HEALTHCARE CLOUD-BASED DATA SECURITY AND PRIVACY *USING: BLOCKCHAIN*

1 MOHIL DWIVEDI
M-Tech Student
Department of computer science & Engg
Buit Bhopal

2 ROHIT GUPTA
M-Tech Student
Department of computer science & Engg
Buit Bhopal

3 DR DIVAKAR SINGH
Head of the departament
Department of computer science & Engg
Buit Bhopal

4. DR ANJU SINGH
Assistant Professor
Department of computer science & Engg
Buit Bhopal

ABSTRACT

One explicit trend determined in tending is that the progressive shift of information and services to the cloud, partially thanks to convenience (e.g. accessibility of complete patient case history in real-time) and savings (e.g. political economy of tending knowledge management). There are, however, limitations to mistreatment typical cryptologic primitives Associate in Nursingd access management models to handle security and privacy issues in an progressively cloud-based surroundings. during this paper, we have a tendency to study the potential to use the Blockchain technology to safeguard tending knowledge hosted among the cloud. we have a tendency to conjointly describe the sensible challenges of such a proposition and any analysis that's needed.

Healthcare could be a data-intensive domain wherever an oversized quantity of information is formed, disseminated, stored, and accessed daily. as an example, knowledge is formed once a patient undergoes some tests (e.g. computerized axial tomography or processed axial tomography scans), and also the knowledge can must be disseminated to the medical specialist so a doc. The results of the visit can then be keep at the hospital, which can must be accessed at a later time by a doc in another hospital among the network.

It is clear that technology will play a major role in enhancing the standard of look after patients (e.g. leverage knowledge analytics to create knowing medical decisions) and doubtless cut back prices by additional expeditiously allocating resources in terms of personnel, equipment, etc. as an example, knowledge captured in paper type is difficult to capture in systems (e.g. expensive

and knowledge entry errors), expensive to archive, and being accessible once required. These challenges could cause medical selections not created with complete info, the requirement for continual tests thanks to missing info or knowledge being keep during a different hospital at a unique state or country (at the expenses of accelerating prices and inconvenience for the patients), etc. thanks to the character of the trade, making certain the se- curity, privacy, and integrity of tending knowledge is very important. This highlights the requirement for a sound and secure knowledge management system.

I - HEALTH RECORDS IN ELECTRONIC FORMS AND HEALTH INFO SYSTEMS

Generally, Electronic Medical Records (EMRs) contain medical and clinical knowledge associated with a given patient and keep by the accountable tending supplier.1 This facilitates the retrieval and analysis of tending knowledge. to raised support the management of EMRs, early generations of Health info Systems (HIS) are designed with the potential to form new EMR instances, store them, and question and retrieve keep EMRs of interest.2 HIS are often comparatively easy solutions, which might be schematically delineated as a graphical interface or an online service. These are typically the front-end with a info at the back-end, during a centralized or distributed imple-cerebration.

With patient quality (both internally and outwardly to a given country) being progressively the norm in today's society, it became evident that multiple complete EMR solutions should be created practical to facilitate sharing of tending knowledge among totally different suppliers, even across national borders, as needed. as an example, in medical commercial enterprise hubs like Singapore, the requirement for period tending knowledge sharing between totally different suppliers and across nations becomes additional pronounced.

To facilitate knowledge sharing or perhaps patient data movableness, there's a necessity for EMRs to formalize their organization and also the style of HIS. Electronic Health Records (EHRs), as an example, are designed to permit patient case history to maneuver with the patient or be created accessible to multi- ple tending suppliers (e.g. from a rural hospital to a hospital within the capital town of the country, before the patient seeks medical attention at another hospital during a totally different country).3 EHRs have a richer organization than EMRs. There have conjointly been initiatives to develop HIS and infra- structures that are able to scale and support future wants, as proved by the assorted national and international initiatives project in India, the epSOS project in Europe, Associate in Nursingd an in progress project to standardize sharing of EHRs.4,5,6

Recently, the generality of good devices (e.g. humanoid and iOS devices and wearable de- vices) has conjointly resulted during a paradigm shift among the tending trade.7 Such devices are often user-owned or put in by the tending supplier to live the well-being of the users (e.g. patients) and inform/facilitate medical treatment and watching of patients. as an example, there's a good vary of mobile applications (apps) in health, fitness, weight-loss, and different tending connected classes. These apps primarily perform as a trailing tool, like registering user exercises/workouts, keeping the count of consumed calories, and different statistics (e.g. range of steps taken), and so on.

