BLOCKCHAIN FOR ELECTRONIC HEALTH RECORDS VIA PROOF-OF-STAKE

Mubashshira Farooqui¹, Om Singh², Sagar Kumar³

¹Dept of Computer Science & Engineering, Galgotias University, Greater Noida, 1713101149
²Dept of Computer Science & Engineering, Galgotias University, Greater Noida, 1713101525
³Dept of Computer Science & Engineering, Galgotias University, Greater Noida, 1713101645

ABSTRACT

Electronic Health Records (EHRs) measure vital and sensitive personal data for assistance, and are often desired to be shared among peers. Blockchain technology facilitates a shared, unchangeable history of all transactions that creates a program of trust, responsibility, and transparency. This provides a new opportunity to implement the safe and reliable EHR management and sharing of knowledge, and harm the system. In this paper, we present our views on blockchain-based aid knowledge management for EHR knowledge exchange between aid suppliers and analytical studies. In conventional electronic health records (EHRs), medicine, customer, and other related information are separately controlled under different authorized hospitals, inconvenient to share the information. Cloud-based EHRs resolve the dilemma of data yielding in conventional EHRs. Nevertheless, cloud-based EHRs have a central problem, such as a key generator center and a cloud-based service center. We resolve to take advantage of developing technology from blockchain to electronic health records (referred to as blockchain-based health electronic records for assistance). Primary, we formally characterize the system model for electronic records in a blockchain consortium setup. Besides, authentication subject is very significant for electronic medical records. However, the current blockchain-based electronic record authentication systems have their own weaknesses. Therefore, in this work, we also propose an authentication scheme for blockchain-based e-health records. Our proposal is an identity-based signature scheme with multiple authorities and proof of stake consensus.

Keyword – Blockchain, ABS, multi-authority, trust, policy, tree, DNF, GID, central authority

I. INTRODUCTION

The blockchain is a public ledger that everyone can access but without the control of a central authority. It is a technology that enables individuals and companies to collaborate with confidence and transparency. One of the best implementations of blockchains is cryptocurrencies like Bitcoin among others, but there are many other applications possible. Blockchain technology is the driving force of the next fundamental revolution in information technology. Many applications of blockchain technology are widely available today, and each has its own strengths in a specific application area. The figure below (Fig.1) represents the Merkel tree for transactions in the blockchain.
The emerging e-health mechanism, which integrates advanced information technology, such as electronic health records and data outsourcing, is being recognized as an enabling technology that provides modern and diverse healthcare applications and services. Often times, data is collected and released for various purposes such as academic uses and government surveys, while patient privacy is protected through data collection. However, he is not satisfied due to poor privacy protection. The data released, which contains sensitive information about each individual such as name, age and health status, may harm the person’s reputation and trust in the company as it is the responsibility of maintaining the privacy of the individual record. Without rigorous mathematical evidence that appropriate privacy technologies are powerful, traditional privacy protection technologies would be no better than no privacy protection at all.

Electronic health records have greater efficiency compared to conventional paper records for storing and retrieving information. In the electronic health records, all relevant medical data is loaded and pooled into servers of infirmary. Hence, as the patients return from the diagnosis to the infirmary, patient or the infirmary can search for past information, inclusive all details as the patient's names, doctor, time, diagnosis, etc. As a principalexertion in the medicinal field, electronic health records have gained widespread heed.

However, numerous problems exist with conventional EHRs. In general, data related to medicine are stored autonomously in different research and medical organizations as they have their self-governing database management. Henceforth, whenever the victim switches from one infirmary to other, he requires to undergo medical scans anew. Thus, results in the wastage of medical data, sources, and a raise in the patients' bodies and monetary loads. Second, in EHR model, at best the jurisdictions have the data, such as hospitals. Thus, also in case of disagreement betwixt the sanatorium and the patient, the sanatorium will always be winning because it can manipulatedata or can also destroy the medical records. This is not fair for patients.

