Article

Blockchain service model of personal health information system issues and open challenges.

Mohammad Pourshafiei, Zuriati Ahmad Zukarnain

Faculty of Computer Science and Information Technology, University Putra Malaysia, Serdang 43400, Selangor, Malaysia; GS56128@student.upm.edu.my (M.P)
*Correspondence: GS56128@student.upm.edu.my (M.P.); zuriati@upm.edu.my (Z.A.Z.);

Abstract: One of the special trends in health care is the increasing availability of data and services to the cloud, especially for convenience (for example, providing a complete patient medical record without interruption) and savings (for example, economic issues). Management of health care data). However, there are limitations to using common cryptographic prototypes and access control models to address security and privacy concerns in an increasingly cloudy environment. In this paper, we explore the potential and capacity of using China's Blockchain technology to protect health care data hosted in the cloud. We also explain the real challenges of such an approach and further research is needed. Health care is a highly data-dependent domain, with large amounts of data being created, published, stored and accessed daily. For example, data are created when a patient undergoes a number of examinations (such as computed tomography or computed tomography scans) and the data need to be sent to the radiologist and then to a physician. The visit results are then stored in the hospital, and then need to be accessed later by another physician at another hospital within the network. It is clear that technology can play an important role in improving the quality of care for patients (for example, using data analytics to make informed medical decisions) and potentially costing more by allocating resources more efficiently in terms of personnel, equipment, etc. , Reduce. For example, paper-based data extraction is difficult to extract into systems (for example, it is costly and may involve data entry errors), archiving them and accessing them as needed is costly. These challenges may cause medical decisions to be incomplete, requiring repeated tests for missing information or missing data stored in another hospital in another state or country (at the expense of increased costs and no convenience). (For patients) and so on. Because of the nature of the industry, it is important to ensure the security, privacy and integrity of health care data. As a result, there is definitely a need for a secure and secure data management system.

Keywords: health care, Hospital;Blockchain technology; security and privacy;

Introduction

Health care is a highly data-dependent domain, with large amounts of data being created, published, stored and accessed daily. For example, data are created when a patient undergoes a number of examinations (such as computed tomography or computed tomography scans) and the data needs to be sent to the radiologist and then to a physician. The visit results are then stored in the hospital, and then need to be accessed later by another physician at another hospital within the network.

It is clear that technology can play an important role in improving the quality of care for patients (for example, using data analytics to make informed medical decisions) and potentially costing more by allocating resources more efficiently in terms of personnel, equipment, etc. , Reduce. For example, paper-based data extraction is difficult to extract into systems (for example, it is costly and may involve data entry errors), archiving them and accessing them as needed is costly. These challenges may cause medical decisions to be incomplete, requiring repeated tests for missing information or missing data stored in another hospital in another state or country (at the expense of increased costs and no convenience). (For patients) and so on. Because of the nature of the industry, it is important to ensure the security, privacy, and integrity of health care data. As a result, there is definitely a need for a secure and secure data management system.

Electronic Medical Records and Health Information Systems

With medical and clinical data relevant to a specific patient and EMRs stored by the responsible medical care provider. And data analysis on data systems "facilitates early generation of health EMRs. To better help, store new EMRs and consult them and retrieve EMRs with the ability to create HIS samples" With a data base in the front end of the user interface, relatively simple solutions can be configured as a control interface. Graphics or a web service are usually represented in a centralised or distributed execution.

Electronic Medical Records and Health Information Systems

Containing medical and clinical data related to a particular patient and EMR ("Electronic Medical Records" generally), stored by the responsible health care provider. And data analysis of data systems "facilitates early generations of health EMRs. To better support new EMR management, store them and query and retrieve EMRs with the capability to create HIS samples" They can be relatively simple solutions that are schematically designed as a supervisory interface, with a database at the forefront of the user interface. Graphics or a web service are described, these are generally in centralized or distributed implementation.

