Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 3, July 2021:3008- 3016

Research Article

Health Identity with Blockchain

Prince S Thomas[1], Vishnu S[2], Anitha Thankam Alex[3], Rafeena R[4], Jomy George[5]

Abstract

Time is a precious element considering the medical field. It can be used to save a life and also misuse of time can waste a life. When a patient is brought in with an emergency casualty, every second counts. Knowing the medical history is an important task in every emergency situation. Finding and analysing the results takes a lot of crucial time. Implementing a solution to access a patient's previous medical data along with personal details will reduce the wastage of precious time. The solution we suggest is the best to provide important data about a patient in the most secure manner. Medical data are to be handled with most confidentially. Implementing this solution in blockchain technology increases the confidentiality of the data being stored. To implement at most security the data is not stored in any of the databases. Every bit of data is encrypted which can only be accessed and monitored by the patient only. At any situation when the data is required to share with authorities the patient can decide which all data to be shared. At emergency situations only a particular set of data is shared which is approved by the patient beforehand. Every data shared can be monitored by the patient and permissions can be revoked. Implementing this solution is sure to bring a great change in the medical field saving a lot of lives at the earliest without wastage of the precious time.

Keywords: *blockchain; hyperledger; fabric; composer; NodeJS; health identity; HER*

[1] Prince S Thomas, TKM Institute of Technology, Department of Computer Science and Engineering, princesthomas3333@gmail.com

[2] Vishnu S, TKM Institute of Technology, Department of Computer Science and Engineering, vishnu14000@gmail.com

[3] Anitha Thankam Alex, TKM Institute of Technology, Department of Computer Science and Engineering, anithathankamalex@gmail.com

[4] Rafeena R, TKM Institute of Technology, Department of Computer Science and Engineering, rafeenar26@gmail.com

[5] Jomy George, TKM Institute of Technology, Department of Computer Science and Engineering, jomygeorge2005@gmail.com

Introduction

Hospitals are a place that 'saves lives.' In certain situations, this is not the case. Due to some lack of knowledge about the patient, it becomes difficult to for the medical department to save life. Sometimes it happens due to unavailability of required documents. Also, if a patient is new to a hospital, i.e., the hospital has no prior knowledge about the patient's conditions they have to do some check-ups to formulate the basic condition of the patient. This is a time consuming process. For a normal patient it is ok. But in a situation like an emergency causality being taken in by a hospital they need to know the medical history of the patient so they need to do all these check-ups. But doing these will take away the precious time to save their life. To avoid this situation this project can be implemented. This project focuses on making all the medical data of any patient accessible anywhere at any time. This will reduce the time taken to do the initial check-ups and can 'save lives.

This project uses the technology Blockchain. Blockchain is a tamper resistant and secure method of storing database. It is a decentralized system. So, data stored are immutable. It is a chain of digitalized information, which are linked cryptographically. Every block of data is encrypted using public key encryption. This doesn't require a centralized authority. Self-Sovereign Identity is the domain used. With the help of SSI, we can make sure the data is safe with the holder. SSI implements a system that will help the holder to keep track of their data, i.e., only they can have permission to share revoke any data stored about him in the blockchain.

Blockchain

Blockchain as the name says, is a chain of digitalized information in which blocks of transactions are cryptographically linked. It is decentralized system and does not need a central trusted authority. In the earlier stages, it was developed for keeping a financial ledger. Network nodes present in the blockchain are responsible for the authenticity and reliability of the stored data in the distributed ledger. Any data uploaded is stored in multiple nodes across the network. Thus, if a data is edited or manipulated, that data has to be edited in all the nodes that store that data simultaneously. If any mismatch occurs in the data this means the data has been tampered with. Thus, assures authenticity and reliability. One can connect to the blockchain by launching a network node in blockchain. Each node in blockchain contributes to decentralization of the network and is capable of storing a complete copy of the distributed ledger. The ledger can be

accessed and viewed by any user. Users can view all the transactions conducted or stored on the network. Proof of work is the original consensus algorithm in blockchain network. This algorithm is used to confirm the transaction and creates a new block to the chain. Nodes participate in consensus, share information about transactions, confirm transactions and store copies of the confirmations. The decentralized nature of blockchain makes them immutable and hence provides security. Use of blockchain in the proposed system makes it tamper resistant. Once a data is added into the blockchain network it remains in the network, and can be used for validation.

