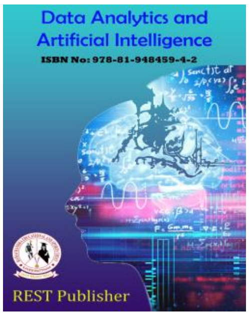
Data Analytics and Artificial Intelligence

Vol: 3(3), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/


Data Analytics and Artificial Intelligence
ISBN No: 978-81-948459-4-2
REST Publisher

Block Chain-Based Electronic Health Records Management

[*] M.Lilly Florence, Poornachandra.R, Konduru Manideep, Maligi Bayya Reddy

Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India.

[*]Corresponding Author Email: drlilly2011@gmail.com

Abstract: *Electronic health records (EHRs) are becoming increasingly popular in healthcare as a means of improving patient care and reducing healthcare costs. However, the security and privacy of EHRs are major concerns, as patient health information (PHI) needs to be protected from unauthorized access, theft, or misuse. To address these concerns, several technologies such as SHA, AES, and blockchain can be used to secure EHRs. SHA (Secure Hash Algorithm) is a cryptographic hash function that generates a unique digital signature for a message or file. AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm that uses a key to encrypt and decrypt data. Blockchain is a decentralized, tamper-proof ledger hat stores data in a secure and transparent way.*

Keywords: *SHA (Secure Hash Algorithm), AES (Advanced Encryption Standard)*

1. INTRODUCTION

The storage and transfer of medical records are critical in the healthcare industry. However, the traditional methods of storing and transferring medical records have proved to be insecure and inefficient. With the increase in data breaches and cyber-attacks, it has become essential to find a secure and efficient way of storing and transferring medical records. Blockchain technology has emerged as a potential solution to the problems of traditional record-keeping systems. This paper proposes an efficient data security mechanism for medical records using blockchain technology with AES and SHA algorithms.

2. RELATED WORK

TITLE: Blockchain technology: Is this the solution to emr interoperability and security issues in developing countries

AUTHOR: G. Kamau, C. Boore, E. Maina, and S. Njenga

YEAR: 2018

The burden of disease is higher by far in developing countries than in the developed world. Developing countries today are turning to technology as the silver bullet or remedy. Indeed, Information and Communication Technology has turned into a key-enabling tool in the enhanced healthcare management. The electronic health records or electronic medical records (EMR) a key component of medical informatics symbolize potential solutions for enhanced healthcare. However, interoperability and security of EMR systems has been the two main challenges of EMR in the healthcare industry. By analyzing existing literature using scoping review research approach this paper explored the potential use of blockchain technology in improving the interoperability and security of EMR systems for the benefit of different stakeholders in health sector in developing countries such as Kenya. To achieve our main objective, five databases were searched and 204 papers screened for inclusion. As a result of the search and screen process, we identified 25 relevant articles.

TITLE: Guide to Attribute Based Access Control (ABAC) Definition and Consideration

AUTHOR: Chung Tong Hu, David F. Ferraiolo, David R. Kuhn
YEAR: 2019

Includes updates as of February 25, 2019] this document provides Federal agencies with a definition of attribute-based access control (ABAC). ABAC is a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. This document also provides considerations for using ABAC to improve information sharing within organizations and between organizations while maintaining control of that information.

TITLE: A blockchain-based architecture for traffic signal control system
AUTHOR: W. Li, M. Nejad, and R. Zhang
YEAR: 2019

Ever-growing incorporation of connected vehicle (CV) technologies into intelligent traffic signal control systems brings about significant data security issues in the connected vehicular networks. This paper presents a novel decentralized and secure by design architecture for connected vehicle data security, which is based on the emerging blockchain paradigm. In a simulation study, we applied this architecture to defend the Intelligent Traffic Signal System (I-SIG), a USDOT approved CV pilot program, against congestion attacks. The results show the performance of the proposed architecture for the traffic signal control system.

TITLE: Medrec: Using blockchain for medical data access and permission management
AUTHOR: A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman
YEAR: 2016

Years of heavy regulation and bureaucratic inefficiency have slowed innovation for electronic medical records (EMRs). We now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. In this paper, we propose MedRec: a novel, decentralized record management system to handle EMRs, using blockchain technology. Our system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, MedRec manages authentication, confidentiality, accountability and data sharing- crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. We incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain “miners”. This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. The purpose of this short paper is to expose, prior to field tests, a working prototype through which we analyze and discuss our approach.

