A Survey on Electronic Health Records using Blockchain with Attribute-based Signature Scheme

Nirmal M. Chhodvadiya[1], Kaushik M. Rakholiya[2], Vaman B. Bhuvani[3], Mr. H. J. Shah[4]

[1, 2, 3]*Student, Dept of Computer Engineering, R. N. G. Patel Institute of Technology, Gujrat, India*
[4]*Professor, Dept. of Computer Engineering, R. N. G. Patel Institute of Technology, Gujrat, India*

---***---

ABSTRACT:- *The healthcare industry has been at the cutting edge of technology since time immemorial. Hardware, software, medication, surgical procedures; As with respect to present scenario in the real world in Medical Domain, advancement in terms of treatments given to patient has reached to a high level. For a maintaining record of patients Electronics Health Records (EHR) systems are widely used in hospitals and primary care centres but it is usually difficult to share information and to collect patient data for clinical research. This is partly due to the different proprietary information models and inconsistent data quality. So, we have discussed many implementation methods of Electronic Health Records using Blockchain Technology along with Attribute Based Signature with multiple authorities taking advantage of ABS with the Blockchain technology, so this could preserve the privacy of patients and maintain the immutability of EHRs. On top of that we have also discussed advantages and disadvantages of EHR is also helps to get why should Electronic Health Records are necessary to build with Blockchain Technology along with Attribute Based Signatures.*

KEYWORDS: Blockchain, Healthcare, EHR, Attribute-based signature (ABS)

1.INTRODUCTION

Healthcare processes are highly collaborative and various people from different disciplines must work together to enhance the quality of care. Achievement of this goal has been revolutionized through the use of computer-based methods. For instance, electronic health record (EHR) is commonly used, replacing paper health record with digital one. EHR can improve the quality of care and also reduce costs [1].

Electronic health record (EHR) systems are a type of health information technology (HIT) that has been widely proposed as a mechanism for improving the quality and positive impact of health care services [2]. Research suggests that well-implemented and fully-integrated EHR systems can promote complete record-keeping and more efficient access to documentation, facilitating information sharing and better coordination of care [3].

EHR systems are widely used in hospitals and primary care centres but it is usually difficult to share information and to collect patient data for clinical research. This is partly due to the different proprietary information models and inconsistent data quality [4].

An EHR system includes (1) longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual or health care provided to an individual; (2) immediate electronic access to person- and population-level information by authorized, and only authorized, users; (3) provision of knowledge and decision-support that enhance the quality, safety, and efficiency of patient care; and (4) support of efficient processes for health care delivery. Critical building blocks of an EHR system are the electronic health records (EHR) maintained by providers…and by individuals (also called personal health records) [5].

An EHR with Blockchain that allows patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship [6].

This paper includes implementation methods for Electronic health record (EHR) systems using Blockchain technology, and smart contracts, could help in some typical scenarios related to data access, data management and data interoperability for the specific healthcare domain. the limitations of the Attribute-based signature & advantages and disadvantages of EHR systems. So, one can get easy ides about implementation of Electronic health record (EHR) systems using Blockchain Technology.

2. LITERATURE SURVEY

Table -1: Literature survey

Features	"Who Owns Medical Records: 50 State Comparison" [6]	"Secure_Attribute-Based Signature Scheme with Multiple Authorities" [7]	"Blockchain-based System for Secure Data Storage with Private Keyword Search" [8]	"Escrow Free Attribute-Based Signature with Self-Reveal ability" [9]	"Approach to Threshold Attribute Based Signatures" [10]	"Efficient Attribute-Based Signatures for Non-Monotone Predicates" [11]
Ownership of Data	Yes	No	Yes	Yes	Yes	Yes
Data verification	Yes	No	No	Yes	No	Yes
Use of AES & RSA & ABS Algorithm	Yes	Yes	Yes	No	No	Yes
Availability	Yes	Yes	No	No	No	No
Data Privacy	Yes	Yes	Yes	Yes	Yes	Yes
Data Modifiable	No	No	No	No	Yes	No

A systematic literature review of empirical research on EHR implementation was conducted. Relevant references in the selected articles were also analysed. Search terms included Electronic Health Record (and synonyms), implementation, and hospital (and synonyms). Articles had to meet the following requirements: (1) written in English, (2) full text available online, (3) focused on hospital-wide EHR implementation, and (4) satisfying established quality criteria.