There also are devices with embedded sensors for additional advanced medical tasks, like brace- lets to live heartbeat throughout workouts, or devices for self-testing of aldohexose. as an example, Leu and collaborators planned a goodphone-based wireless body device network to gather user physiological knowledge mistreatment body sensors embedded during a smart shirt.8 the info (e.g. user's important signs) are often endlessly gathered and sent in period to a wise device, before being sent to a far off tending cloud for any analysis. Another example is close aided Living solu- tions for tending designed to understand innovative telehealth and telemedicine services, so as to produce remote personal health watching.9

These developments have sealed the means for private Health Records (PHR), wherever patients are additional concerned in their knowledge assortment, watching of their health conditions, etc, mistreatment their good phones or wearable devices (e.g. good shirts and smart socks).10,11

There are, however, variety of challenges related to PHRs. as an example, will we have a tendency to depend on the info collected by the patients themselves? ought to the relevanttending suppliers certified data collected by the patients, and if so, however will this be done? United Nations agency ought to be de jure chargeable for a misdiagnosis or delayed identification, thanks to selections being created on the info sent from the patient's device that's later determined to be blemished or inaccurate (e.g. thanks to a malfunction sensor)?

Despite such challenges and doubtless thorny legal problems, having a HIS supported Associate in Nursing scheme of solutions that's able to seamlessly exchange knowledge among themselves and supply the abstraction of one health data storage for any given patient (e.g. physically distributed among multiple concrete software package instances at multiple tending suppliers and mobile apps) can profit all users, starting from patients to tending suppliers to governments.

Cloud computing could be a potential resolution, thanks to the potential to support period knowledge sharing no matter geographical locations, to produce resource snap PRN, and to handle huge knowledge (e.g. hosting of massive knowledge analytical tools) to get helpful

insights from the analysis of big tending data for analysis and policy higher cognitive process.12,13

In Figure one, we have a tendency to demonstrate however cloud facilitate facilitate sharing of tending knowledge among providers, supporting every supplier in managing their knowledge, providing a seamless means of exchanging and doubtless certifying knowledge between EHR and PHR, and providing a unified/comprehensive read of (the scattered) tending records for every patient. In different words, (federated) cloud computing are often accustomed interconnect the various tending suppliers and their PHR solutions, employed by the suppliers to handle any sharp or seasonal changes, and so on.