Given that patient mobility (both within and outside a given country) is increasingly becoming increasingly commonplace in today's society in order to share care data, it is evident that several health strategies among different providers, Even at national borders if needed, facilitated. For example, in important countries of medical tourism centers, such as Singapore, the need for shared health care data has become more pronounced among different providers and across countries. There are ways to formalize the EMR structure to facilitate data sharing, or even the mobility of patient data (needs), in the form of EHRs ("Electronic Health Records"), for example, their HIS data and designed to allow Move patient records or provide multiple healthcare providers (for example, from a rural hospital to a hospital in a nation's capital, before a patient receives a richer data structure than the EHR seeking care Medicine in another hospital in another country) and there are infrastructures capable of scaling HISs as well as initiatives. Develop EMRs and support future needs, as well as through various national and international initiatives such as the project

In Europe and an ongoing project for epSOS in Italy, the FSE project Fasciocolo Sanitario Altronico ("EH standardization of subscriptions, we saw. R and wearable devices"). Such devices can be user-owned or installed by the health care organization to measure the health of users (for example, patients) and inform medical treatment and patient monitoring. For example, a wide range of mobile apps (ups) in the health categories, There are physical fitness, weight loss, and other healthcare-related categories, which are mainly

used as a tracking tool, such as recording workout/workout plans, maintaining calorie intake and other statistics (for, For example, the number of steps taken) and so on.

There are also devices equipped with sensors for advanced medical tasks, such as heart rate bracelets during exercise, or glucose (glucose) self-monitoring devices. For example, Liu et al. proposed a smartphone-based wireless body sensor network to collect user physiology data using body sensors embedded in a smart device. These data (user vital signs) can be collected continuously and transmitted seamlessly to a smart device, before being sent to the cloud of life-support environments with the help of "remote health care" for further analysis. Another example is health care, designed to enable remote health services and remote physicians to provide remote monitoring of personal health.), Where patients compile PHR ("personal health records"). These improvements pave the way for their data, monitoring of their health conditions, etc. using smartphones or wearable devices (e.g., smart clothing). And smart socks) are involved, for example, can we rely on data collected by PHR but some of the challenges associated with patients themselves? Do related health care providers require data from patients? And if so, how can this be done? Who should be legally responsible for the wrong diagnosis?

Or is it a late diagnosis known to make a decision based on data sent from a patient's device that was later found to be defective or inaccurate (for example, due to sensor failure)? Based on the ecosystem of HIS solutions, despite such really challenging and challenging legal issues, having one that can seamlessly exchange data between themselves and provide individual health data storage concepts for each specific patient (for example, physically distributed across multiple instances). Integrated software across multiple health care organizations and mobile upgrades benefit all users, from patients to health care to governments. Cloud computing is a potential solution to support seamless geographic location data sharing (for example, hosting their big data, to provide resource flexibility, if needed, and big data (analytics tools) Big data) to gain insights and insights from analyzing big health care data for policy research and decision making.