Out's proposal creates a new EHR model that can help address the problem in traditional EHRs. Solution that we provide is to take advantage of the transpiring blockchain technology descended from Bitcoin. Ordinarily speaking, the blockchain can be considered a distributed decentralized database. The decentralized feature of the blockchain gets rid of this reliance on power.

In a public blockchain-based Bitcoin system, to enter an agreement upon the block, it take off the node that scripts the block to attain an arbitrary number to meet explicit requirements of the hash function, i.e. proof of work. Although, in blockchain-centric health records that are constructed on the blockchain consortium, the authorities anticipate the block, so the genuineness of the block is always assured. So, in the Bitcoin operation, if anyone needs to manipulate or tamper a block, they only need to tamper the block in more than 51% of the blockchain nodes, while they need to update any change or delete the block for all the supremacy in the blockchain - it will be validated. Proof of Stake Based Electronic Health Records Systems.
The proof of stake can be explained by the figure above (Figure II). Here are the steps to make this system work.

1. If a node in the network wants to become an auditor, it first sends an auditor fee.
2. When the deal is confirmed, he can then wager some coins to compete with the other auditors.
3. Meanwhile, each node is responsible for broadcasting the transactions it receives from clients.
4. When a sufficient number of transactions are generated, the auditors select a leader with the maximum number of coins accumulated. The elected leader then creates a block and broadcasts it to the network.
5. Each node checks the validity of the block, performs all transactions in the block, and adds the block to the chain.
6. Block also has a special reward deal. The leader of the selected round gets the transaction fee for the transactions in the block as a bonus.

II. OBJECTIVES

The main goal is to introduce confidential "blockchain technology" to harm a patient's medical records. Protecting a patient's personal details is not just a matter of moral respect, it is imperative to document trust between the doctor and the patient as well.

Data authentication is required.

III. SCOPE

Ready access to lots of comprehensive and up-to-date patient information, fast, reliable and secure information. Streamline clinical data and powerful tools that take care of, and support the operations of the multidisciplinary team.

Minimize patient information management, paperwork, transcription, and other forms - spend less time searching for unspecified notes, x-rays, and entry or exit information.

IV. REQUIRED TOOL

Database: MongoDB database.
Server: Apache.
Back End: Java, JavaScript, Servlets.
Front end: HTML,CSS, Bootstrap.

V. RELATED WORK

There is some researched work which are attribute-based signatures (ABS) and attribute-based encryption (ABE).

Attribute-based encryption
A comprehensive search has been conducted considering the establishment of attribute-based coding. In the attribute-based coding practice, the text encoded by the dispatcher is specified by a compilation of properties. The dispatcher’s secret key is correlated along with themes as well. The user with properties that meet the threshold attributes can only decipher the ciphertext. Further development to key-policy ABE (KP-ABE) is granting nodes' secret keys to incorporate policy comprising of binary as well as limit gates. Later development to ABE methodology is that it allows the secret key to comprise negative entries. Formalizing the concept of the ABE Coding Script Policy (CP-ABE) and introduced the construct. In CP-ABE, it is possible to encode or define construction to such an extent that lone nodes with characteristics that fulfill this entrance model can decipher the text. Juxtaposed to ABS, ABE necessitates cooperation among two associates to achieve access authority.

Along these are also various study subjects in ABE such as to advance competence of ABE, and to use basic relationships between traits and a suggested ABE hierarchy diagram. To restrict users from partaking private keys for their features, which relate to privileges authorized to the acquire control system, the ABE Responsible Concept was proposed.

To reduce confidence in the authority of an individual trait, Chase and Boˇzovi´c et al intended multi-authority plans ABE with a principal jurisdiction to lessen confidence in the jurisdiction of the traits, whereby each trait jurisdiction issues only a portion of the traits. To further lessen principal jurisdiction confidence, Chase and Chow submitted multi-authority designs without principal jurisdiction respectively. Despite, a centralized jurisdiction architecture has the benefit of combining or eliminating attribute jurisdiction, which does not influence the attribute keys obtained by the node from further theme jurisdictions. Although a composition with isotropic jurisdictions for mutual distribution spends cost on synergies, it is costly on processes of addition and deletion of jurisdiction. These multiple jurisdiction actions are developed over the fundamental ABE scheme. Later the analysis for a multi-authority CP-ABE appeared, introduce DABE with a single master architecture and versatile attribute jurisdictions. Yet, Lewko and Waters did not choose a centralized jurisdiction, and simply used the hashing operations over the global user identity, to control resistance to involvement over several major formations emanating from different jurisdictions and used the latter's binary coding methodology to ensure security.

