International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

EVALUATION OF UTILIZING A MULTI OBJECTIVE FUZZY BASED HYBRID ALGORITHM TO SECURE HEALTHCARE DATA MANAGEMENT SYSTEMS VIA INTEGRATED CLOUD AND BLOCKCHAIN (ICBC) TECHNOLOGIES

***Amrutha [1], Sasi Kala Rani. K [2], Rabiyathul Bachiriya. M [3], Poongodai. A [4], Nithya Priya. S [5], Sunanda Das [6], Saravana Selvam. N[7], Priyanka More [8]**

[1]Assistant Professor, Department of Computer Science and Engineering, Mangalore Institute of Technology & Engineering, Mangalore, Karnataka, India, ammuaithal@gmail.com

[2]Professor, Department of Computer Science and Engineering, Alliance University, Bengaluru, Karnataka, India, sasikala.vetri@gmail.com

[3]Assistant Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamilnadu, India, rabiyathul07@psnacet.edu.in

[4]Assistant Professor, Department of Computer Science and Engineering (AI), Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh, India, a.poongodai@gmail.com

[5]Assistant Professor, Department of Mechatronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India, nithyapriya@skcet.ac.in

[6]Associate Professor, Department of CSE – Cyber Security, Jain (Deemed-to-be-University), Bengaluru, Karnataka, India, das.sunanda2012@gmail.com

[7] Professor, Department of Artificial Intelligence and Data Science, PSR Engineering College, Sivakasi, Tamilnadu, India, n.saravanaselvam@gmail.com

[8]Assistant Professor, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India, priyamore303@gmail.com

Abstract

The Internet of Things (IoT) generates massive volumes of patient and healthcare data every day. Providing the required accuracy for data classification, processing time, and analyzing the vast volumes of data from IoT devices and sensors are said to be the main challenges in IoT. Cloud computing is widely utilized as the foundation for the technologies required to secure healthcare. The healthcare industry has the most promise for blockchain technology since it can be used to integrate fragmented systems, the standard of electronic medical records should be raised, and take a more patient-centric approach to healthcare systems. The objective is to protect medical data, enable patients to use it to support their medical care, and provide reliable consent protocols for data exchange between various institutions and apps. Provide a blockchain-based architecture that verifies user identity using the Secure Hash Algorithm (SHA256) and Proof of

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Stake (POS) cryptography consensus technique to guarantee EHR sharing across many electronic healthcare systems.In this study, we assessed the performance of our proposed architecture using several metrics, and found that blockchain is a reliable security solution for the upcoming IoT network.

Keywords: Blockchain, Electronic Health Records (EHR), Ethereum, and Secure Hash Algorithm (SHA256).

INTRODUCTION

Security and privacy must be maintained when exchanging and storing medical records. [1]Numerous blockchain layers in the healthcare industry are shown in Figure 1.Technological innovations such as the Internet of Things (IoT), Industrial IoT, and big data have enabled the development of smart healthcare systems and the extension and innovation of healthcare around the world. [2] In the field of smart healthcare, Commonly used are EHR and cloud data that combine these EHRs with mobile IoT through IoT and communication devices to offer improved administrative services as well as medical and health services.

Although the smart healthcare industry has advanced quickly, security concerns persist.[3] Decentralization, networking design, confidentiality, tamper-evidence, auditability, and other capabilities offered by blockchain technology might be useful for supply-chain management, transactions, and data sharing.

