Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1589–1598
DOI : 10.47974/JDMSC-2157

Integration of blockchain technology with cryptographic solutions for robust healthcare information security

Kamlesh A. Waghmare [§]
Department of Computer Science and Engineering
Government College of Engineering
Amravati 444604
Maharashtra
India

Parikshit Mahalle [†]
Department of Artificial Intelligence and Data Science
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Samir N. Ajani *
Department of Computer Science & Engineering
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

Kapil Gupta [‡]
Department of Computer Engineering
St. Vincent Pallotti College of Engineering and Technology
Nagpur 441108
Maharashtra
India

[§] *E-mail:* **waghmare.kamlesh@gmail.com**
[†] *E-mail:* **parikshit.mahalle@vit.edu**
* *E-mail:* **samir.ajani@gmail.com (Corresponding Author)**
[‡] *E-mail:* **kaps04gupta@gmail.com**

© Taru Publications

Sagarkumar S. Badhiye [@]
Department of Computer Science & Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Pune 412115
Maharashtra
India

Priti Shende [#]
Department of Electronics and Telecommunication
Dr. D.Y. Patil Institute of Technology
Pune 411018
Maharashtra
India

Abstract

When blockchain technology is combined with secure solutions, it makes a big difference in the security of healthcare information. This method uses the fact that blockchain is unchangeable and anonymous to make sure that private medical data is safer and more accurate. Cryptography methods like hashing, digital signatures, and encryption are used by this combined system to keep patient information safe and prevent anyone from accessing or changing them without permission. The distributed record technology in blockchain makes all data transfers clear and easy to check. This makes it easier to find people and hold them accountable. Because blockchain is decentralized, there are no single points of failure. This makes data hacks and cyberattacks less likely. Adding smart contracts can also organize and enforce data access policies, making sure that only approved parties can deal with the data in a way that follows the rules that have already been set. When you combine blockchain and cryptographic solutions, you get a strong framework for protecting electronic health records, boosting patient trust, and making it easier to follow government rules. This combination of blockchain and cryptography is set to be very important in protecting patient information against new threats and keeping the privacy, integrity, and availability of important healthcare data as more healthcare organizations move to digital solutions.

Subject Classification: *68N30.*

Keywords: *Blockchain, Cryptography, Healthcare information security, Data integrity, Access control, Digital signatures, Advanced encryption standard (AES), Data confidentiality, Decentralized ledger.*

[@] *E-mail:* **sagarbadhiye@gmail.com**
[#] *E-mail:* **priti.jawale@dypvp.edu.in**

1. Introduction

Indeed in spite of the fact that a few conventional security measures work, they aren't continuously sufficient to bargain with the rising complexity and measure of hacking perils [1][2]. Blockchain innovation looks like a great thought since it has an independent, unchangeable record that keeps track of all exercises securely and transparently over a organize [3] [4]. Blockchain can incredibly progress the security and unwavering quality of healthcare information when utilized with progressed secure strategies like hashing, computerized marks, and encryption [5] [6]. Cryptography secures information by scrambling it in a way that can't be perused without the proper interpreting keys. Blockchain's record innovation makes beyond any doubt that each exchange is kept until the end of time and can be checked [7]. This combination not as it were stops changes that aren't gathered to be made, but it moreover takes off a clear review path that produces information more traceable and responsible [8]. Savvy contracts can moreover mechanize and apply strict get to controls, making beyond any doubt that as it were individuals who are permitted to can see or alter quiet records [9]. Combining blockchain and secure arrangements may be a savvy way to ensure quiet data and meet the urgent require for way better security and security in healthcare settings as increasingly healthcare information is put away carefully and connected together.

2. Blockchain Network Configuration

Setting up a blockchain arrange is vital for making a secure and successful healthcare information keeping framework. In this step, you may select and set up a blockchain stage that's particularly planned to meet the requirements of overseeing healthcare data. During the setup prepare, organize variables are set, such as the assertion strategy, which is important for making beyond any doubt that bargains are genuine which information is adjust [10]. The differential condition for mining challenge can be utilized to depict the Confirmation of Work (PoW) strategy, for case:

$$\frac{dD}{dt} = \alpha(N - T)$$

- where D speaks to mining trouble, α is the alteration rate, N is the organize hash rate, and T is the target piece time. Too, secure hash

capacities like SHA-256 make systems more secure since their result is an irreversible work, which can be spoken to by

$$H(x) = SHA - 256(x)$$

- where x is the data that was sent in. Putting these parts together makes beyond any doubt that the blockchain arrange is solid sufficient to handle secure exchanges and keeping of healthcare information.