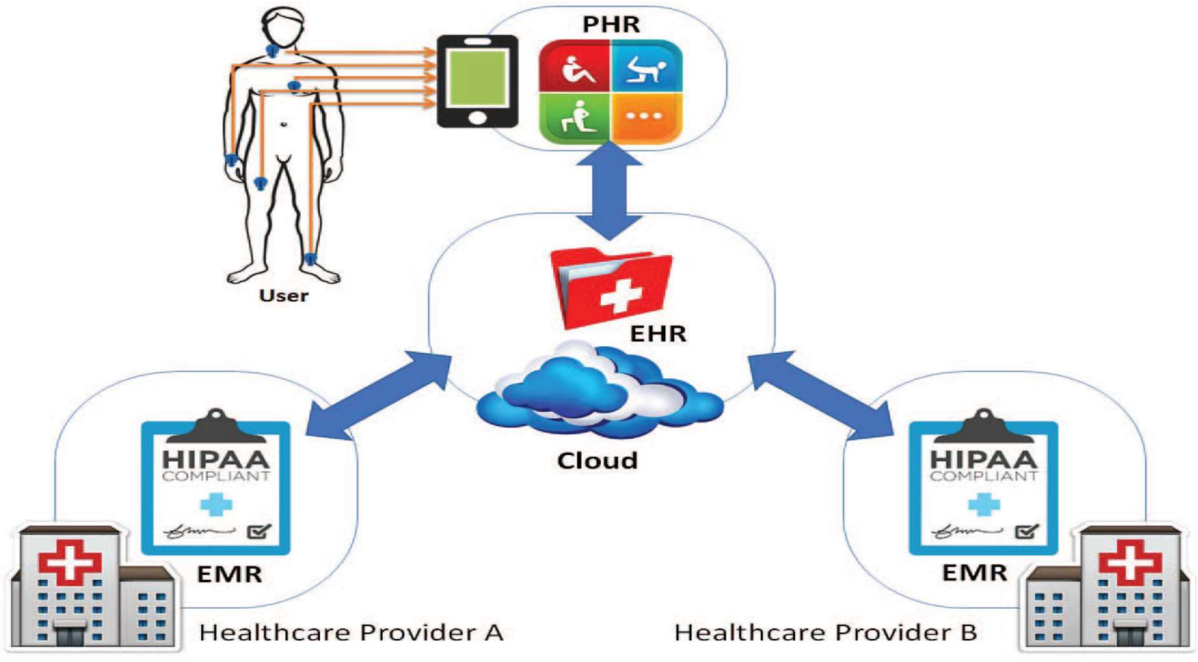

Figure 1. How clouds facilitate the sharing

Information on health care provides confidential and sensitive information that can be very enticing to cybercriminals. Cybercriminals trying to misuse such information, for example, could sell the information to a rival provider to conduct data analysis and identify people who may be uninsured due to medical history or genetic condition. Such information appeals to particular organisations or industries. Therefore, because of the interaction between systems and components, maintaining the protection of the EMR / HER / PHR ecosystem and the systems and their constituent components that make up the ecosystem is important and often difficult. In addition, health care data privacy and integrity are secured not only against external attackers but also against unauthorised network or ecosystem access attempts (for example, health care providers or cloud providers). Such attacks can be deliberate and accidental (for example, data loss or correction) and companies may be disciplined or penalised for such accidents, for example under the Health Insurance Displacement and Liability Act, to be blamed. An active area of research is how to protect the EMR / HER / PHR environment and ensure data protection and data integrity.

To ensure data protection and privacy, approaches include the use of cryptographic basics, such as public-key infrastructure and public clouds. For instance, prior to being outsourced to the cloud, data is encrypted. This, however, restricts the data's search power, since healthcare providers have to decipher (potentially large) data before the decoded data can be searched and decoded. Data processing and detection (for example, copying, encoding, and search) takes time and resources. Based on established policies, access control models are often used to track and limit access to data. For external attacks, such models may be very successful, but they usually do not work as well for internal attacks because someone can lose data access. Approaches to combine access control with a variety of basic cryptographic concepts, such as cryptography based on attributes, are also accessible.

Blockchain to the rescue

There has been a renewed interest in the provision of protected health care data storage using Blockchain. More broadly, blockchain is a technology that can construct a free and distributed online database that contains a list of connected (i.e. block to block) data structures (also known as blocks). The next one, and so the name of the block (blockchain) appears. These blocks are distributed between different infrastructure nodes and are not stored centrally. From the time of creation, each block has its own timestamp, previous block hash and exchange data, and patient health care data and health care provider information in our context. This illustrates the principle of a blockchain. Specifically, a block is generated between all peers as an EMR / HER / PHR, 2-form ecosystem is generated as new health care data is created for a specific patient (for example, from a consulting and medical centre such as surgery).