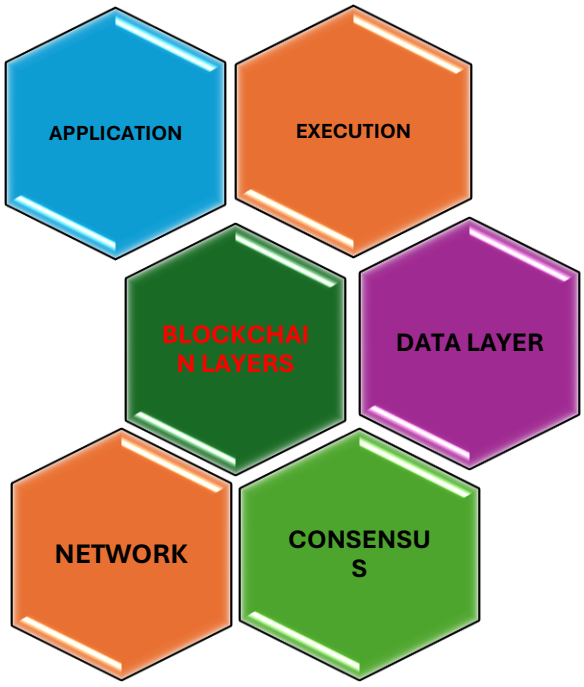

Fig 1: Layers of blockchain

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Blockchain and e-health together can enhance user-centered smart healthcare solutions and solve a number of problems with traditional healthcare solutions, including data security, privacy protection, and information sharing. [4]The data stored in the blockchain is extremely reliable and access through duplication, it has attracted the interest of entire corporate companies. However, there is not enough study on using blockchain in the healthcare industry. Maintaining information system security, creating sustainable supply chain platforms for smart healthcare, creating blockchain-based healthcare monitoring systems, and tracking operating environments for medical devices using the blockchain are the main topics of the majority of current blockchain research.

Blockchain is being marketed as a useful tool, particularly in the securing datas of healthcare, clinical science, health sciences, and insurance sectors, for retaining vitally important sensitive data.[5] Security lapses and secrecy in the medical field are increasing yearly. Now a days privacy of the data were very worst and data hacking are the biggest dangers of securing the medical records when the data is accessible on distributed platforms.[6] Using cryptographic tools and techniques, blockchain technology offers numerous ways to safeguard healthcare system records. Blockchain protects supply chain data, pregnancy records, and other sensitive medical information from cyberattacks.

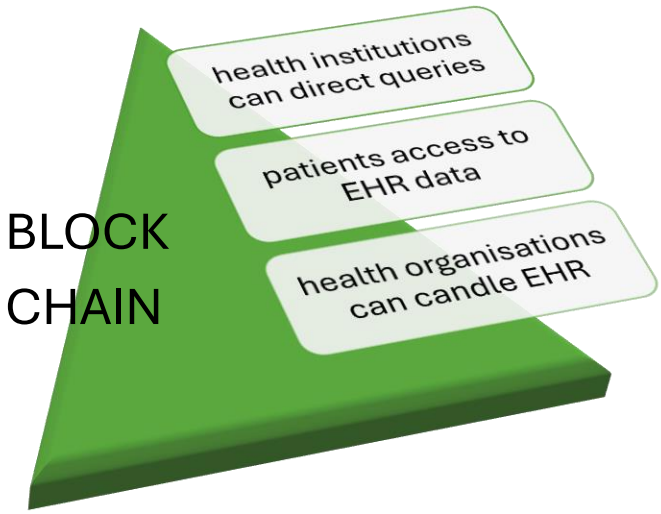

Fig 2: Blockchain uses for EHR.

The private blockchain is not sufficiently open and cannot be widely used because the majority of the data is held by large corporations. This study regulates the blockchain-based standardization of medical records. [7]The blockchain-based smart healthcare framework system that employs the chain method for transaction-level tasks to deliver data records to users or participants in order to reduce communication costs, computation costs, risks, and increase trust

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in blockchain technology.Using the benefits of blockchain technology, smart contracts can be used to securely and efficiently share and manage electronic health records. [8] The intelligent contract is one particular blockchain use in smart healthcare that is system-constrained and relies on medical record management. Utilizing the SHA256 method, we put the framework into practice.For efficient EHR sharing and storage, we select blockchain.

According to this report, Ethereum is a secure healthcare solution that integrates IoT and blockchain. Security, scalability, and processing speed are three important considerations in the system's architecture for remote patient monitoring, particularly for chronic illnesses that require continuous monitoring.

The contributions of this research are as follows

• In order to protect and authenticate the system for sharing health sector records, we suggest a blockchain-based structure.

• The major goal of our study is to use blockchain technology to safeguard the EHR and secure its sharing and storage in the cloud.

• To authenticate the integrity of the data, generate hash values using the SHA256 method and the POS consensus mechanism. In order to make data alterations impermeable, Here, the sensor is used to collect the data, which is subsequently stored on cloud computing-based storage.

LITERATURE REVIEW

In order to emphasize the present difficulties and lay a strong basis for future advancements, the study is to provide a comprehensive and insightful analysis of the current situation with relation to the integration of cloud innovations and blockchain. ANFIS's reliance on big data and the supply chain's lack of security and trust, the research's primary goals are to present hierarchical criteria of service supply chain performance to address the diagnosis of the issues' underlying causes, propose a distributed blockchain-based framework, and propose a smart learning model to address the uncertainty conditions by combining neural networks and fuzzy logic.

