International Journal of Computational Mathematics and Computer Science
Volume 1, Issue 2, July (2024)
ISSN: XXXX-XXXX

Blockchain-based Cloud Smart Healthcare System with Dual Access Control Framework

Dr. Hannah Vijaykumar*
Dean, Computational Studies, Associate Professor and Head,
Department of Computer Science, Anna Adarsh College for Women, Anna Nagar, Chennai 600 040.
Email: hannahvijaykumar@annaadarsh.edu.in

Dr. R. Manimaran
Assistant Professor and Head
Department of Information Technology, J.J. College of Arts and Science, Pudukkottai - 622 442.
Email: rmanimaranjj@gmail.com

Abstract – The Medical Records Management (MRM) is used to store the personal data of numerous patients. Fraudulent activities will be less likely with the use of blockchain-enabled records that can store, track, and manage all the transactions. The standard patient records demand a significant effort in terms of labour hours. For instance, if a patient attends a clinic or a hospital, records pertaining to his or her past must be searched first before being sent to the necessary department for the patient's real examination. The primary objective of this work is to implement Blockchain based Healthcare System with Dual Access Control Framework. The proposed framework used ECDSA signature algorithm for preserve data privacy and provide secured and authenticated data exchange and storage.

Keywords: IoT, Blockchain, Cloud storage, Integration of blockchain and IoT.

1. INTRODUCTION

Blockchain can significantly reduce costs and increase efficiency thanks to these attributes. Persistency, secrecy, decentralisation, and audibility are fundamental characteristics of blockchain innovation. The majority of the time, the Electronic Health Record (EHR) is described as a collection of patients' electronic health data (for example as electronic clinical records – EMRs). For EHR primarily from medical care providers in the clinical settings, EMRs can serve as an information hub.

A blockchain-based secured and privacy preserving data sharing model for IoT devices and applications is developed. With the increasing number of IoT devices and applications, securing data transactions between different entities within and outside the networks is a critical requirement. Distributed systems can address the safety aspects of data transactions but fail to scrutinize data modifications, non-forwarding of data, and fake data forwarding. The

*Corresponding Author

major intend of cloud computing is to use the distributed sources effectively, incorporate them to achieve high throughput, and is capable of resolving widespread computation difficulties. Cloud computing associates with scalability, virtualization, interoperability, the standard of service, and the delivery methods, such as public, private, and the integration of both.

1.1 Healthcare System Security

Medical findings can be anything like patient records or the data that has been received from the patient using sensors. As patient records are generally translated from paper records to digitized mediums, they require more security and authority to be put in the right place to secure the medical findings and the records. Medical services records are being put away in information bases, just approved people have the option to get to those data, and access should be verified and approved. Current strategies to ensure about records have demonstrated not to be as manipulate and replicate a patient's health records can have genuine outcomes. Figure 1 illustrates Smart contracts for transaction management in the blockchain.

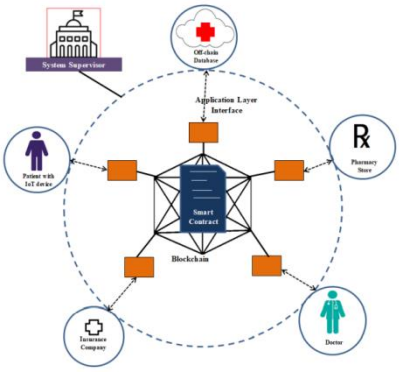

Figure 1 Smart contracts for transaction management in the blockchain

1.2 Health Record Sharing

Healthcare systems are joint efforts of health and information technologies. The digitized way of data sharing can raise the chances of security problems along with the problem of civilian medical records. Healthcare record sharing can be tedious because the same individual's records can be stored in multiple places which will raise the situation of duplicity in the system. A primary issue with wellbeing record sharing is interoperability

2. LITERATURE REVIEW

(Macrinici, Cartofeanu, and Gao, 2018) investigated the numerous fields and places in which blockchain technology might be employed, as well as how it can be used to other nonfinancial industries. The main areas where blockchain can be successfully applied are smart healthcare systems, combating fake medications in pharmaceutical businesses, and digitally signing correspondence and legal contracts.

