IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

SNNO: 2347-3657
Volume 9,Issue3 Aug ,2021

Security and Privacy of Electronic Health Records Sharing Using Hyper ledger Fabric

Mrs. Gangula Pavani, Mrs. Mukka Shirisha, Mrs. Rayees Fathima

Abstract—

Electronic clinical data and affected person facts sharing are essential and taken into consideration as center troubles in fitness care. How to save affected person's statistics securely, the way to get admission to the statistics and the way to make sure the privateers of sufferers when sharing clinical facts amongst numerous fitness carrier vendors or dealers are essential considerations. To cope with the ones crucial considerations, a block chain-primarily based totally generation called Hyper ledger Fabric could be useful. Hyper ledger Fabric is a permission block chain generation that offers a manner to steady the interactions amongst a set of identified participants. In this paper, we are able to display how the implementation of Hyper ledger Fabric to save, control and keep digital clinical data can make sure the security and the privateers of affected person facts.

I. INTRODUCTION

A digital fitness record (EHR) is a virtual record containing exclusive info concerning an affected person's medical history, bodily examinations, treatment, etc. Electronic fitness records (EHRs) offer possibilities to enhance affected person care, embed overall performance measures in scientific practice, and facilitate scientific studies to enhance the identity and recruitment of eligible sufferers and healthcare companies in scientific studies [1]. Many healthcare companies offer sufferers with the cap potential to apply online portals to get right of entry to their EHR for checking their information and to talk with physicians. Additionally, physicians and healthcare companies are enforcing EHRs to growth get right of entry to to fitness care, to enhance the first-rate of care and to lower costs. EHRs facilitate the sharing of affected person data amongst distinct healthcare sellers and might boom performance in the transport of fitness care. Patients generally have
Records saved in a number of places in which they acquire care. Over a lifetime, tons records accumulate at a number of distinct healthcare vendors. EHRs supply the ones fitness vendors the cap potential to coordinate fitness care amongst them and to have get admission to the maximum current records. Moreover, EHRs can reduce steeply-priced redundant exams which are ordered due to the fact one provider does now no longer have get admission to the medical data saved at every other provider's location[2].

In addition, accrued statistics are extraordinarily precious to fitness researchers, medical establishments and nearby fitness government considering the fact that those statistics could be used to preserve tune of disorder progress, enhance patients care first-rate and screen public fitness. Despite the advantages that EHRs provide, a few troubles need to be taken into consideration while imposing EHRs.

1,2,3 Assistant Professor
1,2,3 Department of CSE
1,2,3 Global Institute of Engineering and Technology Moinabad, Ranga Reddy District, Telangana State.

Most of those troubles are targeting factors: privateers and safety. Data sharing amongst EHRs structures has raised a few safety issues due to the fact healthcare statistics is doubtlessly on hand by a number of users that can cause publicity of privateers [3]. Once such statistics are to be had electronically, it opens the door for hackers and different malicious attackers to get admission to the records [4]. Controlling get admission to fitness statistics in EHRs is a massive thing for shielding statistics confidentiality however it isn't sufficient. Additional safety steps are critical to steady patient's information [5]. Patients have the proper to have their clinical facts saved securely and cannot be accessed with the aid of using people who do now no longer have the authority. Also, patient's clinical facts must be saved in a way that forestalls tampering and alteration. Sharing patient's statistics amongst extraordinary parties, such as hospitals, coverage organizations and authority's agencies, provides some other size to making sure privateers of sufferers. Patients are normally very careful approximately sharing their private facts or even greater whilst it worries their private fitness facts. Most EHRs do now no longer grant sufferers the capacity to authorize and revoke gets admission to to their facts.

