Securing Privacy of Patients' Record by Blockchain

[1]Sarang Surve, [2]Shubham Surve, [3]Sofiya Shaikh, [4]Dipali Thakur
[1-4]Graduate Students
[1-4]Computer Engineering Department,
[1-4]Pillai HOC College of Engineering & Technology, Mumbai University, Rasayani, Maharashtra, India

Abstract : In the generation of Big Data, quickly developing information is continually gathered and broke down, by which it prompts advancement and financial development. Today, information has become an important asset in the advanced computerized world. From a security viewpoint, analysts created different strategies focusing on protection stresses over personal information data. Lately, another class of responsible frameworks developed called Bitcoin utilizing Blockchain. The blockchain is a distributed and decentralized records that stores information like the exchange of transactions among people and that record is openly shared over all the nodes of its network. This system helps to protect against Data Ownership, Information records Transparency and Auditability & Fine-grained Access Control. The blockchain is a strong and general issue that is not limited to just the financial sector. In the digital world, It is imperative that information records' respectability and secrecy stays consistent. In day-to-day life, Patients doesn't want to share information about their illness but also want the cure for their illness. Whereas, Researchers want such an illness sample to research and develop medicines. By the help of the blockchain system, Patient information is not completely disclosed to towards researcher of that illness, only the illness sample is shared with patients' identity number. This paper focuses on the application for data like Patients' records by Blockchain. Using Blockchain the big data and other huge amounts of data and its transaction will be secured hence risk about data privacy will be preserved by which the patients' certainty about their information will be luxuriously compensated.

Index Terms **- data, blockchain, medicine, patient record, privacy.**

I. INTRODUCTION

In today's digital world, Data is amassed and studied, leading to innovation and economic growth. Organizations and Commercial Businesses use the collected data to optimize the corporate decision-making process, personalize services, predict future trends and more. Digital Information has become very essential for the development of mankind[1]. While we gather all the profit gained from such a data-driven world, there is an expanding social issue about such data privacy. In centralized organizations – both open and exclusive closed, accumulate a large amount of every individuals' personal and delicate information. Individuals have little or no authority over their own information data that is stored and how it is utilized. In recent years, Public Mass Media has repeatedly covered controversial events related to privacy. Among the better-known case is the report about NSA's surveillance program called PRISM[2], and Facebook's large-scale scientific experiment that was allegedly formed without notifying participants explicitly[3]. The amount of data information is swiftly expanding in our world. According to a recent report[4], it is estimated that 20% of the world's data has been assembled in the past couple of years. The greatest online social network, Facebook, has collected personal data about 300 petabytes since its initiation[5]. Hence, it is a hundred times more then the amount of the Library of Congress has collected in over 20 decades[6]. The most reviewed topics were Blockchain Technology and, depending on it, cryptocurrency. In Google Trends, "Bitcoin" became the second highest searched word in 2017 at the bottom of global news[7]. Although Blockchain Technology is the best-known application area since it is strong and should not be limited to the business sector only. Wherever the digital records are kept, which should be maintained unchanged, Blockchain technology can be considered. Even The Healthcare Sector can achieve benefits from Blockchain technology at various stages like, from patient's report and diagnostic sample for research, to process of drug and medicinal product development, to the better preservation and use of patient records through the e-prescription process.

II. LITERATURE SURVEY

Blockchain has first been introduced in 2008. To overcome the existing security problem of personal data. It has a distributed & decentralized platform for sharing, collecting & storing the data is simpler. Blockchain in the financial sector is used for the transaction of Bitcoins & cryptocurrencies which is digitally accessible & trusted without a central authority - a middleware. The user is less concerned about the attack & only the user has control about them record as a hash value is used for encryption of data.

Blockchain has major benefits in healthcare from maintaining the patients' details & also drug product records. The medical records are secured which is distributed in a secure way. The patients are the owner of their own medical records & has the power to authenticate the third party. It saves time & money & also avoids unnecessary issues to the patients.

III. EXISTING SYSTEM

An analysis of the recently introduced Blockchain based systems in the healthcare industry may show us how to improve this technology for more widespread use. Estonia, a leading country in digital technologies, has been the first country to integrate Blockchain technology into the healthcare system. This section will first examine the Estonian system. Several commercial systems with more limited application areas will then be analyzed.

