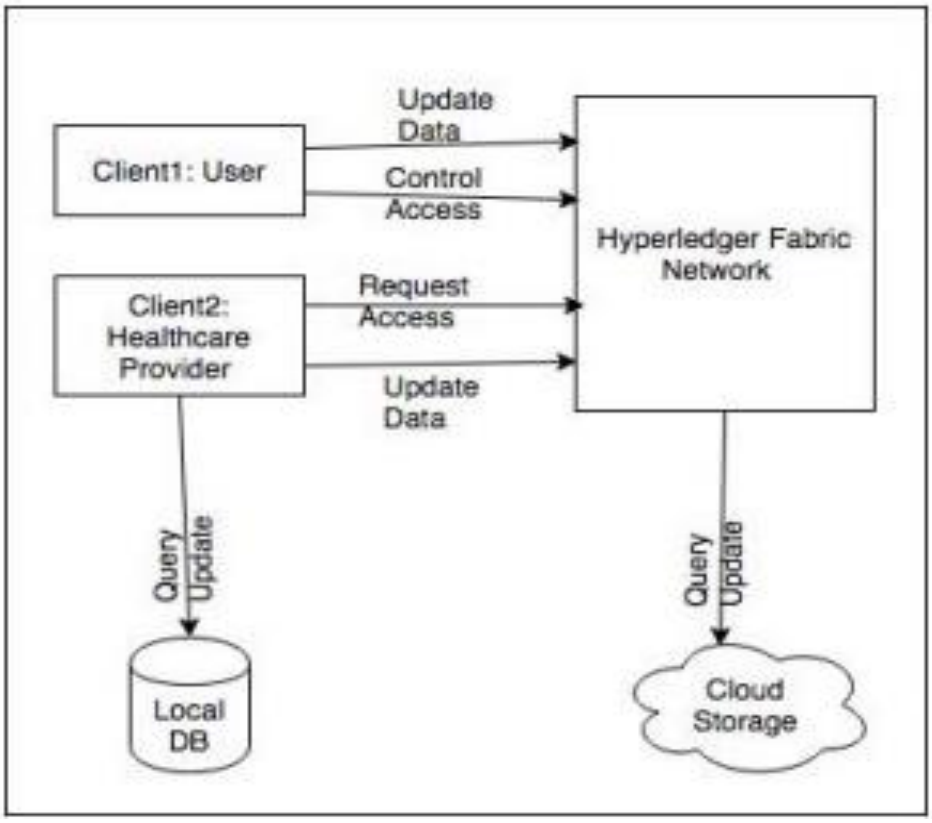

Figure 1: Project Architecture

Blockchain is a peer-to-peer distributed ledger technology that was initially used in the financial industry. The blockchain paradigm can be extended to provide a generalized framework for implementing decentralized computing resources. It is comprised of a continuously growing list of records called blocks that contain transactions. The structure of a blockchain consists of a sequence of blocks in which each one contains the cryptographic hash of the previous block in the chain. A consensus-based mechanism is used to prevent the whole chain from being modified or altered and to decide which block is to be appended to the ledger. The distributed ledger is not controlled by anyone and all the participants on the network can view it. Prior to adding a transaction to the ledger, the transaction must be encrypted and verified by other nodes on the network using consensus protocols. Once a transaction is validated by the majority of nodes, it is added to the ledger and shared by all participants. The added transaction cannot be deleted or changed. Thus, transactions in the ledger are trustable, auditable and immutable. Blockchains are either permission-less or permissioned. In permission-less blockchain, all nodes are required to execute a significant amount of computational work called

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

Proof-of-Work (PoW) to determine whether a new block is valid to be added to the chain. In contrast, all the nodes in permissioned blockchain are required to be identified and be known to all other participants. The consensus protocol in permissioned blockchain may involve PoW or other algorithms such as Byzantine Fault tolerant (BFT). All blockchain systems, permissioned or permission-less, follow the order-execute architecture in which the blockchain network orders transactions first using a consensus protocol and then executes them sequentially in the same order on all nodes. Existing permissioned blockchains typically use BFT consensus or other protocols for atomic broadcast and follow the same order-execute approach. Blockchains support what is called Smart Contract. It is similar to a contract in the real world, but it is a digital contract represented by a program code that resides inside a blockchain. It stores protocols for defining the terms of an agreement and automatically verifies and executes processes that are based on those protocols. This mechanism removes reliance on a third party, so all participants on the network can make agreements and transact directly.

III. MODULES USED

3.2.1 Tensorflow

TensorFlow is a free and open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google.