II. BLOCKCHAIN AND HYPERLEDGER FABRIC

A. Block chain

Block chain is a peer-to-peer dispensed ledger era that became to start with used within side the financial industry [7]. The block chain paradigm may be prolonged to offer a generalized framework for implementing decentralized computing resources [8]. It is made out of a constantly developing listing of information known as blocks that include transactions [9]. The shape of a block chain includes a chain of blocks wherein every one includes the cryptographic hash of the preceding block within side the chain. A consensus-based mechanism is used to save you the entire chain from being changed or altered and to determine which block is to be appended to the ledger [11]. The disbursed ledger isn't always managed via way of means of each person and all the individuals at the community can view it. Prior to including a transaction to the ledger, the transaction needs to be encrypted and tested via way of means of different nodes at the community the use of consensus protocols. Once a transaction is established via way of means of the bulk of nodes, its miles brought to the ledger and shared via way of means of all individuals. The brought transaction can't be deleted or changed. Thus, transactions within side the ledger are trustable, auditable and immutable. Block chains are both permission-much less or permission. In permission-much less block chain, all nodes are required to execute a widespread quantity of computational paintings called Proof-of-Work (Paw) to decide whether or not a brand new block is legitimate to be brought to the chain. In contrast, all of the nodes in permission block chain are required to be recognized and be regarded to all different individuals. The consensus protocol in permission block chain can also additionally contain Paw or different algorithms consisting of Byzantine Fault tolerant (BFT) [11].

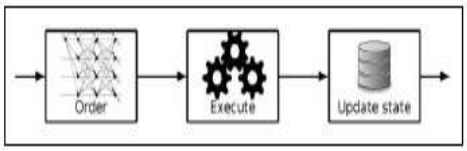

Figure 1. Order-execute architecture [10].

All block chain systems, permission or permission-less, comply with the order-execute structure wherein the block chain community orders transactions first the use of a consensus protocol after which executes them sequentially in the equal order on all nodes as proven in Fig.1. Existing permission block chains usually use BFT consensus or different protocols for atomic broadcast and comply with the equal order-execute approach. Block chains aid what's referred to as Smart Contract. It is much like an agreement within side the actual world, however its miles a digital agreement represented with the aid of using an application code that is living internal a block chain. It shops protocols for outlining the phrases of a settlement and routinely verifies and executes processes which might be primarily based totally on the ones protocols. This mechanism removes reliance on a 3rd party, so all members at the community could make agreements and transact directly.

B. Hyper ledger Fabric

Hyper ledger Fabric is a brand new block chain architecture designed as a modular and extensible

general-purpose permission block chain. Hyper ledger Fabric's design departs from the order-execute paradigm in that Hyper ledger Fabric usually executes transactions earlier than accomplishing final settlement on their order. A Hyper ledger Fabric block chain includes a fixed of nodes that shape a community. Since Hyper ledger Fabric is permission, all nodes that take part within side the community have an identity. The Hyper ledger Fabric CA is a Certificate Authority (CA) for hyper ledger Fabric that gives features for registration of identities, issuance of Enrollment Certificates and certificates renewal and revocation [12]. Nodes in a hyper ledger Fabric community take in one of 3 roles as proven in Fig. 2. Clients are the nodes that constitute end-users. They put up transaction proposals for execution, help orchestrate the execution phase, and broadcast transactions for ordering. Peers execute transaction proposals, validate transactions and hold the block chain ledger. Not all friends execute all transaction proposals, handiest a subset of them referred to as endorsing friends execute transactions. Ordering Service Nodes are the nodes that together shape the ordering service. They set up the entire order of all transactions in hyper ledger Fabric.

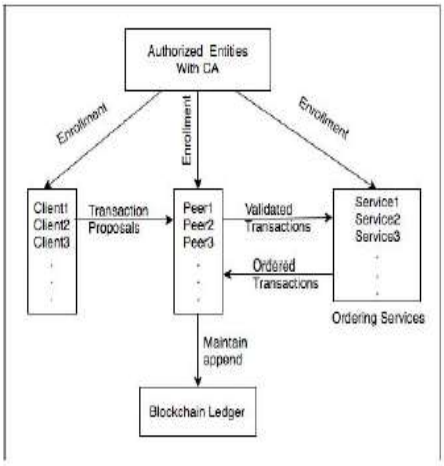

Figure 2. Hyper ledger Fabric Network.