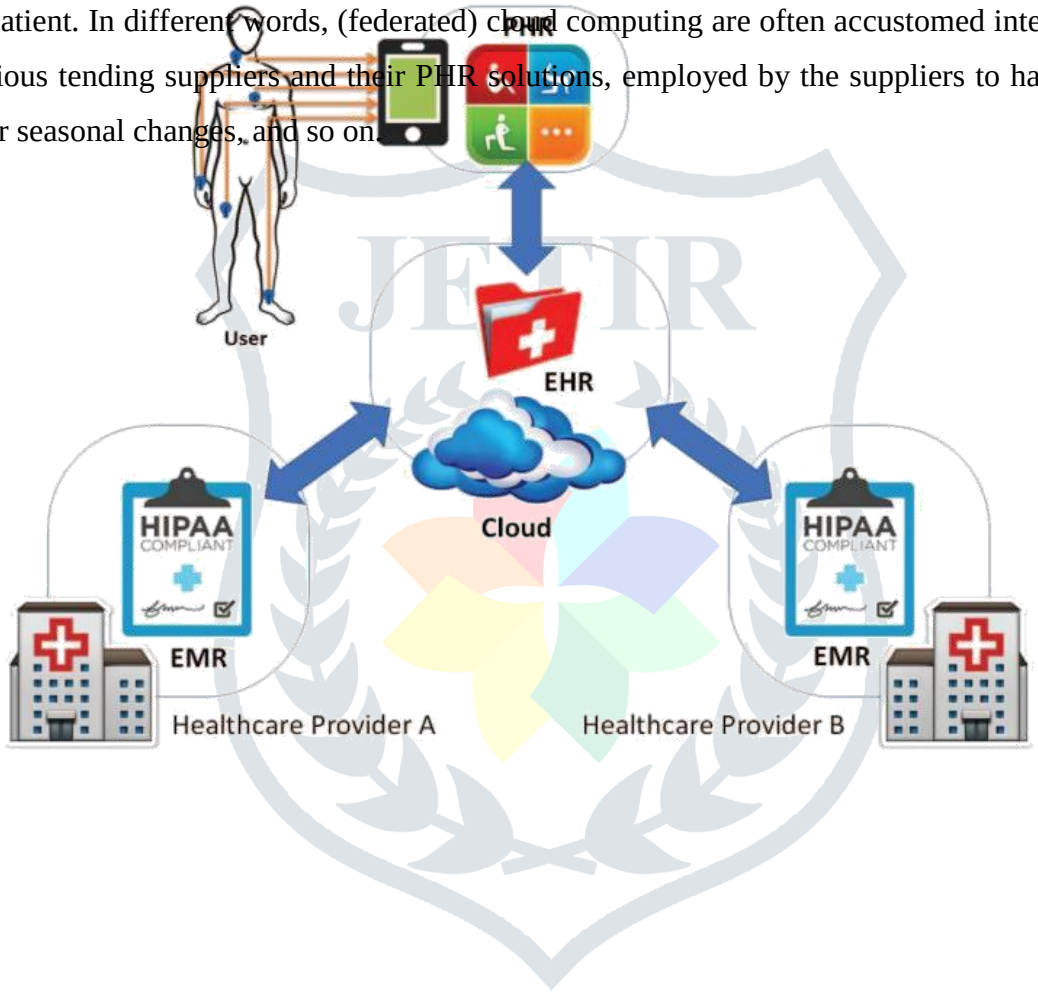

Figure 1. A conceptual cloud-based EMR/EHR/PHR ecosystem.

II- SECURITY AND PRIVACY

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.

Therefore, ensuring the security of the EMR/EHR/PHR ecosystem and the underlying systems and components that form the ecosystem is crucial, yet challenging due to the interplay and complexity between the systems and components. Moreover, the privacy and integrity of healthcare data must be protected not only from external attackers, but also from unauthorized access attempts from inside the network or ecosystem (e.g. employee of the healthcare provider, or cloud service provider). The attacks (e.g. leakage or modification of data) can be intentional and unintentional, and organizations may be penalized or held criminally liable for such incidents, for example under the Health Insurance Portability and Accountability Act.

How to secure EMR/EHR/PHR ecosystem and ensure privacy and integrity of the data is an active research area. Approaches include using cryptographic primitives, such as those based on public key infrastructure and public clouds to ensure data confidentiality and privacy.14 For example, data is encrypted prior to outsourcing to the cloud. However, this limits the searchability of the data, in the sense that healthcare providers have to decrypt the (potentially big) data prior to searching on the decrypted data, resulting in increases in time and costs for the data retrieval and diagnosis (e.g. download, decrypt, and search).15

Access control models have also been used to regulate and limit access to the data, based on predefined access policies.16 Such models can be particularly effective for external attacks, but are generally ineffective against internal attackers as they are likely to be authorized to access the data. There have also been approaches to integrate access control with some cryptographic primitives, such as attribute-based encryption.17

III- BLOCKCHAIN TO THE RESCUE?

There has been recent interest in utilizing blockchain (made popular by the successful Bitcoin) in the provision of secure healthcare data management.18,19,20 Broadly speaking, blockchain is a technology able to build an open and distributed online database, which consists a list of data structures (also known as blocks) that are linked with each other (i.e. a block points to the following one, hence the name blockchain). These blocks are distributed among multiple nodes of an infrastructure, and are not centrally stored. Each block contains a timestamp of its production, the hash of the previous block and the transaction data, and in our context, a patient's healthcare data and the healthcare provider information.

Figure 2 describes our conceptual blockchain-based EMR/EHR/PHR ecosystem. Specifically, when new healthcare data for a particular patient is created (e.g. from a consultation, and medical operation such as a surgery), a new block is instantiated and distributed to all peers in the pa-tient network. After a majority of the peers have approved the new block, the system will insert it

in the chain. This allows us to achieve a global view of the patient's medical history in an efficient, verifiable, and permanent way. If the agreement is not reached, then a fork in the chain is created and the block is defined as an orphan and does not belong to the main chain. Once the block has been inserted into the chain, the data in any given block cannot be modified without modifying all subsequent blocks. In other words, modification can be easily detected. As block content is publicly accessible, healthcare data needs to be protected prior to the data being in the block (e.g. obfuscated and perhaps, encrypted).