Review on "Who Owns Medical Records: 50 State Comparison" [6] In this paper, patients may create, manage, control and sign their own EHRs and define the predicate while the data verifier is allowed to access this signature and verify the correctness. Use of Blockchain that allows patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers.

Review on "Escrow Free Attribute-Based Signature with Self-Reveal ability" [7] In this paper, multiple attribute authority to generate the attribute-based private key in the attribute-based setting and use of a key extraction protocol to replace the key generation algorithm in attributed-based signature (ABS), In which the key generation centre (KGC) cannot to create a signature on behalf of a legal user with attributes satisfying the corresponding predicate.

Review on "Secure_Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Heal Records Systems" [8] In this paper, author propose a multi-authority ABS scheme, supporting complex policies, expressing AND, OR, and threshold conditions. In which a signer can sign a message with his attributes, and the verifier can only know whether the signer owns attributes satisfying his policy.

Review on "Blockchain-based System for Secure Data Storage with Private Keyword Search"[9] In this paper, introduces a system that uses Blockchain technology to provide the client can upload their data in encrypted form and to provides the data owner a capability to grant permission for others to search on his/her data.

Review on "A New Approach to Threshold Attribute Based Signatures" [10] In this paper author propose a novel approach to construct threshold attribute based signatures inspired by ring signatures. Threshold ABS, defined by a $(t, n*)$ threshold predicate and provides a flexible threshold-ABS scheme that realizes this approach and secure with the help of random oracles.

Review on "Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model" [11] This paper presents a fully secure (adaptive-predicate unforgeable and private) attribute-based signature (ABS). The proposed ABS scheme is efficient and practical. Its efficiency is comparable to (several times worse than) that of the most efficient (almost optimally efficient) ABS scheme the security for which is proven in the generic group model.

3.ADVANTAGES

1. With an electronic health records initiative, many medical providers have created online portals. These portals allow patients to access their medical records whenever they wish, as long as they have a secure data or internet connection.

2. EHR allows every patient to reference a treatment plan or understand how their doctor sees their current state of health at any time.

3. When a patient portal is introduced with an EHR system, it can be setup so that patients can input their own data directly into their records. They can enter their data directly into their file days, if not weeks, before their scheduled visit. It saves them time and it saves time on the administrative work by the medical provider.

4. With an EHR system, doctors can immediately place orders for imaging or laboratory work.

5. An electronic order can be sent directly to the pharmacy of choice for a patient.

6. Medical providers have access to all patient data immediately with an electronic health record.

7. EHRs have eliminated the physical transporting, sifting and filing of charts, making data available at all times.

8. With an EHR system fewer storage costs and demands as compared to paper work and file system.

9. The electronic health record stores them all in a standardized format, it is much easier to skim through directly for the information more relevant to your queries at the time.

10. An electronic health record system often provides an online patients' portal that they can use to access their medical history and information wherever and whenever they wish.

11. Online EHR systems can be much safer, since they are stored on a database that you require the right login details to access.

12. Computerized notes are often easier to read than a physician's handwriting. This reduces the risk of errors and misinterpretations that can negatively impact the quality of patient care.

13. Medical and office staff no longer have to waste time sorting through cumbersome paper records. Users can access electronic health records quickly and efficiently with just a few strokes on a keyboard.

14. An effective EMR platform allows you to spend more meaningful time with your patients during a visit. In just a few clicks, you'll have a patient's medical history, lab results, current treatment plan, and previous medical notes at your fingertips.

15. Securely sharing electronic information with patients and other clinicians.

16. Enabling safer, more reliable prescribing.

4. DISADVANTAGES

1. Ransom ware attacks initiated through malware and other security access problems on electronic health record servers, cost numerous hospitals thousands of dollars per incident.

2. Like any software solution, an electronic health record platform must receive regular updates so that it can perform as needed.