Consensus Mechanism

In any centralized system there is a central administrator who has the authority to maintain and update the database. Adding, deleting or updating any records in the database is performed by the central authority. He remains the sole in-charge of maintaining the record. But in such a situation if there occurs any security breach, the entire data in the database will be compromised. Unlike this the public blockchain uses a decentralized system, which is a self-regulating system that runs on a global network. Here, there is no need of a centralized authority. Verification, validation and authentication of any transactions occurring on the blockchain network will be managed by the contribution of hundreds and thousands of participants (nodes) in the network.

Since the publicly shared ledgers are dynamically changing, we need a real-time, reliable, and secure mechanism to ensure all the transactions occurring in the network are genuine. All the participants should agree on the status of the shared ledger. This task is performed by a consensus mechanism. Consensus mechanism, decides if the transactions are legit. Proof of Work (POW), Proof of Stake (POS) are the three major consensus mechanism used commonly.

Proof of work is an approach used in blockchain. It is a consensus protocol that provides rules for creating new blocks. To add a block of a transaction, nodes have to perform several calculations or work to prove that they will not attack the network. Each node in the network calculates the hash value of the block header and the consensus require the calculated value to be smaller or equal to a certain value. Once this condition is met by a node, it would broadcast the block and the rest of the nodes mutually confirm the correctness of the calculated hash value. Once the block is validated, other nodes will append this new block of transactions to their blockchain. This is what happens with a Proof of Work Consensus Mechanism.

Proof of stake is an alternative to PoW. PoW wastes too much resources in doing the calculations. PoS on the other hand saves energy and is more effective. In PoS, the selection was made based on the account balance and the miners need to provide proof about the amount of currency they own. People with more currency were believed to be less dangerous. The method of selecting people based on their account balance was unfair as the person with more currency become dominant in the network. As compared to PoW, PoS is more effective and the mining cost in PoS is nearly zero.

Literature Survey

A. Application of the Blockchain for Authentication and Verification of Identity

The greatest obstacle for migrating any services online is the ability to secure the data and verify the identity of the users of that service. Currently, online authentication relies on a password or on rare occasions the use of dual-factor authentication. The problem with these methods is that passwords are notoriously insecure and dual-factor authentication generally depends on sending a code over SMS or any third-party service. A solution to this problem could be the blockchain, where, by distributing a ledger among all members of the network, blockchain authentication eliminates someone from maliciously modifying the ledger. Every time a 'transaction' or block of data is added to the chain a majority of the network must verify its validity. This guarantees the integrity of the ledger. One could then use public key encryption, such as the extremely secure RSA encryption, to securely send their credentials. The recipient could then verify this against an entry in the immutable blockchain resulting in an incredibly secure and reliable way to handle verification of identity.

B. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

An encryption method is presented with the main property that publicly revealing an encryption key does not thereby reveals the corresponding decryption key. This has two major consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only that person can decipher the message, since only he knows the corresponding decryption key.
2. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his

signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems.

A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1).(q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor.

C. MedRec: Using Blockchain for Medical Data Access and Permission Management

Years of heavy regulation and bureaucratic inefficiency have slowed innovation for electronic medical records (EMRs). We now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. This paper, propose MedRec: a novel, decentralized record management system to handle EMRs, using blockchain technology. This system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, the system manages authentication, Confidentiality, accountability and data sharing – crucial considerations when handling sensitive information. A modular design integrates with providers existing, local data storage solutions, facilitating inter-operability and making the system convenient and adaptable. The System incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain “miners”. This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work concept. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata.

D. Identity Based Cryptosystems and Signature Schemes

This paper introduces a novel type of cryptographic scheme which enables any pair of users to communicate securely and to verify each other’s signatures without exchanging private or public keys, without keeping key directories and without using the services of a third party. The scheme assumes the existence of trusted key generation centres, whose sole purpose is to give each user a personalized smart card when he first joins the

network. The information embedded in the card enable the users to sign and encrypt the messages he sends and to decrypt and verify messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centres do not have to coordinate their activities or even to keep a user list. The centres can be closed after all the cards are issued and the network can continue to function in a completely decentralized way for indefinite period. The scheme is based on a public key cryptosystem with an extra twist: instead of generating a random pair of public/secret keys and publishing one of these keys, the user usually chooses his name and his network address as the public key. Any combination of name, social security number, street address, office number or telephone number can be used, provided that it uniquely identifies the user in a way he cannot later deny and that it is readily available to the other party. The corresponding secret key is computed by a key generation centre and issued to the user in the form of a smart card when he first joins the network. The card contains a microprocessor, an I/O port, a RAM, a ROM with the secret key, and programs for message encryption or decryption and signature generation or verification.

