A Secure Medical Data Sharing Using Block Chain Techniques In Cloud

Mr.J.Noorul Ameen[1], Ms.K.Vinothini[2], Ms.B.Abarnadevi [3]
Department of Computer Science And Engineering
[1] Assistant Professor, .G.S.Pillay Engineering College, Nagapattinam, Tamilnadu, India.
[2,3] E.G.S.Pillay Engineering College, Nagapattinam, Tamilnadu, India.

Abstract- *Block chain technology has gained considerable attention, with an escalating interest in a ranging from data management to healthcare research. Healthcare is a data-intensive clinical domain where a huge amount of data are generated, accessed, and disseminated on a regular basis. Storing and disseminating this large amount of data is crucial, as well as significantly challenging, due to the sensitive nature of data and limiting factors, such as security and privacy. In the healthcare field and clinical settings, safe, secure, and scalable (SSS) data sharing is highly imperative for diagnosis, as well as in combined clinical decision making. The data-sharing practice is quite essential to enable clinical practitioners to transfer the clinical data of their patients to the concerned authority for a quick follow-up. Theses caregivers and general practitioners should be able to transfer the clinical data of their patients in a vastly privacy-sensitive and timely manner, to ensure that both parties have complete and up-to-date information about patient health conditions. Furthermore, there are various interoperability challenges that are faced continuously in this domain. For instance, the safe, secure, and successful exchange of clinical data between healthcare organizations or research institutions can pose severe challenges in practical operation. Block chain technology offers many advantages for health care IT. These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more block chain users.*

Keywords- Block chain,Healthcare,Security

I. INTRODUCTION

Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.

It is clear that technology can play a significant role in enhancing the quality of care for patients (e.g. leveraging data analytics to make informed medical decisions) and potentially reduce costs by more efficiently allocating resources in terms of personnel, equipment, etc. For example, data. captured in form is hard to capture in systems (e.g. costly and data entry errors), costly to archive, and being available when needed. These challenges may lead to medical decisions not made with complete information, the need for repeated tests due to missing information or data being stored in a different hospital at a different state or country (at the expenses of increasing costs and inconvenience for the patients), etc. Due to the nature of the industry, ensuring the security, privacy, and integrity of healthcare data is important. This highlights the need for a sound and secure data management system. Theses caregivers and general practitioners should be able to transfer the clinical data of their patients in a vastly privacy-sensitive and timely manner, to ensure that both parties have complete and up-to-date information about patient health conditions.

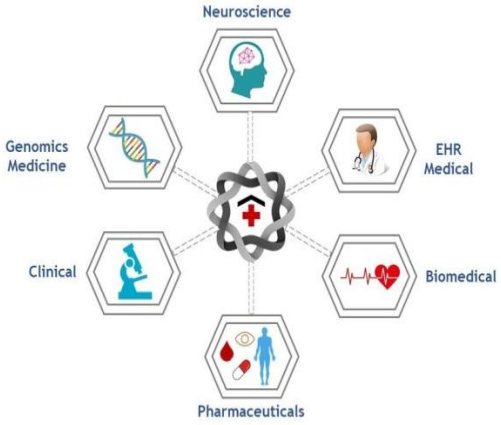

Figure 1.1 Block Chain Architecture

1.1 TRUST IN CLOUD COMPUTING

In cloud, trust is generally related to "levels of confidence in something or someone". Hence can view trust in the cloud as the customers' level of confidence in using the cloud, and try to increase this by mitigating technical and psychological barriers to using cloud services. For more analysis of the definitions of trust in cloud computing. A. Components of Trust in Cloud Computing To best mitigate barriers to confidence, need to understand the main components affecting cloud trust:

1) Security - Mechanisms (e.g. encryption) which make it extremely difficult or uneconomical for an unauthorized person to access some information.
2) Privacy - Protection against the exposure or leakage of personal or confidential data (e.g. personally identifiable information (PII).
3) Accountability - Defined in as "the obligation and/ or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations", accountability goes beyond responsibility by obligating an organization to be answerable for its actions.
4) Audit ability – The relative ease of auditing a system or an environment. Poor audit ability means that the system has poorly-maintained (or non existent) records and systems that enable efficient auditing of processes within the cloud. Audit ability is also an enabler of (retrospective) accountability: It allows an action to be reviewed against a pre determined policy to decide if the action was compliant and if it was not, to hold accountable the person or organization responsible for the action.

