Blockchain Technology In E-Healthcare Applications

Elayaraja P
Software Engineer-Chennai

ABSTRACT
E-Healthcare promises to be the next big wave in healthcare, so the security is must in this system. The security in the sensor network communication is highly recommended to provide data confidentiality and authentication. Many number of security algorithms are proposed by many authors, among the all security model, the Blockchain technology (BT) with distributed Ledger Plays a maximum security level of E-healthcare system. After this process the BT approach applied to secure the sensitive data with different layers function and encryption, decryption process. Once the health information is secured, the access control process considered to the authentication purpose. At finally the simulation results are carried out to analyze the performance the E-healthcare data security model, in terms of throughput, emery and security Level measures.

Keyword: BT with distributed Ledger Plays a maximum security level of E-healthcare.

I. INTRODUCTION
Blockchain Technology (BT) works by storing information in recording ledgers that are distributed in a decentralized manner across all computing devices that are part of the blockchain infrastructure [1-10]. The ledger is stored in a decentralized network of nodes that are created through cryptic processes computed by all miners within the network [11-20]. The inherent characteristics of blockchain architecture and design provide properties like transparency, robustness, auditability, and security [21-30]. A blockchain can be considered a distributed database that is organized as a list of ordered blocks, where the committed blocks are immutable [31-40]. Let’s assume a scenario where patients keep their data in any Electronic Health Record (EHR) system for preservation and also for further access [41]. Patients share their personal data with the doctors and healthcare organizations with the help of these EHR systems. System will store the data on blockchain when the patient shares her data with the system [41-56]. To ensure the confidentiality of outsourced EHRs, existing scheme employs a smartphone-based key agreement scheme to establish a secure channel between the patient and the doctor [57-60], would use the distributed ledger to allow a person to prove he/she exists at a certain time and place, and is verified by a group of individuals through the use of the distributed nature of block chain [61]. Selecting the exact e-healthcare data, the classifier model used, from the classified data, able to access those records and such access needs to be enforced and monitored [10]. Blockchain based access control manager for heath data to enhance the interoperability of this system. Off blockchain mechanism with the involvement of public blockchain was proposed as an access control manager of healthcare data [62].

II. RELATED WORKS
Blockchain has a range of built-in features, such as distributed ledger, decentralized storage, authentication, security, and immutability, and has moved beyond hype to practical applications in industry sectors [63]. Even with these improvements, there are still concerns as blockchain technology has its own specific vulnerabilities and issues that need to be addressed, such as mining incentives, mining attacks, and key management. A comprehensive classification of blockchain-enabled applications across diverse sectors such as supply chain, business, healthcare, IoT, privacy, and data management, and we establish key themes, trends and emerging areas for Storing and running computation on sensitive private healthcare data in cloud are possible by decentralization which is enabled by peer to peer (P2P) network [64-65] leveraging the decentralized or distributed property, blockchain technology ensures the accountability and integrity. Information security and privacy are enhanced by the blockchain technology in which data are encrypted and distributed across the entire network [66]. It can ensure both information security and privacy while simultaneously increasing the trust of the public sectors. The relevant aspects of the blockchain technology and we discuss some use cases in the healthcare area which might be improved by the use of this technology [67-70]. It’s provided the security, anonymity and data integrity without any third-party
III. METHODOLOGY FOR SECURITY

Blockchain innovation as an approach to achieve a reliable and user enabled answer for e-Health environment. Electronic Health Records (EHRs) are never made to deal with lifetime records among different organizations, and patients leave their information dispersed among different institutions. For secure the healthcare database, basically classifier, that is Support Vector Machine (SVM) utilized to categorize E-healthcare data in sensitive and non-sensitive data. Enhancing the security of E-healthcare services information, user-based access control used. The underlying distributed ledger record innovation of Bitcoin is additionally demonstrated as the Bitcoin square chain, to recognize it from other square chain advancements [71-75]. This blockchain technology utilized to support drug prescriptions and supply chain management, pregnancy and any risk data management as well as to support access control, data sharing and managing of an audit trail of medical activities Healthcare systems could improve security and reliability of patients' information since patients would have power over their social insurance records. At last, the authorization procedure determines which part of information can be confined to an outer requester upon the security approach.

3.1 BT- A Distributed Ledger Technology

It’s a distributed database, maintained by a consensus protocol run by nodes in a peer-to-peer network. This consensus protocol replaces a central administrator, since all peers contribute to maintaining the integrity of the database. This distribution model consists of different layer functions that are fabric layer, application layer and networking layer. This all layers are used for secure communication consensus, public key infrastructure, and database structuring. However, there are concepts for decentralized governance model that sit in the application layer, and enable network participants to have a say in future updates to the fabric layer.