(Xia et al., 2017) proposed securing personal health data framework by providing privacy, security, integrity, and access control of health records of patients as it uses SAAS (Software as a Service) network for its implementation. It takes into consideration patient data and converts it into personalized data. Although the risk is minimized by architecting the correct mechanism there still exists some risks associated with it which is that people tend to exchange their reports with others.

(Shahnaz, Qamar, and Khalid, 2019) proposed the applications of Blockchain technology except for the financial domain. The major focus was emphasized on how Blockchain can help us in day today life for the maintenance and security of electronic health records. (Shahnaz, Qamar, and Khalid, 2019) proposed the applications of Blockchain technology except for the financial domain. The major focus was emphasized on how Blockchain can help us in day today life for the maintenance and security of electronic health records.

(Shahnaz, Qamar, and Khalid, 2019) proposed the applications of Blockchain technology except for the financial domain. The major focus was emphasized on how Blockchain can help us in day today life for the maintenance and security of electronic health records.

The existing research works based on ledger-based blockchain techniques are elucidated as follows, Rajput, A.R et al. [56] developed emergency access control management model (EACMS) for health record using blockchain system. In this model, various rules were employed based on smart contracts for controlling emergency situations and period length. Moreover, hyperledger composer was applied for generating Business Network Archive (BNA), which identifies the system capacity. Here, every transaction was disturbed with data fetching and authorization from ledger, which was performed by smart contracts. Besides, this model functions depends on smart contracts of ledger for providing effectual, secured and auditable system.

Thwin, T.T. and Vasupongayya, S [87] presented blockchain enabled access control method for preserve privacy for personal health record scheme. In this model, blockchain was included for supporting tamper resistance feature. Moreover, cryptographic and proxy re-encryption algorithms were devised for preserving privacy of system. In addition, the features, like tamper resistance, revocability consent, and auditability were included for better performance. Moreover, proxy re-encryption model enables the user for sharing their decryption abilities with others for security purpose.

Healthcare and innovation go hand in hand while the latter is applied to medical diagnosis and treatments. All the procedures in the system are stored as immutable records, and hence they cannot be manipulated [Wang et al., 2018]. Patient device tracking, insurance billing, and pharmacy store settlements are part of the healthcare applications. Negotiations between these entities require authentication and privacy mechanisms. Transaction speed inside the blockchain must be improved for smother and hassle-free transactions inside the network [Tanwar et al., (2020)]. The patient data collected can be stored on-chain or offchain by the healthcare applications. Care should be taken while sharing data from this storage to preserve data privacy and prevent unauthorized access [Rahman et al., (2021)]

3. PROPOSED SYSTEM

Blockchain Account Creation

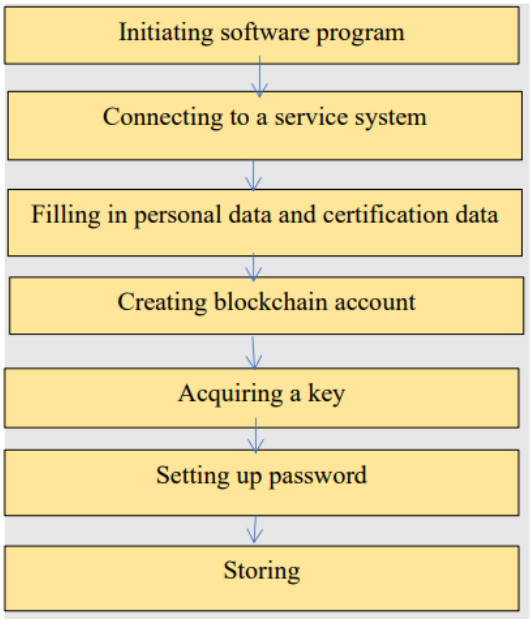

Figure 2 Block diagram

Figure 2 shows how to create a blockchain account. A series of sub-level transactions are completed before any transaction is initiated. The software programme is what kicks things off. The Serving System, which is in charge of several crucial activities including accessing and processing patient requests as well as verifying and registering all patient transactions, is connected. Once a connection has been made, the user interface enables updating of the patient's personal information as well as several forms of authentication such private key and certification information.