**Attribute-based signatures**

Newly, there are numerous endeavours to create trait-based signs. This concept comparable to ABS, ambiguous identity-based signature has been introduced as well as implemented, allowing users to create signatures with a portion of their properties. To accomplish the equivalent result as an identity-based signature, the idea of an attribute-based signature was introduced, although it was indicated that the model is weak to partial key replacement attack. Furthermore, for this work, the scholars do not consider any notion of secrecy, which leads to the leakage of properties practiced in composing signs to auditor. To gain poor attribute secrecy, an ABS scheme was introduced of the boundary (d, n), enabling nodes to give signedtext amidst a subsection of the attributes that meet the locked bound, and only the signer's attributes are selected by sign holder. Rather than a constant k and have flexible threshold value, scholars practiced a hypothetical collection of attributes while giving signature further created (C, G) boundary chart ABS, to achieve attribute location specificity. Though, in both systems, the size of signature elements is thrice the features applied for the signature. To intensify performance, Li et al. merging every component of the confidential feature into one while maintaining the secrecy of the attribute and the flexibility (C, G) - limit system. Besides lengthening the system deprived of arbitrary sayings scholars performed a related job while these systems could not present significant systems, that is, any method shaped by binary and limit gates. Scholar created an ABS schema utilizing monochrome extension applications that back a strong collection of rules, i.e. method consists of binary along with boundary gates. It contains the site's seclusion fronting everyone, including all jurisdictions. Though, safety is fragile because the at best construct was demonstrated in non-proprietary group model. Then, they schemed the leading ABS scheme along with adequate safety installed in the conventional system. Although, system's more complex and less efficient than the conventional system.

**VI. PROBLEM FORMULATION**

Attribute-based systems allow users to take various attributes of 1 or more exceeding attribute references, moreover, their positions lean along collection of attributes they control. Node's inclinations (for example, transferring information, accessing a source) dependent on their respective attributes. When extending manifold advantages, like moderate management value and versatility in access power, these models additionally grant basic cryptographic hurdles. Lately, coding systems which are feature-based are developed to address any coding
difficulties. One-by-one authentication solutions are suggested. A legitimate signature does not disclose other additional erudition around the methods that were used to generate signs.

In ABS nodes cannot fake signatures by traits that they don't even have by complicity. Yet schema ABS exhibit the collection of attributes that fulfill the system, the consequent search for this system provides a guarantee of privacy of the attribute of the sender, this is the authentic signer resides incognito without awe of cancellation. It cannot be distinguished among all nodes whose traits correspond to the method defined for signature. ABS have many features like access control for systems like feature-based, a personality-based signature system computes private key depending node's traits. Sender signs messages applying his private key for collection of his attributes. The sign is verified using the attribute rule and it's successful if the sender's attribute verifies under the policy. Following this approach, the sign does the identity of the sender remain incognito and attribute are used as the source of truth.

For this, we will use a signature-based on multi-source attributes, DNF MABS. According to this approach, a regular separation is used from (DNF) to prove the method, which requires the signatory to parse it while signing, but which provides the ability to express negative traits. The most significant feature is that this method reduces the value of combining other theme authorization greatly since legacy attribute authorities do not need to recalculate users' secret keys. Additionally, we use signature technology to improve efficiency. We divide blockchain-based electronic health records users into 3 layers. The initial level, assigned as Layer 0, is the Electronic Health Records Server. The following layer, assigned as layer 1, comprises various types of institutions, like clinics, dispensaries, medical coverage companies, research organizations, drug companies, etc. The next layer, to which level 2 resembles Level 1 personnel, consists of the medical practitioner, scholars, inmates, coverage agents, etc. In blockchain-based electronic health records systems, all relevant medicinal data stored will be shared with all Level 1 nodes who can attain consent, concerning the reliability of the distributed data, based upon a precise method. Nodes on level 2 are responsible for creating information related to medicine, as medicinal reports by specialists, coverage policies from a coverage agent, etc. The correctness regarding this erudition could be ensured through an appropriate sanction method by first-level nodes to respective operators.