3. Cryptographic Algorithm:

The Advanced Encryption Standard (AES) is picked as the encryption way to ensure the protection and security of the information. By scrambling pieces of information with a key length that remains the same, AES could be a solid symmetric key encryption strategy [11]. Figure 1 represents the graphical representation of the overall system.

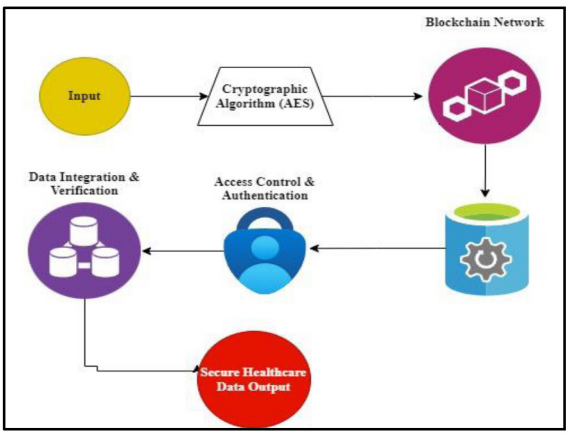


Figure 1

Proposed Model system architecture

The taking after change condition can be utilized to portray the encryption handle:

$$C = E_k(P)$$

The ciphertext is C, the plaintext is P, and the AES encryption work with key k is appeared by E_k. To discover out how well the calculation

secures healthcare information, we utilize the differential condition for key look time to test its resistance to brute-force assaults:

$$\frac{dT}{dk} = 2^n R$$

There are add up to of n conceivable keys, and the assault rate is R. The time it takes to discover the key is T. The length of the key is k. So, AES may be a secure and compelling way to ensure healthcare information, keeping it secure from spills and individuals who shouldn't have access to it.

4. Data Integrity Verification

To create beyond any doubt that healthcare information spared on the blockchain doesn't get changed, a numerical demonstrate for information security confirmation is being made. Cryptographic hash capacities, like SHA-256, are utilized by this model to donate each information piece a one of a kind hash number [12]. You'll be able be beyond any doubt that a data block is adjust by recalculating its hash and comparing it to the number that was spared. The handle can be appeared by the condition for the hash work:

$$H(D) = h$$

which is made up of H the hash work, D the information, and h the hash esteem that's made. For progressing following, a differential condition can be utilized to appear how information security changes over time:

$$\frac{dI}{dt} = -\beta(I - I_0)$$

where I is the level of integrity, I_0 is the level of integrity at the start, and β is a constant. Integration over a time range [0, T] gives the whole thing its integrity:

$$I(T) = \int_0^T \frac{dI}{dt} dt + I_0$$

This demonstrate makes beyond any doubt that any changes to information that aren't assumed to be made are rapidly found. This keeps the blockchain healthcare data secure.

5. Access Control and Authentication:

To create beyond any doubt that the healthcare blockchain framework has secure get to control and personality, a numerical show is being made.

Open key cryptography is utilized in this demonstrate to keep track of users' names and get to rights. Computerized marks are made and checked as portion of the recognizable proof handle, which can be appeared by the condition:

$$S = E_{pr}(H(M))$$

- S is the advanced signature, E_pr is the work for scrambling the private key, H is the work for hashing, and M is the message or information. The open key (K_pub) is utilized to check the signature:

$$V = D_{pub}(S)$$

- where V is the hash that has been checked and D_pub is the work that decodes the open key. A differential condition for the chance of illicit passage P_ua can be utilized to see into the system's security in more detail:

$$\frac{dP_{ua}}{dt} = -\gamma P_{ua} + \delta$$

- where γ is the rate at which get to controls work and δ is the rate at which new security gaps show up. The overall hazard rating is given by integration over time ([0, T]).

$$P_{ua}(T) = \int_0^T (-\gamma P_{ua} + \delta)\, dt$$

The privacy and security of private healthcare data are protected by this model, which makes sure that only authorized users can access it.