Algorithm for storing patient information in the database

```
Input: patientID, E_SP(patient_body_parameters )
Output: bool
pragma solidity ^0.5.12;
mapping(address => bool) authorizedPatients;
 if( isPatientAuthorized(patientID))
 {
  store encrypted patient body parameters into the database;
  record transaction in the blockchain;
 }
 function public isPatientAuthorized(address patientID) public view return (bool
approved)
 {
    return authorizedPatients[patientID];
 }
```

ECDSA algorithm

This work used ECDSA Key algorithm for Digital signature. The newly established user can also set a password through his or her user interface to guard against illegal access to both his or her data and the Blockchain in general. One of the simplest and safest digital signature algorithms is ECDSA. A thorough design of the elliptic curve parameters prevents an attacker from being able to solve the ECDLP in less than exponential time. The ECDSA methods for key generation, signature generation, and signature verification are presented in this subsection. The parameters of the ECDSA domain are q, E(Fq), P, n, and h. Table 1 provides a summary of these factors.

Table 1 ECDSA Key Generation Algorithm

Input: Standard domain parameters
Output: Key Pairs: Public Key- Q, Private Key- d

1. For an elliptic curve $E(\mathbb{F}_q)$, choose P of order n, $P \in E(\mathbb{F}_q)$
2. Choose a random integer d such that $2 \leq d \leq n-2$.
3. Compute $Q = dP$.

The public key and private key for ECDSA signatures are constructed using domain settings in table 1 for key generation. The creation of signatures is covered by Algorithm 2.

Table 2 ECDSA Signature Generation Algorithm

Input: Message to be signed m, Private Key d, Elliptic Curve Domain Parameters
Output: ECDSA Signature (m, r, s)

1. Signer chooses a random integer k, such that $2 \leq k \leq n-2$
2. Compute $R = kP$
3. $r = x(R) (\text{mod } n)$, where $x(R)$ is x- coordinate of R.
4. Compute $s = k^{-1}(h(m) + dr) \ (\text{mod } n)$

ECDSA signatures are verified using Algorithm 3. The algorithm outlines the procedures for checking each ECDSA signature individually.

Table 3 ECDSA Signature Verification Algorithm

Input: ECDSA signature (m, r, s), Public Key Q
Output: Signature Accept or Reject

1. Verifies if $(r, s) \in [1, n-1]$, else rejects the signature.
2. The verifier computes $w = s^{-1} (\text{mod } n)$
3. Compute $u = h(m)w \ (\text{mod } n)$
4. Compute $v = rw \ (\text{mod } n)$
5. Calculate value of $R.y$ to retrieve point R through square root method from received r value
6. Compute $R = uP + vQ \in E(\mathbb{F}_q)$, and accept the signature if and only if $x(R) = r \ (\text{mod } n)$, where $x(R)$ is x- coordinate of R.

4. RESULTS AND DISCUSSION

The laptop with Intel core i7 processor clocking at 2.20GHz and 24 GB RAM, running on Ubuntu LTS 18.04 operating system is used as the miner. Table 4 summarizes the execution time by various security processes in the system.

Table 4 Timings of security specific processes in the proposed system

Process	Time
SHA – 3 256	193 µS on Raspberry Pi 3 B 191 µS on Raspberry Pi 3 B+
Block Time	11.21 Seconds
Migration and deployment of smart contract	9.14 Seconds
Mining Time	1.7 Seconds
Total Deployment Cost	0.00179117 ETH