Proposed System

A person goes to a clinic to undergo some basic tests in their body. Initially if the person is new to the system their personal id will be created by the clinic through the online software. And the result of the test will be provided to the person through the online portal. The clinic send a request to the person for granting permission to upload the test result. The person can accept or reject the test result. If the person accepts the request, the test result is uploaded to the person's account. This medical data, uploaded by the clinic can only be viewed by the person. If the person goes to a hospital, and the hospital requires the person's medical reports received from the clinic, the hospital will request for the medical data through the online portal to the patient with the help of their id. Upon receiving the request, the patient can select the data they wish to share with the hospital and the time until which the data has to be shared. Thus, on accepting to share the data, the hospital will get the data required. After the assigned time, the data will be removed from the hospital records. If this person met with an accident and is taken to the nearest hospital, and the hospital doesn't have any data regarding the patient, they have to conduct tests in order to get the data. But since the patient have the medical record in their wallet the hospital can use this software to get data about the patient quickly without taking tests for each data to

be collected. Here the patient will have a person added as the trusted contact in their record, this person will give permission to the hospital to access data from the patient's wallet.

If a person has to apply for a job, he/she have to submit their medical details, the proposed system helps us to share these details with the person's account. The company can view and verify these details. For this the company requests access to the medical data. If the person grant permission, the company can verify these details. If the person deny permission, the company cannot access the data. In a situation where a person has to provide some certificate regarding their medical condition, they can use this method to provide the certificate.

System Implementation And Architecture

Each person (holder) who visits a health centre for the first time will be registered into the network and will be provide with a unique digital identity. This unique digital identity will be stored in the ledger (blockchain). Every UID (holder identity) will be equipped with its own wallet. When a holder undergoes any medical diagnosis in a clinic or hospital (issuer), the results of that test will be sent to the holder wallet, through the network with the help of the online portal referring the holder's UID. The patient or the holder can then decide whether to store this information or not. If he/she decides to store this information, the digital certificate of that result will be stored in the user's wallet and hash of this certificate will be added to the ledger, which can be further used for validating the certificate.

In situations, when a patient visits another hospital or any other institutions that require their medical data, that institution acts as the verifier. Once the holder visits such an institution (verifier), they first scan the holder's UID and verifies the holder's credentials by comparing with the data stored in the ledger. Once the credentials are verified and if the past medical data of the patient is required for the treatment, they can easily be obtained from the holder's wallet. In such a scenario, the hospital will request the user for the required data. The patient can evaluate the request and choose whether to provide all the requested data or not. He or she can also select specific data to be shared and reject all other data requests. Once the request is approved the data can be shared from the user's wallet. This data is time bounded. The holder can decide how long the data should be available to the verifier. The data will be removed from the verifier's system when the time reaches the limit. The contents of the holder's wallet cannot be accessed by any other party without the consent of the holder.

The holder can assign a person to be a trusted contact, and that person can access the holder's wallet in case of emergency situations. The holder can otherwise choose not to assign a trusted contact and rather choose to set some information as public that may come useful in an emergency situation.

Result and Discussion

This project generates a software that helps on managing the medical records of any individual. Any medical data can be stored and shared through this software. Entire control of the medical data in this wallet is in the hands of the individual. This system can simplify the life of the individual by making their medical data accessible across all the health care centres he visits. In cases when a trusted contact can't be reached during any emergency situations, accessing the data is difficult. To avoid this situation, biometric verification can be added to this system, as a future enhancement.

Conclusion

Health Identity is a method of storing all the medical details about a person securely in a manner only the holder can give and take access of the data stored about him in the blockchain. It's completely tamper-resistant and secure. For a person to tamper with the data stored in blockchain he/she has to tamper with the entire blockchain ecosystems which is impossible. The data is encrypted with the famous RSA encryption. It uses, a public and a private key only the holder will know the private key. So, anything encrypted with the public key can only be decrypted by the holder of the data. This Makes the system much more secure. Implementing this system is going to make changes in the medical field. A lot of precious time can be saved since, time is the most important factor for a person. Hyperledger Fabric and Composer can be used to develop this software. Fabric is a modular framework for applications and software. Composer is a set of collaborations tools used for development of software. ReactJS or NodeJS can be used to develop the software. REST API (Representational State Transfer) is created by the composer.

References

1. Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, "A survey of attacks on Ethereum Smart Contracts," Universita degli Studi di Cagliari, Cagliari, Italy
2. Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2nd International Conference on Open and Big Data, 2016
3. Adi Shamir, "Identity-Based Cryptosystems and Signature Schemes"

4. RL Rivest, A Shamir, and L Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems
5. Ben Cresitello, Dittmar, “Application of the Blockchain For Authentication and Verification of
6. Identity,” Noveber 30, 2016
7. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017