Distributed to a network of patients. The system will position it in the chain after the majority of peers have accepted the new block. This helps us to reliably, consistently and consistently obtain a global view of the patient's medical history. If no agreement between the different nodes is reached, a branch in the chain is formed and the block is identified as missing and will not belong to the main chain. After the block is inserted into the chain, without changing all subsequent blocks, the data for each block cannot be changed. Reform or shift, in other words, is easily observable. Since block information is publicly accessible, it is important to secure healthcare data (e.g. blurred, or clearly encrypted) before the data is put on the block.

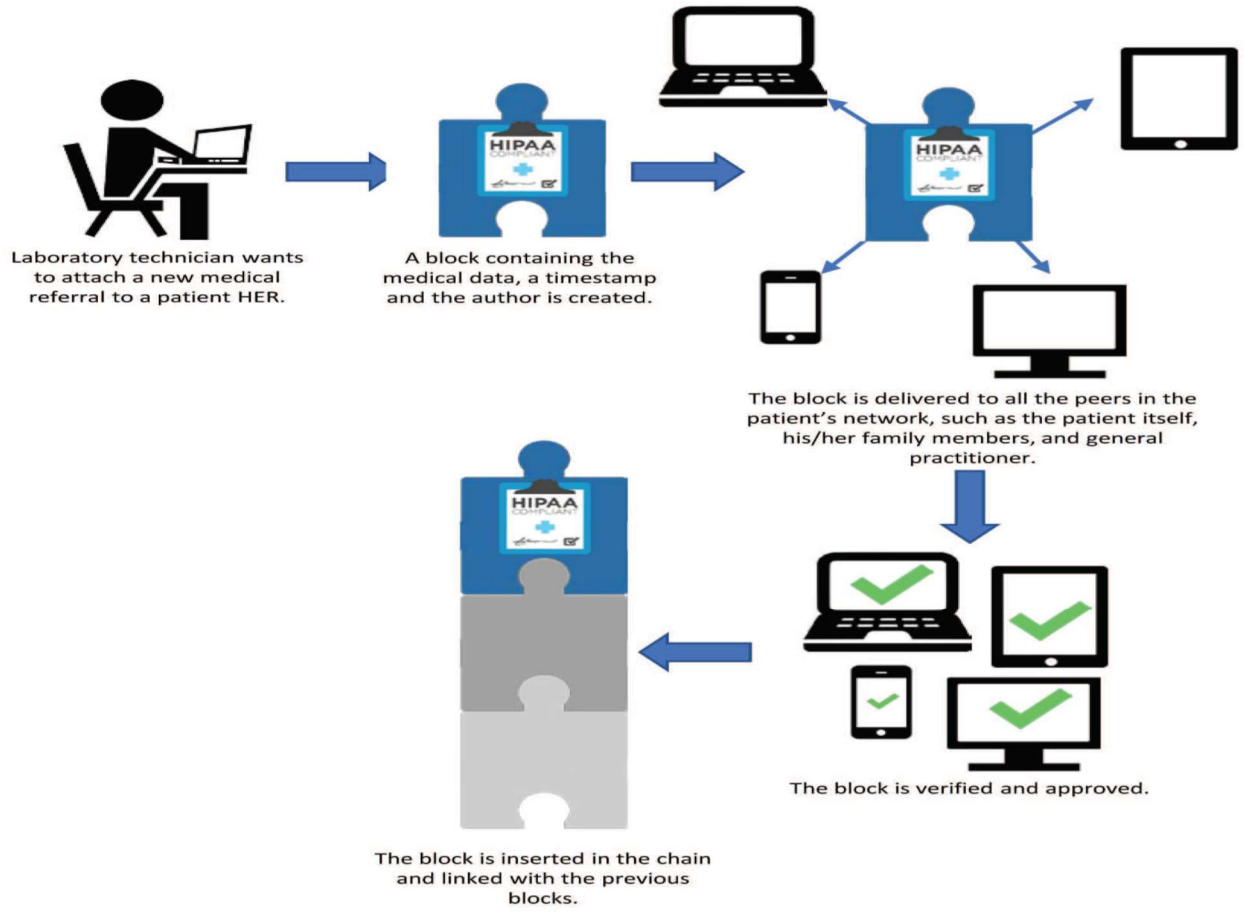

Figure 2. How to attach a new medical referral

Conceptually, Blockchain is a design-safe because it provides the ability to achieve decentralized consensus and coordination and agility against deliberate or unintentional attacks. The key advantages of applying a Blockchain to our subject area:

1. Without the involvement of a trusted mediator, consensus can be achieved; thus avoiding a performance bottleneck and a specific failure point. Patients have control over their data.

2. Medical records in the form of Blockchain data are complete, concise, timely, accurate and easily distributable;

3. Blockchain changes are visible to all members of the patient network and all data entry is non-confidential. Also, any unauthorized manipulation can be easily detected.

As with any safety solution, there are limitations associated with a blockchain-based approach that needs to be carefully studied. For example, blockchain technology can be a bit disruptive and require substantial rethinking and significant investment in the entire ecosystem (for example, replacing existing systems and redesigning business processes). In other words, before taking action, health care providers, especially government-covered providers, need to perform a loss-benefit analysis to understand investment returns and any potential implications (for example, legal and financial). For example, the same records can remain in several nodes in the network, located in different countries that have different privacy and data protection requirements (for example, the European Union and the US).

Restrictions

This analysis did not concentrate on the usage of blockchain outside patient care in the health sector, such as the health insurance marketplace, the supply chain of the pharmaceutical industry, or the credentialing phase of the health care provider in which blockchain is proposed to reinvent these industries The COVID-19 pandemic has revealed many high-value use cases where blockchain-enabled technology could address evolving societal needs and facilitate rapid responses to disruptions, such as supply chain management to connect health care organisations to reliable sources for required medical supplies, monitoring and tracking the origin and journey of drugs from pharmacy to patient administration, and As part of the pandemic response, a further the study might examine blockchain research in these areas.