Blockchain-based electronic health records in a blockchain consortium setup.

- **Level 0**: The Electronic Health Records Server (EHRs) is responsible for creating system parameters. Server EHRs are different in EHRs based on blockchain than EHRs based on cloud. In cloud-based EHR, only relevant medicinal records are collected in server. Though, within blockchain electronic health records, sole responsibility concerning the server is to choose the general parameters for all users.

- **Level 1**: This layer comprises infirmaries and other institutions. The nodes at this level comparable to the officials in the blockchain federation. Authorities can download and store data on their node. Layer 1 nodes also play a vital part in Key Generation and Secret Key Generation Authorities for Layer 2 nodes. Though, it's vital in consortium blockchain to check that no node can gain possession or handle Layer 2 nodes secret keys. This one of the differences between blockchain and cloud based EHR models.

- **Level 2**: It consists of medical practitioners, scholars, insurance representatives, etc. The nodes resemble operators of Level 1 nodes, for example, an insurance agent works in a health insurance company. Level 2 nodes are responsible for providing specific, relevant medical data. For instance, physicians do an examination, and insurance representatives endorse an insurance policy.

Consistent with the system model, blockchain-based electronic health records authentication involves the following two situations:

- **Case 1 (Level 2 Authentication)**: The information provided by Level 2 nodes’ needs to be validated. For instance, some doctors need to confirm the examination.

- **Case 2 (Level 1 Authentication)**: The status corresponds to the credibility of the block information provided by Level 1 nodes, that is, the authorities.

The 3elements are nodes, attribute authorities (AA), and central authority (CA). Each central authority and attribute authorities authorize individual keys for issuing keys to nodes. Besides, attribute authority would obtain the secret keys via central authority. All diverse agreements do not necessarily know others and do not trust others. They assign the attribute keys to nodes individually. although, the central authority is relied by every
attribute authority. They know adequate information about attribute authorities’ clandestine status to rebuild the clandestine values, that are utilized for creating attribute keys for nodes. This system permits creating or removing attribute authorities.

The first is the requirement that all nodes have a universal identifier (GID). These GID should have the following attributes: (1) ID should be unique for all nodes (2) ID can be verified by authorities. The GID can be any unique identity as SSN or another identification sequence that the nodes have verifiable credentials on. The necessity of this GID can be explained by the following scenarios: Alice first requests the attribute group keys B1 from reference one and Bob requests keys for attributes from group B2 with reference 2. Alice’s second request attribute set B1 reference 1 attribute group B2 from Authority 2. From the authorities’ point of view,’ both scenarios are the same because nodes cannot be identified with anything except for their traits hence authorities must communicate and verify the traits of both nodes. For prevention from collusion attack from various nodes, we bind their attributes and identity together with a unique global identity (GID), so various nodes don’t group their attributes to mimic the legitimate signer. To have a unique identity the nodes should present with their unique GID to authority to have a unified set of keys. Though, this method only designates some of the features a site should have. Hence, verification of signature should be independent of GID (besides that same GID should be allotted to all secret keys).

For implementing the method, CA rebuilds every secret value for AA as furthermore, CA creates private key d aimed at node. Hither the feign is that here are K property references. A node amidst GID u gets the ok, ωk, u attribute set from x-th attribute authority AAk (x = 1, ..., K). In place for using an arbitrary number, Tr MABS is performed. From multiple authorities the clandestine value yk is accepted and u aimed at node u utilizing a pseudorandom function f. Hence, CA presently collect the seed sk by both PRFs.

Below figure (Fig. III) represent key generation method in this system.