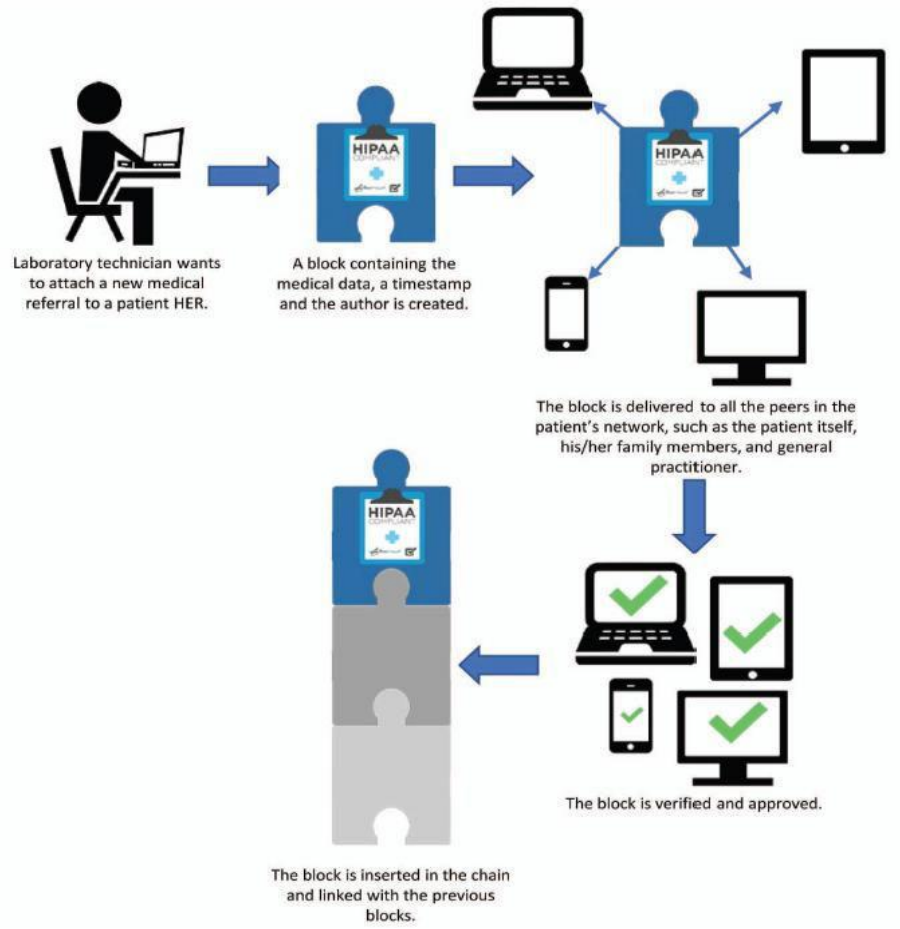

Figure 2. A conceptual blockchain-based EMR/EHR/PHR ecosystem.

Conceptually, blockchain is secure by design that provides the capability to achieve decentralized consensus and consistency, and resilience to intentional and/or unintentional attacks. Key benefits of deploying a blockchain in our approach are as follows:

1. Agreement can be reached without the involvement of a trusted mediator; thus, avoid- ing a performance bottleneck and a single point of failure;

2. Patients have control over their data;

3. Medical history as a blockchain data is complete, consistent, timely, accurate, and eas- ily distributed; and

4. Changes to the blockchain are visible to all members of the patient network, and all

data insertions are immutable. Also, any unauthorized modifications can be trivially detected.

As with any security solutions, there are limitations associated with a blockchain-based approach that need to be carefully studied. For example, blockchain technology can be somewhat disruptive and requires a radical rethink and significant investment in the entire ecosystem (e.g. replacement of existing systems and redesigning of business processes). In other words, before taking the plunge, healthcare providers particularly publicly funded providers will need to undertake a cost benefit analysis to understand the return on investment and any potential implications (e.g. legal and financial). For example, the same record can reside in multiple nodes of the network, located in different countries with different privacy and data protection requirements (e.g. EU and US).