Estonia is an EU country that has invested heavily in digital technology for over 20 years. In 2000, the Estonian parliament adopted both the basic human right of internet access and the legality of digital signatures. This also means that digital signatures

will be accepted in all Estonian institutions. In the same legal framework, it is stated that only "master record" can be updated when "once-only" writing is not possible. Thus, the storage of multiple copies of the data has become unnecessary and invalid. All these goals can be realized with Blockchain technology.

Estonia's Blockchain technology is a KSI (Keyless Signature Infrastructure) based, multi-purpose system integrated into the registration system of many government agencies. This system aims at fast detection of voluntary or involuntary data manipulation. Because it is a multi-purpose system, the data is not held in the Blockchain system, only the hash value of the information data stored in the conventional databases is recorded in the system and the user gets a token for each recorded original data. When a data is entered into the system, it is compared with the stored hash values in the system and the originality is checked first. Thanks to this structure, the user data, for example, the MR data of the patient, is not taken out of the hospital system.

The platform that enables different institutions to participate in the Blockchain in the Estonian system (e-Estonia) is called X-Road. X-Road provides the integration of the databases of the government and private sector institutions included in the system and the communication with the data transfer between the institutions. For secure data transfer, all data that goes out of the office on X-Road are digitally signed and encrypted, and the data coming from outside will be processed in the data log only after verifying the correctness [8]. X-Road also supports functions such as writing to the database, transferring large data files, and searching the databases in the system.

The health system of Estonia also takes its place in this general Blockchain system. In the system, the patient is observed as the principal owner of all his own data and decides himself/herself of the access of third parties. Who is viewing the data is logged in the Blockchain system and it is considered within the scope of the criminal offence to look unauthorized to the patient's data. The system has two main applications: 1) Electronic patient records, 2) Electronic prescription. The electronic patient registration system combines the information from many health institutions and acts as a centralized national system to provide this information to the patient and to healthcare professionals with access to it at a standard interface. The reliability and access log of patient records are controlled by Blockchain technology. The e-prescription has been electronically filled to the nearest of the prescriptions (99% at the moment). While the pharmacy can access the prescription with the patient's identity card, the system can automatically charge the insurance information and charge for the prescription. Instead of visiting the doctor for the drugs to be taken again, the doctor can write a new prescription through the e-prescription and the medicine can be taken from the nearest pharmacy.

It is based on the use of KSI Blockchain Mixed Trees (Hash Trees, HT). To support a high number of signing operations, all operations in a time slot are collectively recorded as a mixed tree. The key values at the top of the trees are linked together to form a generic HT, and the name is called karma. The key at the top of the calendar has been changed into a system in which the date change is made very difficult by pressing at a physical moment like a newspaper during regular time intervals [9].

We recently announced that we will compile and present the patient information collected with Apple iOS 11.3, which is collected from Personal Health Registers (12 hospitals so far in the US). Although it is not in the blockchain technology, it is thought that this is a very important development in terms of the compilation of the health records and the interest of technology companies in the subject [10].

Not long ago, in January 2018, the Dubai Health Authority (DHA) announced that they would develop an integrated system for individual vaccine registrations [11]. At the same time, DHA is building a Blockchain-based Health Personnel Registration System, which aims to speed up the process of giving part-time work or temporary medical licenses to professionals for a certain period of time.

IV. PROPOSED SYSTEM

The three subjects involving in our system are Individual Users (can be patient or doctor): using mobile phone who are interested in seeking benefits by applications, Services that provides applications who require computation for handling individual data for operational reasons and Nodes by which entities committed with preserving the blockchain and storing a shared private key-value data for beneficial purpose. Note that while users in the system normally remain anonymous, we could store service profiles on the blockchain and verify their identity. The system itself is designed as follows. The blockchain acknowledges two new forms of activities: T-access which is used for access authority management and T-data which is used for storage of data and reclaim. These network operations will be effectively incorporated into a mobile software development kit (SDK) that services can use in their development process. To demonstrate, consider the following example: an individual user installs the application program which uses our designed platform for preserving his/her medical record privacy. As the user client joins for the first time, a new shared (maybe user or service) identity is generated and sent, along with the associated consent, to the blockchain in a T-access transaction. Data collected on the phone (e.g., sensor data such as Geo-location, Blood-Pressure Monitor, etc) is encrypted using a shared encryption key and sent to the blockchain in a T-data transaction, which later forwards it to an off-blockchain key-value store, while accommodating only a pointer, which is the SHA-256 hash of the data, on the publicly shared ledger. The service and the user can request the data using a T-data transaction with the pointer(key) linked to it. Then the blockchain will verify the digital signature which belongs to either the user or the service. For the service, its access permissions to the data are monitored and verified as well. Finally, the user can modify the authority granted to service at any time by issuing a T-access transaction with a new set of authority, containing revoke access to previously stored data. Developing a mobile-based dashboard that allows the patient to overview of its data and the ability to change authority which is genuinely irrelevant and is similar to enhancing centralized-wallets. An implementation of Kademilia, a Distributed Hash Table (or DHT), by which the off-blockchain key-value is stored with added persistence using LevelDB2 and an interface to the blockchain. The DHT is preserved by a network system of hubs & nodes (conceivably disjoint from the blockchain network), who satisfy approval of reading/write transactions. Data are adequately randomized over the hubs & nodes and cloned to guarantee high accessibility. It is useful to note that alternative off-blockchain solutions for storage could be considered.