1.2 RELATED WORK

Similarly, Ivan demonstrated an approach towards secure health data storage by implementing a public block chain (a decentralized database system with open access control to anyone connected to the network) for encryption. In this method, the encrypted healthcare data is stored publicly, developing a block chain based personal health record (PHR). Their proposed method enabled patients to have better access of their clinical data, where they can freely not only access and monitor their data, but also contribute to their record and share with any associated caregiving agency.

In another study, Chen et al. proposed an integrated block chain and cloud storage based framework, to manage and share patient's personal medical data. The proposed scheme could be used to achieve the safe and secure storage and exchange of personal patient medical data. The suggested approach is unique in its nature, as it gives patients complete access to and control over their personal medical data, thus excluding the involvement of any external third party.

Recently, Wang et al. proposed a framework, based on parallel execution and artificial healthcare systems, to evaluate the healthcare status of patient diseases. The proposed method assesses the overall condition, diagnosis, and treatment process of the patient, and analyzes the associated therapeutic procedures through parallel executions and computational trials for clinical decision making. The suggested system has been tested on real, as well as artificial, healthcare systems, to evaluate the accuracy of diagnosis and effectiveness of treatment.

II. PROPOSED SYSTEM

A shared distributed infrastructure that provides a comprehensive view of an individual's health data across a lifetime is an equally essential component of interoperable health IT systems. Utilization of the proposed health block chain described in this concept has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection.A health care block chain would likely promote the development of a new breed of "smart" applications for health providers that would mine the latest medical research and develop personalized treatment paths. One huge application of block chains in medical industry includes medicinal drug supply chain management. Supply management is a crucial issue to safeguard in all sectors, but it has a greater importance in healthcare, due to its increasing complexity. This is because any compromise to the healthcare supply chain effects the wellbeing of a patient. Block chains provide a safe and secure platform to eliminate this problem and, in some cases, prevent fraud occurrence as well, by introducing higher data transparency and improved product traceability. Since a record in block chain can only be validated and updated through a smart contract, manipulating the block chain isn't easy.

Healthcare data contain personal and sensitive information that may be attractive to cybercriminals.

For example, cybercriminals seeking to benefit financially from the theft of such data may sell the data to a third-party provider, who may perform data analysis to identify individuals who may be uninsurable due to their medical history or genetic disorder. Such data would be of interest to certain organizations or industries.

A block chain approach are as follows:

1. Agreement can be reached without the involvement of a trusted mediator; thus, avoiding a performance bottleneck and a single point of failure;
2. Patients have control over their data;
3. Medical history as a block chain data is complete, consistent, timely, accurate, and easily distributed; and
4. Changes to the block chain are visible to all members of the patient network, and all data insertions are immutable. Also, any unauthorized modifications can be trivially detected.

III. BLOCKCHAIN'S ROLE IN PATIENT DRIVEN INTEROPERABILITY

At a high level, block chain technology can be thought of as a platform for digital exchange, where the platform functions without a traditional intermediary. Health data can live in multiple systems and sharing data requires numerous points of collaboration between entities. As interoperability becomes more patient-centric, there is an opportunity to leverage block chain technology to facilitate this exchange and give patients greater control over their data. Block chains enable a centralized and shared mechanism for the management of authentication and authorization rules surrounding data. For example, a block chain may have "Smart Properties" an entity whose ownership is managed through a block chain to allow some form of digital property to have clean ownership. The custodian of the data (for example, the patient), is clearly represented on the block chain, and can subsequently assign access rules and permissions around their data, enabling easier sharing. A second way block chain technology could foster patient-driven interoperability is through data availability. As patients move to take more ownership of their health data, one of their first tasks will be to gather all of their clinical data together, for example, by establishing an API connection to every system that has data would like to use. Once a patient has established these connections, can then collect and aggregate their health data as appropriate. Such a task might be cumbersome if the patient had to manage this on their own. Yet a block chain platform could facilitate this particularly if done in conjunction with block chain enabled digital access rules.