IV -CHALLENGES

While data integrity and distributed storage/access of blockchain offer opportunities for healthcare data management, these same features also pose challenges that need further study.21 The strong data integrity feature of blockchain results in immutability that any data, once stored in blockchain, cannot be altered or deleted. However, if the record is healthcare data, then such personal data would come under the protection of privacy laws, many of them would not allow personal data to be kept perpetually—Article 17 of the soon-enforceable General Data Protection Regulation in the EU has strengthened the rights of individuals to request personal data to be erased. One of the principles of the Organization for Economic Cooperation and Development privacy guideline, on which many data protection laws are based, provides the right-to-erasure to individuals. Given the sensitivity of healthcare data, anyone planning to use blockchain to store them cannot ignore this legal obligation to erase personal data if warranted.

Another practical issue is on how fit it is for blockchain to store healthcare data. Blockchain was originally designed to record transaction data, which is relatively small in size and linear. In other words, one only concerns itself about whether the current transaction can be traced backwards to the original ―deal‖. Healthcare data, such as imaging and treatment plans, however, can be large and relational that requires searching. How well blockchain storage can cope with both requirements is currently unclear.

In order to deal with these challenges, many have suggested the notion of off-chain storage of data, where data is kept outside of blockchain in a conventional or a distributed database, but the hashes of the data are stored in the blockchain. This is said to be the best of both worlds, as healthcare data is stored off-chain and may be secured, corrected, and erased as appropriate. At the same time, immutable hashes of the healthcare data are stored on-chain for checking the authenticity and accuracy of the off-chain medical records.

This idea, however, is not without potential challenges. With the tightening of data protection laws around the world and the attempts by privacy commissioners to regard metadata of 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 blockchain is fit to store personal data may start all over again.

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

4. Records: A Review of the Research Literature,‖ Int'l Journal of Medical Informatics, vol. 77, no.

5. 5, 2008, pp. 291–304.

6. 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.

7. M. Moharra et al., ―Implementation of a Cross-Border Health Service: Physician and

8. Pharmacists' Opinions from the epSOS Project,‖ Family Practice, vol. 32, no. 5, 2015, pp. 564– 67.

9. S.H. Han et al., ―Implementation of Medical Information Exchange System Based on EHR

10. Standard,‖ Healthcare Informatics Research, vol. 16, no. 4, 2010, pp. 281–289.

11. 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.

12. F.Y. Leu et al., ―A Smartphone-Based Wearable Sensors for Monitoring Real-Time

13. Physiological Data,‖ Computers and Electrical Engineering, 2017.

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

15. P.C. Tang et al., ―Personal Health Records: Definitions, Benefits, and Strategies for
16. Overcoming Barriers to Adoption,‖ Journal of the American Medical Informatics Assoc., vol.
17. 13, no. 2, 2006, pp. 121–126.

18. 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.

A. Mu-Hsing Kuo, ―Opportunities and Challenges of Cloud Computing to Improve Health
19. Care Services,‖ Journal of Medical Internet Research, vol. 13, no. 3, 2011.

20. V. Casola et al., ―Healthcare-Related Data in the Cloud: Challenges and Opportunities,‖
21. IEEE Cloud Computing, vol. 3, no. 6, 2016, pp. 10–14.

22. S. Nepal et al., ―Trustworthy Processing of Healthcare Big Data in Hybrid Clouds,‖ IEEE Cloud Computing, vol. 2, no. 2, 2015, pp. 78–84.

23. G.S. Poh et al., ―Searchable Symmetric Encryption: Designs and Challenges,‖ ACM
24. Computing Surveys, vol. 50, no. 3, 2017.
25. Q. Alam et al., ―A Cross Tenant Access Control (CTAC) Model for Cloud Computing:
26. Formal Specification and Verification,‖ IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, 2017, pp. 1259–1268.

27. 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.

28. 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.

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.

29. J. Zhang, N. Xue, and X. Huang, ―A Secure System for Pervasive Social Network- Based
30. Healthcare,‖ IEEE Access, vol. 4, 2016, pp. 9239–9250.

31. J. McKinlay et al., ―Blockchain: Background, Challenges and Legal Issues,‖ DLA Piper

32. Publications, 2016; doi.org/https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain- background-challenges-legal-issues/.