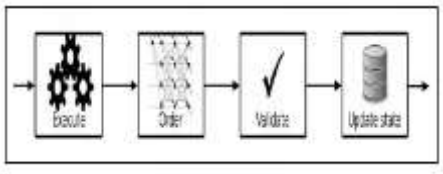

Figure 3. Execute-order-validate architecture [10].

Hyper ledger Fabric features as a disbursed operating machine that executes disbursed packages written in a general-cause programming language. Disbursed software for hyper ledger Fabric includes parts: A clever settlement referred to as chain code is the relevant part of a disbursed software in hyper ledger Fabric. It is an application written in Go, Node.js or Java language that runs to put into effect the enterprise good judgment and to create transactions. Two varieties of chain code are available. One for growing packages which can be evolved with the aid of using entrusted developers. The different kind is known as device chain code that perform positive venture for handling the block chain device An endorsement coverage is used to outline and designate the friends that execute transactions. Hyper ledger Fabric differs from different block chain structures in those transactions within side the different structures are sequentially performed on all friends once they are delivered to the ledger in a few order. On the different hand, in hyper ledger Fabric, the transactions are first performed in any order the use of chain code in predefined friends (endorsement friends) to decide the actual ordering that might offer the end result previous to including them to the ledger. Thus, a given chain code may be saved non-public from friends that aren't a part of the endorsement policy. The structure of hyper ledger Fabric follows an execute-order-validate paradigm for disbursed execution of entrusted code in an entrusted environment. It separates the transaction circulate 3 steps, (1) executing a transaction and checking its correctness, thereby endorsing it; (2) ordering thru a consensus protocol; and (three) validating transactions as according to software unique consider assumptions, which additionally prevents race situations because of concurrency. Fig. three illustrates the execute-order-validate structure. In this structure, the customers create transactions and ship them to the endorsing friend's special through the endorsement policy.

Each transaction is then achieved by particular friends and its output is recorded; this step is called endorsement. Then, customers acquire and assemble endorsement into transactions and broadcast them to the ordering section. The ordering section makes use of a pluggable consensus protocol to supply a very ordered series of encouraged transactions grouped in blocks which are introduced to the friends. Finally, friends append the obtained blocks to the block chain [10] [11].

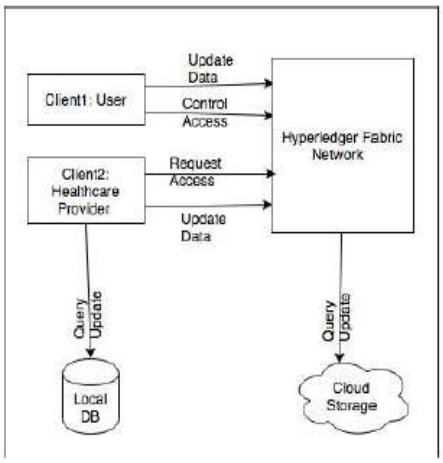

Figure 4. EHR abstract architecture based on hyper ledger Fabric

III. EHR BASED ON HYPERLEDGER FABRIC

Hyper ledger Fabric is a higher answer to conquer most of EHRs control issues. It lets in various get right of entry to levels; sufferers can get right of entry to their scientific statistics whenever from everywhere and manage who can view their statistics and how a great deal they see. Additionally, hyper ledger Fabric enables distinctive healthcare retailers to request permission to get right of entry to and have interaction with scientific statistics. Each interplay amongst all contributors is secure, obvious and auditable, and could be recorded as a transaction on a disbursed ledger. By using hyper ledger Fabric framework, EHR will beautify privateers of sufferers and facilitate complete get entry to and manage over their data. As a permission block chain, hyper ledger Fabric will permit handiest permitted healthcare carriers to study and write at the patient's clinical record. Moreover, block chain era guarantees that EHR updates are correct and tamper-proof. Fig. four indicates 4 major additives to construct a EHRs machine primarily based totally on hyper ledger Fabric architecture: User, Healthcare Agents, hyper ledger Fabric Network and Cloud Storage. In an EHR primarily based totally on hyper ledger Fabric, healthcare sellers which include clinical practitioners, hospitals, laboratories and coverage businesses can host friends with ordering offerings and nearby databases. Each collaborating fitness care agent begins off evolved up a peer or endorsing peer node with the ability to create ledger transactions. Endorsing Peers have the authority to execute chain code, Individual EHR customers consisting of patients, medical doctors and researchers can create and invoke a transaction through hyper ledger customer applications. Clients connect with friends for speaking with the block chain.