The offered DNF MABS schema has the resulting algorithms:

**Setup of DNF** is done set via CA, it enters the guard parameter and the threshold value d, outputs the parameters of the public parameters, secret master key MK, furthermore seeds sk to the AAk (k = 1, 2, 3, ..., K).

**Key Generation of DNF** is triggered via CA later AAk, input parameters, mk, sk, location GID u and sub-attribute set ok, ωk, u, and dCA secret key and attribute key SKk, u output to signer.

**DNFSignature** is triggered via signer, parameter input, method A, dCA, S K k, u, and M letter, and it creates a signature on the message.

**DNF verification** is triggered by a validator, input parameters, letter sign set (M, σ), policy A, further outputs an acceptable boolean value if σ is a cogent sign via the sender which has attributes ω = K k = 1 ok, u satisfies A, that is, A (ω) = 1.

**Setup of DNF** Initially, determine the traits in the U universe as factors in Z q. Suppose there are K assigned property references. Designate a default Ωk attribute set from d factors for the AAk attribute authority (x = 1, ..., K). CA selects the seeds s1, ..., sK for all trait powers, selects g ∈ G1, α ∈ Z∗ q randomly, and sets g1 = gα. Next, he selects an arbitrary factor g2 ∈ G1 furthermore computes Y = e (g1, g2). Pair hash functions are too accepted by CA as H1, H2: {0, 1}∗ → G1. General factors are = (q, G1, G2, e, g, g1, g2, Y, H1, H2), main key is
α. For the authority of the AAk attribute, its secret key is sk, this is set via CA. The secret key for CA is (s1, ..., sK, α).

**DNF Generation of key:** The node with GID receives a secret key by CA like

\[ d_{CA} = g^\alpha \prod_{k=1}^{K} y_k \]

Where \( y_k, u = f_{sk}(u) \). After that, he obtains attribute keys via the attribute authorities.

Attribute authority k-thAAk assigns an attribute key to nodes attribute set \( \omega_k, u \) as follows: Initially, determine d-1 order polynomial \( pk() \) arbitrarily so that \( pk(0) = y_k, u = f_{sk}(u) \). Create a novel attribute set \( \omega_k = \omega_k, u \cup \Omega_k \).

For each \( i \in k \), choose \( r_{ki} \in \mathbb{Z}_q \) and calculate it

\[ d_{ki0} = g_{pk(i)} \]

\[ d_{ki1} = g^{r_{ki}} \]

Later node's attribute index would be

**DNF Mark:** Suppose someone owns secret key concerning attribute collection \( \{\omega_k, u\} \) aimed at 1 kk. A), the signature \( u \vDash A(\omega) = 1 \). According to the definition of DNF, if unit separation could be met, the DNF could be fulfilled. Hence, if the registrar u finds any \( j, X_j \subseteq \omega \), then the \( j \) joint could be fulfilled, later \( A(\omega) \) has value 1. Perhaps letter \( j \) is equivalent. Given execution, sender solely chooses unit \( j \). Suppose \( I = |X_j| \), Then 1 1 d N. Aimed at every \( k \), at most succinct \( l_k \) of 1 \( X_j \) attributes is issued from the attribute authority AAK (Notelk can be equivalent to 0).

The signer defines a subset of the value property of \( l_k k \in X_j \cap \omega_k, u \) and takes the later sequence: Initially, select \( r, r' k_1, r' k_2, ..., r' k, l + d - l_k \in \mathbb{Z}_q \), and select a subset of Default attributes' \( \omega_k \subseteq k \). Determine \( S_k = \omega' k U \Omega' k \).