While distributed ledgers allow any peer to create new transactions and read from the shared database, malicious changes to historical transactions are spotted by honest peers. Distributed ledgers such as blockchain are exceedingly useful for financial transactions, not only this, its applicable in E-healthcare applications. They cut down on operational inefficiencies. Greater security is also provided due to their decentralized nature, as well as the fact that the ledgers are immutable. Specialized distributed consensus protocols enable databases to be shared in a peer-to-peer network without the need for all participants to trust each other. Distributing databases between multiple peers in a trustless fashion has enabled novel decentralized applications such as cryptographic currencies.

3.2 E-Healthcare Security analysis Via BT

Hyper ledger is considered a permissioned BT, which means that only designated parties are allowed access to the BT, in contrast to the public blockchain which is open to all. In healthcare, this type of blockchain design can be useful as it defines a defined user base consisting of providers, payers and other affiliated parties to only be allowed access in the blockchain. From the classified healthcare data, we are taken sensitive data to security model, In addition to the protocol, additional inclusion and exclusion criteria were employed based on the significance of the topic and the frequency BT, Healthcare, or both were referenced in the research.

Procedure of BT

BT is a block that records some of the transactions made in a given amount of time. A block may be understood as an individual bank statement. Blocks are linked together in chronological order using hashes so that nobody can tamper with this ledger, while being accessible to everyone. Each block contains the hash of the previous block [18]. Therefore, if a person intends to tamper with it, he must change all the hashes of the blocks before. This BT model worked based on Hash function concept, a single node may announce its conclusion about the submitted information. Other nodes in the system just verify it. The miner, which announced the conclusion, first, is rewarded after majority of the other nodes verify it as being correct. Since verifying the result is a computationally inexpensive task, the process does not take much time. The only way to change the blockchain data is to have more than 51% of computational power, and in that scenario, it is more logical to mine rather than attack for benefits. The blockchain is also well suited because it does not have a single point of failure, which makes it robust.

Important Elements in BT

Distributed Ledger: Sensitive E-healthcare data are distributed ledger offers a measure of resilience by
limiting the impact of a cyber-security incident experienced by any single node.

**Hash Functions:** This function utilized to the secure the information in cloud storage systems, it makes it difficult to reproduce the data from the hash alone.

- The proposed data secure approach considers the hash function with three features given below which needs to be fulfilled for this examination.
- The previous block hashes can be more than one if the blockchain is branched and all of them are appended.
- Basically each block contains the block hash with previous block hash cash and time stamp, block version with nonce, and Target address include the message.

3.3 Access Control Model for E-Healthcare

Control Security Model architecture is based on the scenario of data interoperability and supports the security fundamentals of healthcare systems along with the capability of providing fine grained access control. It makes use of three different security and privacy requirements: identification, authentication, and authorization. Identification is not an original security issue in itself, but its purpose is to identify users. Thus, it is used to affect the way a user can be authenticated. Better secure the E-health data some terms are considered that is

**E-Healthcare Data owner:** Attribute-based access policy, separating his own particular data into various parts, encrypting each part by using symmetric encryption strategies under various content keys.

**User:** The user is approved to access the data if the access policy associated with the cipher information which was characterized by data owner is fulfilled by data attribute.

**Service provider:** The SP consists of data servers to control data access, and a data service director to deal with the attributes of users.

**Central authority:** This is a completely trusted gathering that is in charge of entitling, denying, and updating the attributes of users. It produces public and private parameters for the frameworks and stipends the diverse access to users based on their attributes.

IV. RESULT ANALYSIS

Above discussed methodology are implemented in MATLAB 2015a with i7 processor and 4GB RAM. To evaluate the performance this method, E-healthcare data are utilized. The performance analyzed in terms of Throughput, Energy and Encryption & decryption Time.

Figure 1: Graph for E-Healthcare Data Classifier

Figure 1 shows the E-healthcare data classification accuracy, here our selected classifier Model compared to the K-Nearest Neighbor (KNN) and Naive Bayes (NB) classifier. “X” axis represented the size of data and “Y” shows the Accuracy level of data classification process. For example the database size is 300 the accuracy of SVM is 89.22%, it’s compared to the NB, and the difference is 2.5 to 6%, similarly KNN classifier. From this graph the classifiers show good to excellent results on data classification.

V. CONCLUSION

This BT concept was originally associated with digital currency, but many other potential uses for the technology are emerging, including Integrity applications for healthcare data being transacted around a large multi-tier network and or archival systems. This chapter detail discussed the Security of E-healthcare in ledger distributed system, its get better security level, throughput and energy level. From this study to get the maximum scalability, security and performance of E-healthcare security process. As using BT cipher encryption it is hard to break the security by intruder as compare to that of stream cipher. Nice trade-off between security and performance will help to put forward good solutions.
to actual applications. In future optimization techniques with BT used for healthcare data security model.

**REFERENCE**


Journal of Emerging Technology and Advanced Engineering, 2(6).


Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.