IV. METHODOLOGY

Step 1 : Transaction data

A block chain that stores transaction data.

Step 2 : Chaining the blocks (with a hash) .A bunch of blocks of transaction data. These blocks are now being linked (aka chained) together. To do this, every block gets a unique (digital) signature that corresponds to exactly the string of data in that block.

Step 3 : The signature (hash) is created.

In block chain, this signature is created by a cryptographic hash function. A cryptographic hash function is a very complicated formula that takes any string of input and turns it into a unique digit string of output.

Step 4 : The signature qualify, and who signs a block

A signature doesn't always qualify. A block will only be accepted on the block chain if its digital signature starts with a consecutive number of zeroes.

Step 5 : To make the block chain immutable a block will unchain it from the subsequent blocks. In order for an altered block to be accepted by the rest of the network, it needs to be chained to the subsequent blocks again.

Step 6 : Determines the rules.

The block chain protocol does this automatically by always following the record of the longest block chain that it has, because it assumes that this chain is represented by the majority.

Step 7 : Crypto currencies(Verification)

Most crypto currencies are built upon their own block chain protocol that may have different rules from the Bit coin block chain. Block chains also have the potential to safely register data in the form of medical records, identities, history records, tax records and much, much more.

V. CONCLUSION

The healthcare record, storage and sharing of this data would lay a scientific foundation for the advancement of medical research and precision medicine, help identify and develop new ways to treat and prevent disease and test whether or not mobile devices engage individuals more in their health care for improved health and disease prevention. Block chain technology definitely has a place in the health IT ecosystem, should strongly consider basing their interoperability strategy on block chain and using block chain to promote the advancement of precision medicine. In future work the question remains, however, as to just how safe personal brain data would remain on a block chain. The decentralized and transparent nature of block chains would certainly prevent data from being altered or stolen, but many of the general concerns regarding large scale data collection still apply: That sensitive data might end up being sold to third parties for questionable marketing purposes, and that users might still be indirectly identifiable (as they are with bit coin) via pseudonymous identifiers or patterns of data. Consequently, this block chain based healthcare framework will engage individuals more in their healthcare, which will ultimately improve the quality of life in a more befitting manner.

FUTURE WORK

Personal data as personal data, it may not be very long that hashes of personal data are considered as personal

data; then the whole debate of whether block chain is fit to store personal data may start all over again. Block chain specific infrastructure, vehicular cloud advertisement dissemination, and Skyline query processing, which should be further investigated in the near future.

REFERENCES

[1] Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Block chain Based Medical Records Secure Storage and Medical Service Framework. J. Med. Syst. 2018, 43.

[2] M. Ciampi et al., "A Federated Interoperability Architecture for Health Information Systems," Int'l Journal of Internet Protocol Technology, vol. 7, no. 4, 2013, pp. 189.

[3] S.H. Han et al., "Implementation of Medical Information Exchange System Based on EHR Standard," Healthcare Informatics Research, vol. 16, no. 4, 2010, pp. 281–289.

[4] D. He et al., "A Provably Secure Cross Domain Handshake Scheme with Symptoms Matching for Mobile Healthcare Social Network," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, 2016; doi.org/DOI: 10.1109/TDSC.2016.2596286.

[5] Ivan, D. Moving toward a block chain based method for the secure storage of patient records. In ONC/NIST Use of Block chain for Healthcare and Research Workshop; ONC/NIST: Gaithersburg, MD, USA, 2016.

[6] F.Y. Leu et al., "A Smartphone Based Wearable Sensors for Monitoring Real Time Physiological Data," Computers and Electrical Engineering, 2017.

[7] M. Memon et al., "Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes," Sensors, vol. 14, no. 3, 2014, pp. 4312–4341.

[8] M. Moharra et al., "Implementation of a Cross-Border Health Service: Physician and Pharmacists' Opinions from the epSOS Project," Family Practice, vol. 32, no. 5, 2015,pp. 564–567

[9] P.C. Tang et al., "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption," Journal of the American Medical Informatics Assoc., vol. 13, no. 2, 2006, pp. 121–126.

[10] Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.Y. Block chain Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Trans. Comput. Soc. Syst. 2018, 99, 1–9.