TensorFlow was developed by the Google Brain team for internal Google use. It was released under the Apache 2.0 open-source license on November 9, 2015.

3.2.2 NumPy

Numpy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

It is the fundamental package for scientific computing with Python. It contains various features including these important ones:

- A powerful N-dimensional array object
- Sophisticated (broadcasting) functions
- Tools for integrating C/C++ and Fortran code
- Useful linear algebra, Fourier transform, and random number capabilities

Besides its obvious scientific uses, Numpy can also be used as an efficient multi-dimensional container of generic data. Arbitrary data-types can be defined using Numpy which allows Numpy to seamlessly and speedily integrate with a wide variety of databases.

3.2.3 Pandas

Pandas is an open-source Python Library providing high-performance data manipulation and analysis tool using its powerful data structures. Python was majorly used for data munging and preparation. It had very little contribution towards data analysis. Pandas solved this problem. Using Pandas, we can accomplish five typical steps in the processing and analysis of data, regardless of the origin of data load, prepare, manipulate, model, and analyze. Python with Pandas is used in a wide range of fields including academic and commercial domains including finance, economics, Statistics, analytics, etc.

3.2.4 Matplotlib

Matplotlib is a Python 2D plotting library which produces publication quality figures in a variety of hardcopy formats and interactive environments across platforms. Matplotlib can be used in Python scripts, the Python and IPython shells, the Jupyter Notebook, web application servers, and four graphical user interface toolkits. Matplotlib tries to make easy things easy and hard things possible. You can generate plots, histograms, power spectra, bar charts, error charts, scatter plots, etc., with just a few lines of code. For examples, see the sample plots and thumbnail gallery.

For simple plotting the pyplot module provides a MATLAB-like interface, particularly when combined with IPython. For the power user, you have full control of line styles, font properties, axes properties, etc, via an object oriented interface or via a set of functions familiar to MATLAB users.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

3.2.5 Scikit – learn

Scikit-learn provides a range of supervised and unsupervised learning algorithms via a consistent interface in Python. It is licensed under a permissive simplified BSD license and is distributed under many Linux distributions, encouraging academic and commercial use Python.

IV. CONCLUSION

EHRs play a significant role in improving patient's care and enhancing the delivery of health care services. However, in spite of the anticipated benefits of this technology, there is widespread concern that patient's privacy and the security of the medical data will be compromised. These issues may impede widespread use of EHRs. In this paper, we introduced a blockchain-based platform, called Hyperledger Fabric, which can be adopted to overcome those issues by preserving privacy and providing stronger security. Building EHRs based on Hyperledger Fabric will ensure that patients have full access control to their records, patient's data are stored securely and only verified participants can interact with patient's sensitive data. Implementing Hyperledger Fabric features on EHRs helps ensuring health information sharing among all parties on the network securely without concerns about exposing patient's privacy and confidentiality.

V. REFERENCES

[1] M. R. Cowie et al., "Electronic health records to facilitate clinical research," Clinical Research in Cardiology, vol. 106, no. 1. pp. 1–9, 2017.

[2] N. Menachemi and T. Collum, "Benefits and drawbacks of electronic health record systems," Risk Manag. Healthc. Policy, vol. 4, pp. 47– 55, 2011.

[3] F. Rezaeibagha and M. Yi, "Distributed clinical data sharing via dynamic access-control policy transformation," Int. J. Med. Inform., vol. 89, pp. 25–31, 2016.

[4] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in International Conference of the IEEE Engineering in Medicine and Biology Society, 2006, pp. 5453–5458.

[5] F. Ozair, N. Jamshed, A. Sharma, and P. Aggarwal, "Ethical issues in electronic health records: A general overview," Perspect. Clin. Res., vol. 6, no. 2, p. 73, 2015.

[6] "Hyperledger Fabric," 2018. [Online]. Available: https://www.hyperledger.org/projects/fabric. [Accessed: 21-Apr2018].

[7] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," 2017.

[8] G. Wood, "Ethereum: a Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014. [Online]. Available: https://gavwood.com/paper.pdf. [Accessed: 18-Apr-2018].

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," J. Gen. Philos. Sci., vol. 39, no. 1, pp. 53–67, 2008. [10] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," 2018.

[10] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform," in Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, 2018, no. Section 4, pp. 51–58.

[11] "Hyperledger Fabric CA," 2017. [Online]. Available: https://hyperledger-fabric-ca.readthedocs.io/en/latest/.[Accessed: 05- May-2018].

[12] https://www.anaconda.com/download/

[13] https://www.python.org/downloads/release/python-360/