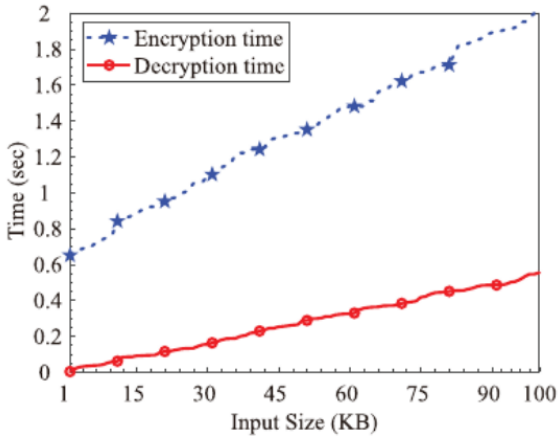

Figure 3 Computational time for registration and retrieval

The solid line in Figure 3 represents the decryption process or the retrieval of MRM from the scheme, while the dashed line in this work analyses the delay during encryption and signing of MRM versus the size of MRM. Particularly for real-time smart healthcare systems, it is necessary to explore how encryption and decryption affect end-to-end delays.

Table 5 compares the proposed framework to conventional donation methods.

Properties	Traditional Donation method	Proposed donation framework based on blockchain technology
Structure	Centralized	Decentralized
Security	Less	High
Transparency	No	Yes
Risk	High	Low
Control	Not Provide control to contributors	Provide Control to Contributors

Table 5 displays a contrast between the suggested method and currently used methods. The dispersed strategy rendered the possibility of a single point of failure impossible. The suggested system is strong by traditional standards, and the blockchain's usage of digital signatures makes it immune to non-repudiation attacks.

5. CONCLUSION

A proposed method to integrate blockchain and IoT is designed and implemented. Initially, the central authority based security for IoT devices is discussed and the disadvantages of such methods are explained. Then, the decentralization based security using blockchain is explained in detail. A healthcare application is demonstrated as proof concept to evaluate the performance of the system. The developed model provides high-level identity management data privacy and access control with the help of smart contracts. Also, it is evident from the block processing time as a function of increasing number of blocks are as low as 3 seconds compared to the existing similar models where processing time is more than 50 seconds. The proposed method offers better security solutions without incurring much computational costs

REFERENCES

[1] Ammad, M., et al. (2020). A Novel Fog-Based Multi-Level Energy-Efficient Framework for IoT-Enabled Smart Environments. IEEE Access, volume 8, pp. 150010-150026.

[2] Azad, M. A., J. Arshad, S. Mahmoud, K. Salah and M. Imran (2019). A privacypreserving framework for smart context-aware healthcare applications, Transactions on Emerging Telecommunications Technologies., volume 4, pp. e3634.

[3] Besher, K. M., S. Beitelspacher, J. I. Nieto-Hipolito and M. Z. Ali (2021). Sensor Initiated Healthcare Packet Priority in Congested IoT Networks. IEEE Sensors Journal, 21(10), pp. 11704-11711.

[4] Biswas, S., K. Sharif, F. Li, B. Nour and Y. Wang (2019). A Scalable Blockchain Framework for Secure Transactions in IoT. IEEE Internet of Things Journal, 6(3), pp. 4650-4659.

[5] Celia, L., and Y. Cungang (2018). (WIP) Authenticated Key Management Protocols for Internet of Things. Proceedings of 2018 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA. pp. 126-129.

[6] Choi, S., J. Ko and J. Kwak (2019). A Study on IoT Device Authentication Protocol for High Speed and Lightweight. International Conference on Platform Technology and Service (PlatCon), pp. 1-5.

[7] Cirillo, F., D. Gómez, L. Diez, I. Elicegui Maestro, T. B. J. Gilbert and R. Akhavan (2020). Smart City IoT Services Creation Through Large-Scale Collaboration. IEEE Internet of Things Journal, 7(6), pp. 5267-5275.

[8] Ding, W., H. Rui, Y. Zheng, Q. Xinren, H. D. Robert, T. Y. Laurence, and D. Mianxiong (2019). An Extended Framework of Privacy-Preserving Computation with Flexible Access Control. IEEE Transactions on Network and Service Management, 17(2), pp. 918-930

[9] Elayan, H., M. Aloqaily and M. Guizani (2021). Digital Twin for Intelligent Context-Aware IoT Healthcare Systems. IEEE Internet of Things Journal, 8(23), pp. 16749-16757.