Challenges

While data integration and distributed storage/access to blockchain provide opportunities to manage health care data, these features also present challenges that require further study.The integrity feature of robust blockchain data makes it invisible so that no data can be modified or deleted after being stored in the blockchain. However, if that record is health care data, then such personal data will be protected by privacy laws, many of which do not allow personal data to be held public - Article 17 of the Privacy Act. Public data »Implemented soon in the EU, has strengthened the rights of individuals to request the removal of personal data. After the organization's principles of economic development and cooperation are the privacy guidelines that underpin many data protection laws, it provides individuals with the right to clean up. Given the sensitivity of health care data, anyone who uses blockchain to store it cannot ignore the legal requirement to erase personal data.

Another practical issue is how to tailor it to blockchain to store health care data. Blockchain was originally designed to record transaction data, which is relatively small in size and linear. In other words, one of its only concerns is whether the current transaction can be routed back to the original "ideal". Health care data, such as imaging and treatment plans, can be large and proportionate that need to be searched. The extent and quality of blockchain's ability to cope with both requirements are currently unclear.

To address these challenges, many have referred to the concept of caching outside the data chain, in which case data is stored outside the blockchain in a common or distributed database, but in data synchronization. They are stored in a blockchain. This is said to be the best of both cases, as health care data is stored off-chain and can be cleaned, immunized, modified and cleared if appropriate. At the same time, non-preventable hassle-free health care data is stored on the chain to verify the authenticity and accuracy of medical records from the chain.

But, the idea is not always without potential challenges. With the enforcement of data protection laws around the world tightening and stricter efforts by the High Commissioner for Privacy to consider personal metadata as personal data, it may not be too late in integrating personal data into Consider the title of personal data; therefore, the whole debate over whether blockchain is suitable for storing personal data may resume from scratch.