Arbitrarily takes \( s \in \mathbb{Z}_q \). Statistics - count \( (\varepsilon_{ki} = d_{ki}^{\delta_{ki}} g^\delta_{ki})_{i \in \omega_k} \) The expressive policy for Flexible multi-authority attribute-based signature schemes is:

\[ \{\sigma_{ki} = g^{r'_{ki}}\}_{i \in X_j / \omega_k'} \]

\[ \sigma_0' = g^{s} \]

Finally, the signature computed is

\[ (\sigma_0, \{\sigma_{ki}\}_{i \in X_j / \omega_k'}, \sigma_0') \]

**DNFVerify:** Post receiving the signature

\[ (\sigma_0, \{\sigma_{ki}\}_{i \in X_j / \omega_k'}, \sigma_0') \]

with policy A, check if

\[ e(g, \sigma_0) \prod_{i \in X_j / \omega_k'} e(H_i(i), \sigma_{ki}) e(H_2(M), \sigma_0') \in \mathbb{Z}_q \]
If the comparison is correct, the sign is correct furthermore the algorithm’s output is accepted. Otherwise, the output of the algorithm is rejected.

VII. ANALYSIS

Test: The accuracy of affirmation is supported by the latter equations:

\[
\begin{align*}
\prod \mathcal{Q}(a_k, \mathcal{A}) & - e_{g, d} \prod \mathcal{Q}(a_k, \mathcal{A}) \prod \mathcal{Q}(a_k, \mathcal{A}) \\
& - e_{g, d} \prod \mathcal{Q}(a_k, \mathcal{A}) \prod \mathcal{Q}(a_k, \mathcal{A}) \\
& = e_{g, d} \prod \mathcal{Q}(a_k, \mathcal{A}) \prod \mathcal{Q}(a_k, \mathcal{A}) \\
\end{align*}
\]

VIII. DESIGN

The model scheme is the most crucial and essential part of any structure as it is used to develop the model as of conjecture. Thispartemphasiseson module, structure, and factors that are consolidatedin the direction of forming structure of the entire system. The scope of this offered structure is to design such a decentralized model as a secure, private, blockchain model aimed at EHR.

Later is EHR model design which is proposed (Fig IV).

Table 1 and table 2 are comparison of two schemes.
EHR Architecture defined in levels (Fig. V).

Use Case diagram of level 0 for data provider and other nodes in blockchain (Fig. VI).

IX. IMPLEMENTATION OF MODULE

**Block structure**

The block structure includes the components: index, timestamp, data, hash, and previous hash.
A blockchain is built unitedly by several chunks linked in a system, creating distributed reinforcement. Block’s header has the hash of the preceding block. A block has 3 components as: the information, present block’s hash, and preceding block’s hash. Information of block is related to sort of chain used. For Bitcoin, type of information is the coin, e-money. The hash collected in blocks has the SHA-256 encryption to uniquely identify the block in the chain.

The figure below (Figure VII) shows the blocks in the blockchain.

**Figure VII**

**Block’s hashing**

Block must fragment for preserving probity of information. The hashing technique SHA-256 is used to seize block content.

**Block’s generation**

To generate a block, the hash of the previous block and generating remaining needed element (= index, hash, data, and timestamp). End-node provides the final block.

**Proof of Stake**

Based on `SHA256(hash of previous block + address + time of block creation) <= 2^256 * balance`

**Storing the blocks**

Blocks are stored in chain format. The new or current block links with previous block via previous block’s hash.

**Block’s integrity**

Blocks or chain are verified via checking their integrity. The hash which is received to new block of preceding block is verified with preceding block’s hash code. If the condition fulfills the chain is integrated.

X. CONCLUSION AND FUTURE SCOPE

In the paper, we presented how blockchain technology could be beneficial to the healthcare division and how it can be practiced in electronic health records. Notwithstanding advances in the healthcare division and technical modification in EHR models, they still face several of the concerns that this new technology addresses, such as the blockchain. Our offered structure is a blend of solid record storage along with strict access controls for those documents. It builds such a model that is easy for users to practice and experience. Also, the structure offers steps to guarantee the method addresses the data storage dilemma where it uses ABS. Role-based also serves the model because medical documents are only availed to trusted and relevant people. This additionally determines the erudition inconsistency issue in the EHR model. In the future, we intend to achieve more functions. For the aforementioned, we need specific deliberations because we require to determine how much a patient will pay to consult a doctor about this decentralized model operating on the blockchain. We will too need to establish specific strategies and rules that regulate with postulates of the healthcare division.

REFERENCES