[10] Elbery, A., H. S. Hassanein, N. Zorba and H. A. Rakha (2020). IoT-Based Crowd Management Framework for Departure Control and Navigation," in IEEE Transactions on Vehicular Technology, 70(1), pp. 95-106.

[11] Gangoiti, U., A. López, A. Armentia, E. Estévez, O. Casquero and M. Marcos (2022). A Customizable Architecture for Application-Centric Management of Context-Aware Applications. IEEE Access, volume 10, pp. 1603-1625.

[12] Haghi, M., S. Neubert, A. Geissler, H. Fleischer, N. Stoll, R. Stoll, and K. Thurow (2020). A Flexible and Pervasive IoT-Based Healthcare Platform for Physiological and Environmental Parameters Monitoring. IEEE Internet of Things Journal, 7(6), pp. 5628-5647.

[13] Hammi, M. T., B. Hammi, P. Bellot, and A. Serhrouchni (2018). Bubbles of trust: a decentralized blockchain-based authentication system for IoT. Computers and Security, volume 78, 126–142.

[14] Javed, A., A. Malhi, T. Kinnunen and K. Främling (2020). Scalable IoT Platform for Heterogeneous Devices in Smart Environments. IEEE Access, volume 8, pp. 211973-211985

[15] Kaur, K., G. Kaddoum and S. Zeadally (2021). Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem. IEEE Transactions on Intelligent Transportation Systems, 22(8), pp. 5178-5189.

[16] Korenda A.R., F. Afghah, B. Cambou and C. Philabaum (2019). A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices. Proceedings of 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 1-8.

[17] Liu, H., X. Yao, T. Yang and H. Ning (2019). Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health. IEEE Internet of Things Journal, 6(2), pp. 1352-1362.

[18] Mamvong, J. N., G. L. Goteng, B. Zhou and Y. Gao (2021). Efficient Security Algorithm for Power-Constrained IoT Devices. IEEE Internet of Things Journal, 8(7), pp. 5498-5509.

[19] Marino, F., C. Moiso, and M. Petracca (2019). PKIoT: A public key infrastructure for the Internet of Things. Transactions on Emerging Telecommunications Technologies. 30(7).

[20] Nabeel, N., M. H. Habaebi and M. D. R. Islam (2021). Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT. IEEE Access, volume 9, pp. 165754-165765.

[21] Psarra, E., I. Patiniotakis, Y. Verginadis, D. Apostolou and G. Mentzas (2020). Securing Access to Healthcare Data with Context-aware Policies. Proceedings of 2020 11th International Conference on Information, Intelligence, Systems and Applications, pp. 1-6.

[22] Rahman, M. Z. U., S. Surekha, K. P. Satamraju, S. S. Mirza and A. LayEkuakille (2021). A Collateral Sensor Data Sharing Framework for Decentralized Healthcare Systems. IEEE Sensors Journal, 21(24), pp. 27848-27857

[23] Saleem, M. A., Z. Ghaffar, K. Mahmood, A. K. Das, J. J. P. C. Rodrigues and M. K. Khan (2021). Provably Secure Authentication Protocol for Mobile Clients in IoT Environment Using Puncturable Pseudorandom Function. IEEE Internet of Things Journal, 8(22), pp. 16613-16622.

[24] Tanwar, S., K. Parekh, and R. Evans (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, volume 50, 102407.

[25] Wang, S., J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F-Y Wang (2018). Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. IEEE Transactions on Computational Social Systems, 5(4), pp. 942-950.

[26] Xu, J., K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu (2019). Healthchain:A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things Journal, 6(5), pp. 8770-8781.

[27] Yanambaka, V.P., S. P. Mohanty, E. Kougianos and D. Puthal (2019). PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. IEEE Transactions on Consumer Electronics, 65(3), pp. 388-397.

[28] Zheng, W., C. -F. Lai, D. He, N. Kumar and B. Chen (2021). Secure Storage Auditing With Efficient Key Updates for Cognitive Industrial IoT Environment. IEEE Transactions on Industrial Informatics, 17(6), pp. 4238-4247.