Conclusions

Blockchain solutions, while innovative, rely on traditional technologies for back-end processes like authentication and data processing. In essence, the blockchain infrastructure is much like an armadillo, with a hard shell on the outside, but soft and vulnerable on the inside—especially on commodity hardware. The

blockchain may be secure, but if attackers can find a way in, for example through poor access controls, the whole infrastructure may be vulnerable. These components include everything from the network IP address, the blockchain layer, back-end components such as databases and object stores, the APIs, the externally-facing IP addresses, and the mobile applications associated with the network.

Access control is critical to blockchain security, and often permissions and access controls are implemented at the application level but not at the blockchain layer. If hackers compromise any application and access internal networks, they could hit any number of APIs associated with the blockchain. With no access controls, a malicious actor could literally do anything and everything they wanted on the chain itself.

It is without question that blockchain provides the enterprise with almost endless opportunities for innovation. However, the challenges of exponential data make it complex to identify clearly those opportunities with the required certainty that the data can be trusted. Blockchain will be foundational in helping companies build the stable, resilient, and highly available systems of record. Additionally, blockchain, when built on the right architecture, can enable the scale required to not only meet current, but future demands for growth while maintaining the integrity, trust, and privacy that has become the bedrock of its existence.

Author Contributions: Investigation, M.P.; Methodology, Z.A.Z.; Supervision, Z.A.Z.; Validation, Z.A.Z, Writing—original draft, M.P.; Writing—review & editing, Z.A.Z;,M.P. authors have read and agreed to the published version of the manuscript.

Funding: This research is sponsored by University Putra Malaysia.

References

1. M. Steward, “Electronic Medical Records,” Journal of Legal Medicine, vol. 26, no. 4, 2005, pp. 491–506.
2. R. Hauxe, “Health Information Systems—Past, Present, Future,” Int'l Journal of Medical Informatics, vol. 75, no. 3–4, 2006, pp. 268–281.
3. K. Häyrinena et al., “Definition, Structure, Content, Use and Impacts of Electronic Health Records: A Review of the Research Literature,” Int'l Journal of Medical Informatics, vol. 77, no. 5, 2008, pp. 291–304.
4. 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– 202.
5. 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.
6. 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.
7. D. He et al., “A Provably-Secure Cross-Domain Handshake Scheme with SymptomsMatching 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.
8. F.Y. Leu et al., “A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data,” Computers and Electrical Engineering, 2017.
9. M. Memon et al., “Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes,” Sensors, vol. 14, no. 3, 2014, pp. 4312–4341.

10. 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.
11. S. Marceglia et al., "A Standards-Based Architecture Proposal for Integrating Patient mHealth Apps to Electronic Health Record Systems," Applied Clinical Informatics, vol. 6, no. 3, 2015, pp. 488–505. 36January/February 2018
12. A. Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services," Journal of Medical Internet Research, vol. 13, no. 3, 2011.
13. V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities," IEEE Cloud Computing, vol. 3, no. 6, 2016, pp. 10–14.
14. S. Nepal et al., "Trustworthy Processing of Healthcare Big Data in Hybrid Clouds," IEEE Cloud Computing, vol. 2, no. 2, 2015, pp. 78–84.
15. G.S. Poh et al., "Searchable Symmetric Encryption: Designs and Challenges," ACM Computing Surveys, vol. 50, no. 3, 2017.
16. Q. Alam et al., "A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, 2017, pp. 1259–1268.
17. M. Li et al., "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 8, no. 3, 2016, pp. 2084–2123.
18. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, 2016, pp. 2084–2123.
19. A. Azaria et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management," Proceedings of the 2nd Int'l Conference on Open and Big Data (OBD 16), 2016, pp. 25–30.
20. J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social NetworkBased Healthcare," IEEE Access, vol. 4, 2016, pp. 9239–9250.