TITLE: Blockchain based access control
AUTHOR: D. D. F. Maesa, P. Mori, and L. Ricci
YEAR:2017

Access Control systems are used in computer security to regulate the access to critical or valuable resources. The rights of subjects to access such resources are typically expressed through access control policies, which are evaluated at access request time against the current access context. This paper proposes a new approach based on blockchain technology to publish the policies expressing the right to access a resource and to allow the distributed transfer of such right among users. In our proposed protocol the policies and the rights exchanges are publicly visible on the blockchain, consequently any user can know at any time the policy paired with a resource and the subjects who currently have the rights to access the resource. This solution allows distributed auditability, preventing a party from fraudulently denying the rights granted by an enforceable policy. We also show a possible working implementation based on XACML policies, deployed on the Bitcoin blockchain

TITLE: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control
AUTHOR: X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang,
YEAR: 2016

Healthcare data are a valuable source of healthcare intelligence. Sharing of healthcare data is one essential step to make healthcare system smarter and improve the quality of healthcare service. Healthcare data, one personal asset of patient, should be owned and controlled by patient, instead of being scattered in different healthcare systems, which prevents data sharing and puts patient privacy at risks. Blockchain is demonstrated in the financial field that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we proposed an App (called Healthcare Data Gateway (HGD)) architecture based on blockchain to enable patient to own, control and share their own data easily and securely without violating privacy, which provides a new potential way to improve the intelligence of healthcare systems while keeping patient data private. Our proposed purpose-centric access model ensures patient own and control their healthcare data; simple unified Indicator-Centric Schema (ICS) makes it possible to organize all kinds of personal healthcare data practically and easily. We also point out that MPC (Secure Multi-Party Computing) is one promising solution to enable untrusted third-party to conduct computation over patient data without violating privacy.

3. EXISTING SYSTEM

Azaria et al. proposed a decentralized record management system to handle EHRs. The system gives patients an immutable log and easy access to their medical information. However, the protocol used is based on consensus mechanism of proof-of-work which consumes massive computing resources. Measaetal. Proposed a block chain-based solution to publishing the policies expressing access rights of resources and allowing the distributed transfer of such rights among users. The authors presented a Bitcoin based proof-of-concept implementation without describing any experiment or evaluation. Wang et al. proposed an iOS App termed Healthcare Data Gateway based on blockchain to enable patient to own, control and share their own data. Ekblaw et al. proposed the MedRec prototype to give patients an immutable log and access to their medical information across healthcare providers and treatment sites. There have been various attempts to address the proper access control issues on data management using blockchain. Zyskind et al. described a decentralized data management system which ensures users own and control their data and proposed a protocol to enable automated access-control manager using multi-party computation.

4. PROPOSED SYSTEM

In this project we have proposed to manage EHRs: concept, prototype and implementation. This study focuses on Secure Hash Algorithm (SHA) and Advanced Encryption Standard (AES) to find and analyze submitted articles concept or implemented to manage EHR using blockchain. In-depth technical analysis focused on commodity pricing based on privacy, security, scalability, accessibility, cost, consensus algorithm and blockchain type used.Finally, future research directions, ultimately, will lead to enthusiasm in incorporating new blockchain-based systems for proper EHR management.

5. MATERIAL AND METHODS

Sha-256 Algorithm: SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits. Message Length: The length of the cleartext should be less than 264 bits. The size needs to be in the comparison area to keep the digest as random as possible. Digest Length: The length of the hash digest should be 256 bits in SHA 256 algorithm, 512 bits in SHA-512, and so on. Bigger digests usually suggest significantly more calculations at the cost of speed and space. Irreversible: By design, all hash functions such as the SHA 256 are irreversible. You should neither get a plaintext when you have the digest beforehand nor should the digest provide its original value when you pass it through the hash function again.

6. METHODOLOGY

The proposed system utilizes blockchain technology to store and transfer medical records. The medical records are encrypted using the AES algorithm before being stored on the blockchain. The SHA algorithm is used to generate a hash value for each record to ensure its integrity. The blockchain network consists of nodes that validate and verify transactions. The proposed system allows authorized users to access medical records securely and efficiently.

Hospital Manager Maintains the Data's: Hospital register and login then add department in the list and also can create authentication for doctor, patient, and lab Assistant and finally can view the feedback.