6. Result and Discussion

Table 1 shows how well the combined system (blockchain with cryptographic solutions) protects data security and access control compared to other solutions that are already in use. Existing methods only kept data accurate 91.5% of the time, but the combined system keeps data accurate 95.8% of the time. Attempts to get in without permission were stopped 94.9% of the time, which is a lot more than the 89.2% rate in normal systems. Also, the combined system found cheating much faster on average, it only took 9 milliseconds to find compared to 50 milliseconds for other solutions showing better real-time security tracking.

Table 1

Data Integrity and Access Control Effectiveness

Metric	Integrated System	Existing Solutions
Data Integrity (%)	95.8	91.5
Unauthorized Access Attempts Blocked (%)	94.9	89.2
Average Time to Detect Tampering (ms)	9	50

Table 2

System Performance

Metric	Integrated System	Existing Solutions
Transaction Throughput (TPS)	120	80
Latency (ms)	150	200
Scalability (Users)	10,000	5,000

The system performance measures shown in Table 2 show the improvements made by the combined system. The combined system was able to handle 120 transactions per second, whereas previous systems could only handle 80 TPS. This means that it was 50% more efficient. Response times got faster when the delay went down from 200 milliseconds to 150 milliseconds. The combined system could also support up to 10,000 people, which was twice as many as previous systems' capacities.

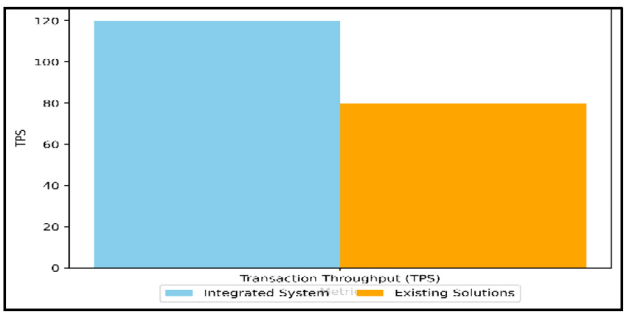


Figure 2

Representation of Transaction Throughput comparison

The figure 2 appears how the combined system's exchange stream (TPS) compares to that of other alternatives that are as of now input. With

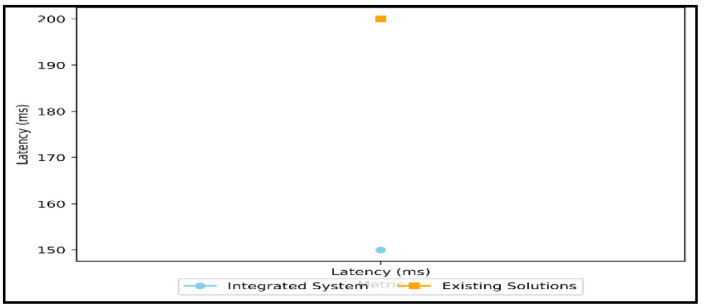


Figure 3

Representation of Latency comparison

120 TPS, the combined framework is much quicker than current solutions' 80 TPS, appearing a 50% enhancement within the speed of exchange handling. The truth that this change was made appears how well the blockchain and cryptography work together to handle more exchanges per moment, which makes it a more dependable way to control healthcare information.

This figure 3 appears how the slack is distinctive for the combined framework compared to other alternatives that are as of now out there. The idleness of the combined framework is 150 milliseconds, whereas the delay of current choices is 200 milliseconds. This lower delay implies that information is prepared and reactions are sent more rapidly, which is exceptionally vital for real-time healthcare apps. The way better delay execution appears that the combined framework can make it less demanding to get information and conversation to each other in healthcare systems.