3. EHR must be updated on a regular basis.

4. When the doctor forgets the electronic device, then gaps of information may begin to appear in the patient record.

5. Electronic health record systems are not cheap.

6. Lack of interoperability between electronic health records (EHRs).

7. Cost of set-up and maintenance of electronic health records (EHRs) is often a deterrent.

8. EHRs actually increase the physician workload. With written notes, documentation tended to be briefer and straight to the point. With EHRs, much more documentation is required of physicians before, during and after a patient visit.

9. With EHRs, there are no give-and-take conversations or question-and-answer scenarios.

10. For every task large or small — whether it's a basic wellness visit, a diagnosis, a procedure, a treatment or a prescription — the EHR system requires a corresponding update.

11. EHRs allow for easier access to sensitive information, there is an increased risk of privacy violations.

12. Many EHR systems allow for auto-population of data for new records. While these shortcuts save some time and effort on behalf of the physician, they can also result in inaccurate new records if the previous auto-populated record is not current.

13. It takes time due to factor in the preliminary research like determining budget and deciding which features need as well as the time spend doing product demos and negotiating with vendors to building electronic health records system (EHRs).

14. With EHR Cyber security issues like medical staff must be trained in basic digital security to ensure they do not leave their stations vulnerable to unauthorized access. Having patient's data fall into the wrong hands is not acceptable.

5. CONCLUSION

In this paper, we have discussed many implementation methods of Electronic Health Records using Blockchain Technology. Among which, attribute-based signature (MAABS) scheme with multiple authorities is superior for taking advantage of ABS with the block chain technology, this proposal could preserve the privacy of patients and maintain the immutability of EHRs. Also we have provide different ABS methods for EHR with their limitations. In addition to that advantages and disadvantages of EHR is also helps to get why Electronic Health Records should are necessary to build with Blockchain Technology along with Attribute Based Signatures.

6. REFERENCES

[1] Bleich, H.L. and W.V. Slack, Reflections on electronic medical records: When doctors will use them and when they will not. International Journal of Medical Informatics, 2010. 79(1): p. 1-4.

[2] Chase HS, Mitrani LR, Lu GG, Fulgieri DJ. Early recognition of multiple sclerosis using natural language processing of the electronic health record. BMC Med Inform Decis Mak 2017 Feb 28;17(1):24

[3] Elias B, Barginere M, Berry PA, Selleck CS. Implementation of an electronic health records system within an interprofessional model of care. J Interprof Care 2015;29(6):551-554.

[4] Chen, R., Enberg, G. & Klein, G.O. BMC Med Inform Decis Mak (2007) 7: 10. https://doi.org/10.1186/1472-6947-7-10

[5] National Institutes of Health, Committee on Data Standards for Patient Safety. Key Capabilities of an Electronic Health Record System: Letter Report. Washington, DC: National Academies Press; 2003

[6] Health Information and the Law. George Washington University Hirsh Health Law and Policy Program. (Aug. 20, 2015). Who Owns Medical Records: 50 State Comparison. [Online]. Available: http://www.healthinfolaw.org/comparative-analysis/who-owns-medical- records-50-state-comparison

[7] Cui, Hui & Wang, Guilin & Deng, Robert & Qin, Baodong. (2016). Escrow Free Attribute-Based Signature with Self-Revealability. Information Sciences. 367. 10.1016/j.ins.2016.07.010.

[8] Rui Guo, Huixian Shi, Qinglan Zhao, Dong Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems", Access IEEE, vol. 6, pp. 11676-11686, 2018.

[9] Shangping Wang, Yinglong Zhang, Yaling Zhang, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems", Access IEEE, vol. 6, pp. 38437-38450, 2018.

[10] Selvi, S.S., Venugopalan, S., & Rangan, C.P. (2011). A New Approach to Threshold Attribute Based Signatures.

[11] Okamoto T., Takashima K. (2011) Efficient Attribute-Based Signatures for Non-monotone Predicates in the Standard Model. In: Catalano D., Fazio N., Gennaro R., Nicolosi A. (eds) Public Key Cryptography – PKC 2011. PKC 2011. Lecture Notes in Computer Science, vol 6571. Springer, Berlin, Heidelberg