The proposed six-layer conceptual architecture also includes the data layer, connection layer, blockchain layer, smart layer, ANFIS layer, and application layer. In 2021, Bamakan et al. [9] As long as data security and integrity are preserved, it is also essential to further integrate blockchain security with cloud computing's dynamic potential.A valuable tool for analysts, experts, and collaborators who want to learn more about and advance the fusion of blockchain technology with cloud advances.Lopez, et al. (2024) [10] use the ProximaX blockchain platform to show how effective the suggested methodology is in decentralized networks. This study demonstrates that the suggested research framework is a secure, energy-efficient system that adjusts to changing circumstances.Venkatesan et al. (2024) [11] blockchain's promise to improve cloud computing's security, trust, and access control. This scholarly article also explores the emerging topic of blockchain-based access control systems and presents the findings of selected articles from various academic archives. Based on this thorough review of the literature, twelve different types of blockchain-based access control paradigms can be identified. Blockchain

Received: August 03, 2025

Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

technology study in access control systems is critically analyzed in this article, with an emphasis on the security, compatibility, and scalability issues by Irshad et al. (2024) [12].

The model based on the framework will be tested and evaluated using an action research design. Regression model analysis will be used as an assessment metric criterion to assess the model utilizing a fuzzy logic inference theory and expert judgment technique. Fuzzy logic-based user risk estimation strategies that cover severe, high, moderate, and low categories will be used to manage unclear data ranges. The AI data mining approach will be used for data collecting, and the sample size data sets will then be cleaned, pre-processed, and annotated. Omondi et al. (2024)[13] explained about the suggested method combines a decay algorithm with fuzzy reputation. After that, it determines each IoT user's quantifiable reputation value. This takes a number of factors, including the frequency of requests and the access request rate. Decisions about access control are based on this new reputation value. The efficiency of the suggested framework is assessed through extensive experiments and simulations. The performance of the suggested framework was then examined and contrasted with that of the current methods.Alqbaishi *et al.* (2024)[14]can also identify barriers that prevent the two concepts from being combined, such high energy usage, scalability issues, difficulties handling big data, etc. For different knowledge-defined networks in general, researchers have not yet looked into blockchain-based network solutions in a range of application areas which take into account the creation and sharing of information through a variety of methods like meta-heuristics, fuzzy logic, and machine learning by Wijesekara et al. (2023) [15].

PROPOSED METHOD

For all healthcare professionals and patients, we provide a secure Ethereum blockchain built on the architecture to handle and protect the demanding healthcare data. The suggested system is based on a cryptographic POS consensus approach. The main argument in favour of blockchain adoption is its immutability. Hyperledger uses the POS consensus technique to create private smart contracts that let two parties to exchange medical information.

This method reduces processing capacity and energy consumption while improving data privacy by isolating transactions. Figure 3 illustrates the suggested framework's design. The framework allows for the safe exchange and preservation of EHR between parties and stakeholders.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