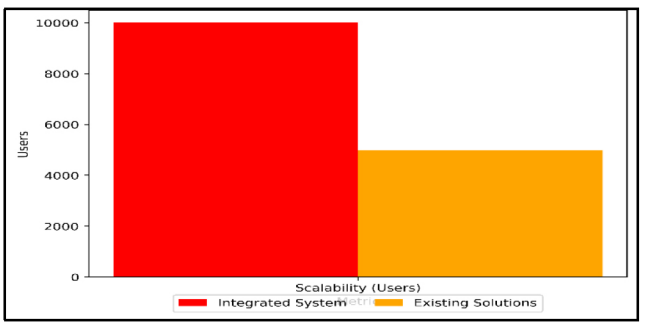


Figure 4

Representation of Scalability comparison

In terms of the number of individuals it can handle, the figure 4 appears how versatile the combined framework is compared to other choices. The combined framework can handle up to 10,000 clients, which is twice as numerous as the current alternatives, which can as it were handle 5,000 clients. This way better adaptability appears how solid and adaptable the combined framework is. It works well in big healthcare settings where allowing a growing number of people is important for quick data access and management.

7. Conclusion

Combining blockchain technology with encryption solutions is a completely new way to make sure that healthcare information is safe. This system uses the unchangeable and decentralized nature of blockchain along with strong security methods like AES and digital signatures to make sure that data is always correct, private, and only accessible to the right people. Traditional security measures aren't nearly as good as this system at stopping illegal entry, finding tampering, and supporting growth. This new system not only protects patient data from new online risks, but it also makes healthcare data management more trustworthy and open. Adopting blockchain and encryption technologies will be very important for keeping private medical data safe, making sure that regulations are followed, and delivering safe, effective healthcare as digital healthcare systems continue to develop.

References

[1] S. Baskar, K. Ramar, and H. Shanmugasundaram, "Data Security in Healthcare Using Blockchain Technology," in *Proc. 2021 Int. Conf. Decision Aid Sciences and Application (DASA)*, Sakheer, Bahrain, pp. 354–359 (2021).

[2] T.-L. Zhu and T.-H. Chen, "A Patient-Centric Key Management Protocol for Healthcare Information System Based on Blockchain," in *Proc. 2021 IEEE Conf. Dependable and Secure Computing (DSC)*, Aizuwakamatsu, Fukushima, Japan, pp. 1–5 (2021).

[3] B. R., V. D., B. E., V. C., and S. D. S., "Design of a Blockchain-Based Internet of Healthcare System Using Cryptography Network Security," in *Proc. 2024 Int. Conf. Science Technology Engineering and Management (ICSTEM)*, Coimbatore, India, pp. 1–6 (2024).

[4] M. Fartitchou, H. E. Marraki, L. Lafkir, A. Azzouz, K. E. Makkaoui, and Z. E. Allali, "Public-Key Cryptography Behind Blockchain Security," in *Proc. 2022 5th Int. Conf. Networking, Information Systems and Security (NISS)*, Bandung, Indonesia, pp. 1–5 (2022).

[5] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," *IEEE* (2019).

[6] S. Chakraborty, S. Aich, and H.-C. Kim, "A Secure Healthcare System Design Framework Using Blockchain Technology," in *Proc. Int. Conf. Advanced Communications Technology (ICACT)* (2019).

[7] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE* (2019).

[8] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology," *IEEE* (2020).

[9] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, "Blockchain Technology in Pharmaceutical Supply Chain: Ensuring Transparency, Traceability, and Security," *J. Stat. Manage. Syst.*, vol. 27, no. 2, pp. 417–428 (2024), doi: 10.47974/JSMS-1266.

[10] S. Rouhani, L. Butterworth, A. D. Simmons, D. G. Humphery, and R. Deters, "MediChainTM: A Secure Decentralized Medical Data Asset Management System," in *Proc. IEEE Int. Conf. Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber Physical and Social Computing (CPSCom), Smart Data (SmartData)*, pp. 1533–1538 (2018).

[11] M. Fartitchou, K. El Makkaoui, N. Kannouf, and Z. El Allali, "Security on Blockchain Technology," in *Proc. 3rd Int. Conf. Advanced Communication Technologies and Networking (CommNet)*, pp. 1–7 (2020).

[12] D. Dhabliya, S. Kunche, S. Dingankar, S. S. Dari, R. Dhabliya, and V. Khetani, "Blockchain Technology as a Paradigm for Enhancing Cyber Security in Distributed Systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 729–740 (2024), doi: 10.47974/JDMSC-1923.

Received November, 2024