All the transactions are finished most effective in endorsing friends that include precise chain code even as the alternative friends validate and commit transactions to the ledger. The Hyper ledger gives a box to begin up a peer, utilities that the friends can use to generate cryptographic keys, and certificate, and a Certificate Authority to authorize those certificate within side the network. Each corporation that participates within side the material is issued a virtual certificates for get right of entry to the network. Public/non-public keys also are generated for every patron to signal transactions, identify/authenticate it, and begin a hyper ledger Peer. Each transaction within side the block chain includes the client's ID in addition to encrypted pointer to the scientific file. The patient's facts and permission IDs for facts get admission to could be saved off-block chain in nearby healthcare provider's database and a pointer to the file could be encrypted and saved within side the block chain in cloud storage. Cryptographic keys are used for secured facts sharing in addition to gaining access to patient's facts. A pair of personal and public keys is generated for encryption, decryption and get admission to control. Only the ones customers that are indexed in permission IDs may have the important thing to decrypt the underlying file. Personal affected person records and medical information are not reachable directly. Other contributors along with medical doctors and coverage businesses can request permission from sufferers to get admission to their saved information. For instance, if a medical doctor wishes to get admission to an affected person's scientific record, a transaction is created by the medical doctor's patron software inquiring for information get admission to with the medical doctor ID encrypted and digitally signed. Once the peers confirm that the medical doctor ID is gift within side the permission IDs, the transaction is executed. When a medical doctor requests get admission to for the primary time, if the affected person approves the request, the ID is introduced to the permission IDs within side the affected person's scientific record.

Hyper ledger Fabric capabilities permit all contributors to proportion fitness records this is correct and up to date by recording all transactions, along with affected person records accesses or changes, which have ever befell at the community. These recorded records of transactions cannot be deleted or tampered. Because of this technology, all contributors do not want to in my opinion accept as true with every different at the community. They can

engage at once with every different without concerns because the entire community is established and could confirm all the transactions on it. This implementation concentrates on sufferers first and guarantees that best the sufferers have the whole manipulate over their fitness facts and what kind of statistics they need to percentage. They are answerable for granting, denying and revoking statistics get right of entry to for another parties. They aren't required to signal a consent shape that specifies what kind of statistics will be shared. If an affected person seeks scientific remedy, the affected person could percentage the fitness statistics with the favored healthcare provider. When the remedy is done, the statistics get right of entry to can be revoked through the affected person to disclaim in addition statistics get right of entry to through the healthcare provider.

IV. CONCLUSIONS

EHRs play a big function in enhancing patient's care and improving the shipping of fitness care services. However, no matter the predicted advantages of this technology, there may be enormous issue that patient's privateers and the safety of the clinical facts will be compromised. These troubles may also hinder enormous use of EHRs. In this paper, we delivered a block chain-primarily based totally platform, referred to as Hyper ledger Fabric, which may be adopted to triumph over the ones troubles via way of means of maintaining privateers and imparting more potent security. Building EHRs primarily based totally on hyper ledger Fabric will make certain that sufferers have complete access manipulate to their records, patient's facts are saved securely and simplest established members can have interaction with patient's touchy facts. Implementing Hyper ledger Fabric functions on EHRs enables making sure fitness statistics sharing amongst all events at the community securely without worries about exposing patient's privateers and confidentiality.

REFERENCES

[1] M. R. Bowie 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-Apr- 2018].

[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.

[11] 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.

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