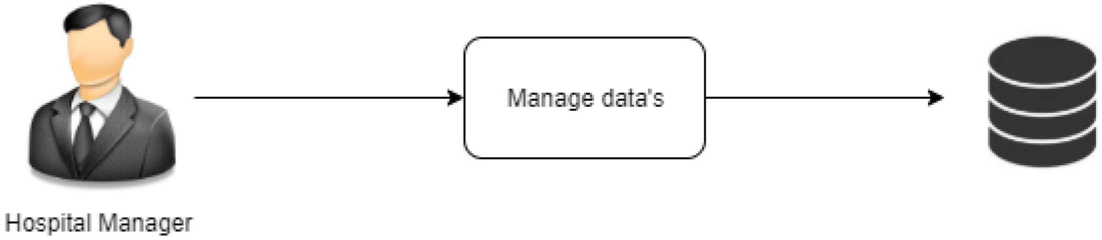


FIGURE 1. Hospital Manager

Doctor Request Patient File: Doctor register and login then can update profile and also request patient file to view the data. After accepting the file by patient request status been changed and can be view in request status. At last the patient files can be viewed and also view the blockchain performed on the data.

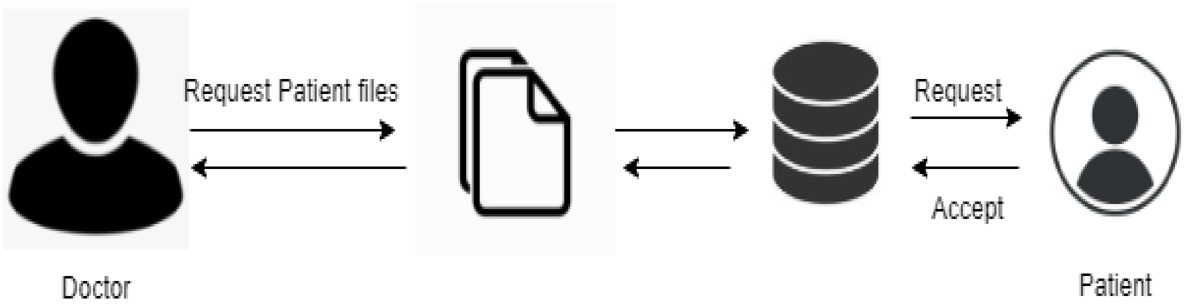


FIGURE 2. Doctor Request

Patient View the Report File: Patient register and login then can view report file and view file request the doctor request to access been sent and the by accepting the request doctor can access the data.

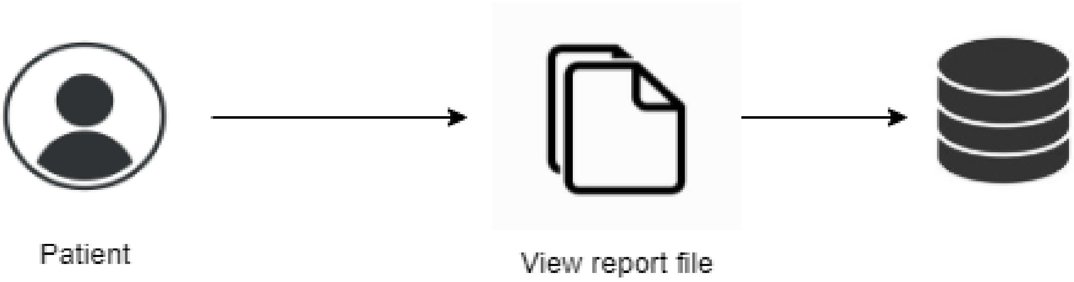


FIGURE 3. Patient View

Lab Assistant Makes the Report Entry: Lab assistant register and login make patient report entry and can view the report files and can update the profile.