V. CONCLUSION

Blockchain technology has the advantage of providing verifiable records of reality, giving ownership and control of records, enabling instant transfer of service charges, as well as the incompatibility of computational complexity and thus energy expenditure, and Bitcoin's dependence on ransom software and illegal substance exchange has the disadvantages of having a bad image nowadays [12]. The blockchain systems, which are special to reduce costs, and which are subject to a permit, are considered as alternatives to open systems [13].

Another disadvantage is that there is no strong, reference platform that everyone accepts. Platform differences we rank as the biggest obstacle to the effective sharing of electronic patient data can also affect Blockchain applications. This is now considered to be one of the most fundamental problems in the financial sector, which investigated the application of Blockchain before the health sector [14]. IBM Hyperledger Fabric, J.P. Morgan Quorum, R3 consortium Corda, and so on.

On the other hand, both the advantages and disadvantages can be considered a point of a very current topic Chain Block, and many people with this issue in different countries including Turkey (although currently only limited crypto money) is not relevant. This will help to find the financial support to be worked on in this regard and to increase the potential for access to future Blockchain-based products. On the other hand, Blockchain technology may be at the "hype" point of development and may lead to disappointments due to the expectation that all problems of the existing systems will allow quick resolution.

We're talking about the health of the application, retention of electronic patient records and effect payment of insurance premiums that may seem to be two major applications. If access to image-based data is available in electronic patient records, unnecessary imaging can be reduced to save money and avoid unnecessary radiation to the patient.

VI. ACKNOWLEDGMENT

It is a privilege for us for being associated with Prof. Archana Arudkar, our guide, for this project work. We have been greatly benefited by her valuable suggestions and ideas. It is a great pleasure to express our gratitude to her for her valuable guidance, constant encouragement and patience. We express our gratitude to Principal Dr. Madhumita Chatterjee, Dean Dr. Shrikant Charhate and Dr. Ashok Kanthe, Head, Department of Computer Engineering for their constant encouragement, co-operation, and support. We wish to express our warm and sincere thanks to our project coordinator Prof. Srijita Bhattacharjee for her continuous support and feedback to improve our academic performance.

REFERENCES

[1] K Schwab, A Marcus, JO Oyola, W Hoffman, and M Luzi. Personal data: The emergence of a new asset class. In An Initiative of the World Economic Forum, 2011.
[2] James Ball. Nsa's prism surveillance program: how it works and what it can do. The Guardian, 2013.
[3] Vindu Goel. Facebook tinkers with users' emotions in news feed experiment, stirring outcry. The New York Times, 2014.
[4] ScienceDaily. Big data, for better or worse: 90% of world's data generated over last two years. 2013.
[5] Scaling the facebook data warehouse to 300 pb, 2014.
[6] Michael Lesk. How much information is there in the world?
[7] Google's See what was trending in 2017 – Global.
[8] X-Road - interoperability services, e-estonia. Feb 15, 2018.
[9] A. Buldas, A. Kroonma, R. Laanoja, Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees, Secure IT Systems, NordSec, 2013.
[10] Apple to launch Health Records app with HL7's FHIR specifications at 12 hospitals. Jan 24, 2018.
[11] Dubai Health authority to have unified immunization records. Jan 31, 2018.
[12] M.B. Hoy, An Introduction to the Blockchain and Its Implications for Libraries and Medicine, Medical Reference Services Quarterly, vol. 36, no 3, Jul-Sep 2017, p 273-279
[13] P. Taylor, Applying blockchain technology to medicine traceability. Feb 1, 2018.
[14] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst. 2016;40(10):218.