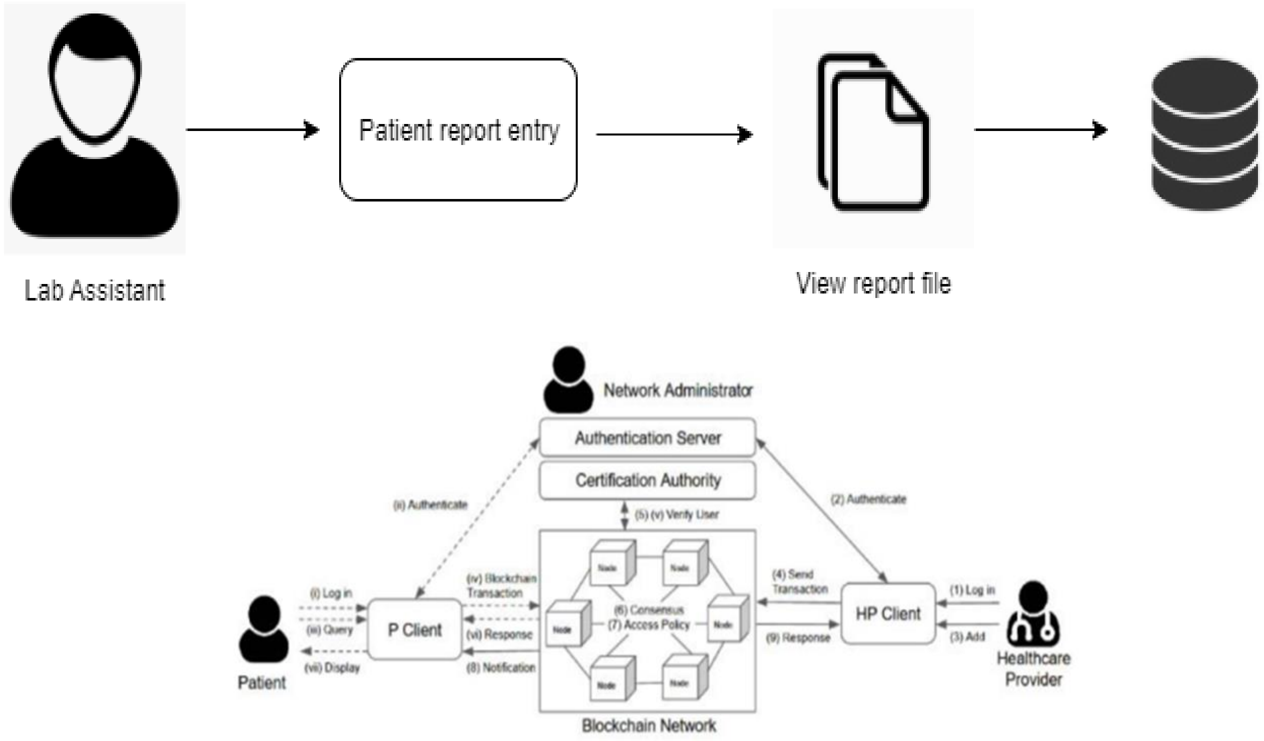


FIGURE 4. Lab Assistant Makes

7. RESULT

The proposed system ensures the integrity, confidentiality, and accessibility of medical records. The use of AES encryption ensures that the medical records are secure and cannot be accessed by unauthorized users. The SHA algorithm ensures that the records are tamper-proof and cannot be altered. The decentralized nature of the blockchain ensures that there is no single point of failure, and the records can be accessed from anywhere at any time.

8. CONCLUSION

Blockchain can control decentralized commercial centers and coordination stages for different segments of artificial intelligence, including information, calculations, and registering power. These will cultivate the development and appropriation of simulated intelligence to an exceptional level. Blockchain will likewise enable simulated intelligence's choices to be increasingly straightforward, logical, and reliable. As all information on the blockchain is freely accessible, simulated intelligence is the way to furnishing clients with secrecy and protection. Blockchain can empower information sharing since it gives straightforwardness and responsibility with respect to which client's information, when, and by whom. As blockchain puts the control of information again into client's hands, they will have more trust in sharing information and realizing that their information will be utilized appropriately to give better personalization or to other great motivation. Specialists and scientists could get to (anonymized and enormous) clinical records and cases, generously speeding up the revelation of solutions for infections and the improvement of better treatment ideal models and clinical strategies. Patients with uncommon maladies, particularly, would discover new expectations, as specialists could get to comparative cases from all around the globe. Machine Learning models can legitimately be taken care of information (anyway the rights will be overseen by a focal power). This will expand the precision and effectiveness of machine learning models thus their ease of use. The Human services industry straightforwardly relates to the life of an individual. This could help patients just as specialists.

REFERENCES

[1]. S. Vyas, M. Gupta and R. Yadav, "Converging Blockchain and Machine Learning for Healthcare," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 709-711.

[2]. N. Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [online] Available: https://bitcoin.org/bitcoin.pdf.

[3]. Peng Zhang, Douglas C. Schmidt, Jules White and Gunther Lenz, “Blockchain Technology Use Cases in Healthcare”, 2018 Advances in Computer, Elsevier.

[4]. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.

[5]. B. Shah, N. Shah, S. Shakhla and V. Sawant, "Remodeling the Healthcare Industry by employing Blockchain Technology," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, 2018, pp. 1-5.

[6]. MS Muneshwara, A Lokesh, MS Swetha, M Thungamani, “Ultrasonic and image mapped path finder for the blind people in the real time system,” IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) IEEE, page no 964-969 2017

[7]. J. Huang, Y. W. Qi, M. R. Asghar, A. Meads and Y. Tu, "MedBloc: A Blockchain- Based Secure EHR System for Sharing and Accessing Medical Data," 2019 18th IEEE International Conference On Trust, Security and Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 594-601.

[8]. X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5

[9]. J. Qiu, X. Liang, S. Shetty and D. Bowden, "Towards Secure and Smart Healthcare in Smart Cities Using Blockchain," 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 2018, pp. 1-4.

[10]. K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019.