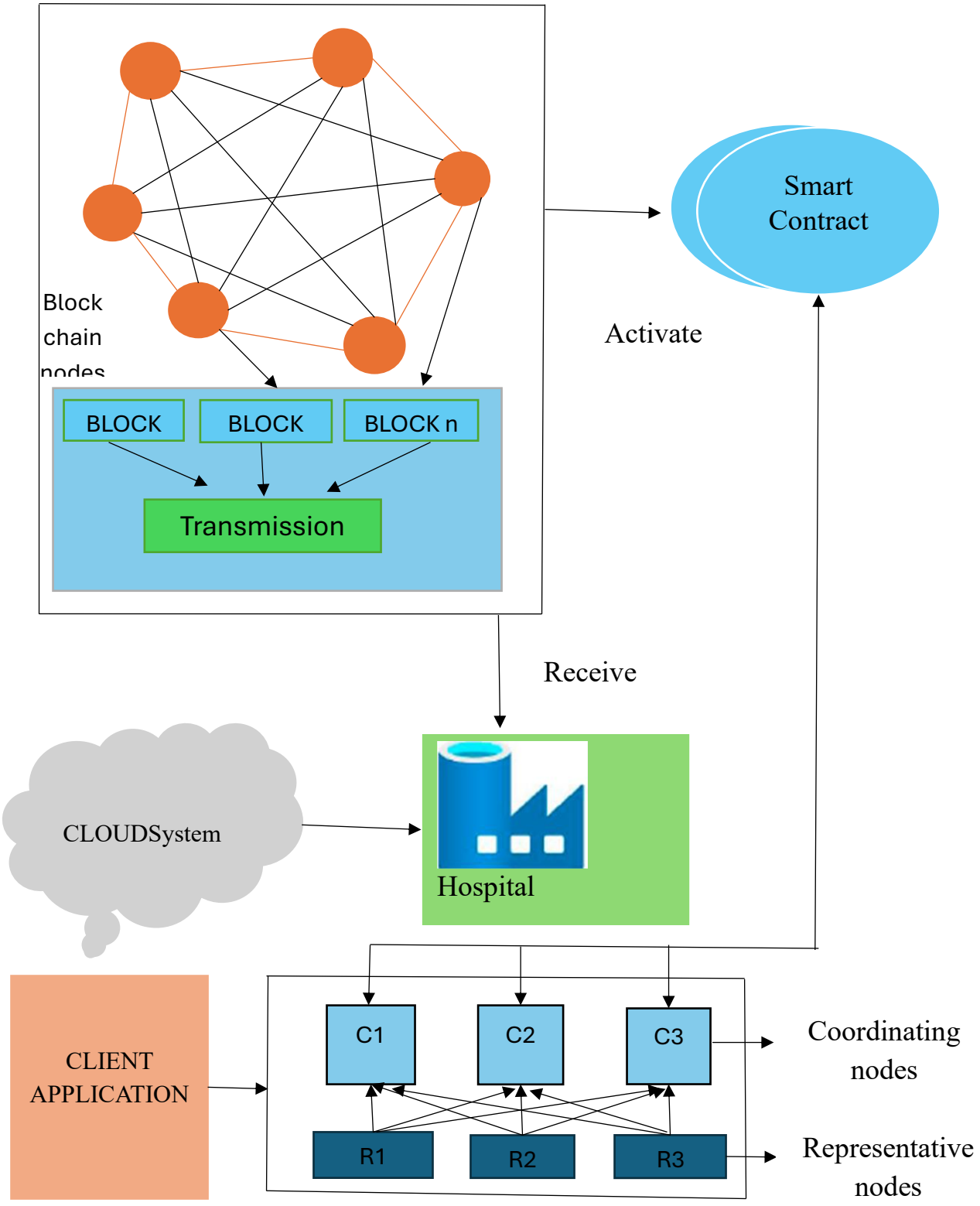

Fig 3: The proposed flow of cloud computing in Blockchain

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Data collection: Information from multiple sensors attached to the wearable device, including temperature, ECG, and blood pressure sensors, is collected for additional analysis and decision-making. Following data collection, preprocessing, noise reduction, and filtering are carried out.

Data security: Patient data gathered from sensors must be transmitted from gateway devices to the cloud. Therefore, when designing a framework for monitoring healthcare, it is necessary to take the security and integrity of such data into account. A watermarking and encryption process has been developed to safeguard the proposed architecture. During the encryption process, the data is changed into an unidentifiable format to prevent unauthorized access.

Data analysis: The patient's health data, which is kept on cloud servers and comprises pictures of the afflicted areas, descriptions of their symptoms, treatments, and treatment plans, is examined for future research in the field of clinical decision-making. These data could be subjected to a variety of machine learning algorithms and data visualization strategies to improve our comprehension.

Disease prognosis The diseases that a patient is likely to develop in the future can be predicted based on their age, height, weight, and ancestry. The correlation between the vital indicators can be used by machine learning to predict the proportion of expected disease.

An Ethereum-based decentralized network built on the blockchain. In the beginning, it was used on the popular cryptocurrency Blockchain. Ethereum's goal was to create an open-source smart contract platform that could be used with blockchain technology. Moreover, this technique uses peer-to-peer networking to propagate. Ethereum also makes the Solidity language available to programmers so they can build their own blockchains. It was created for smart contracts, the pinnacle of Ethereum technology. Transactions are the means by which Ethereum and outside parties interact. It allows external users to alter the state of a file or collection of data on the Ethereum blockchain network. The sender-author, who has a 20-byte address, and the recipient, who also has a 20-byte address, are some of the components that make up an Ethereum transaction.

A "smart contract" is a collection of instructions that may be used to accomplish any blockchain transaction. When users send transactions, this piece of code is run. Because they operate directly on the blockchain, they are impervious to change and manipulation. Any type of blockchain activity can be programmed using the programming language using smart contracts. Once the relevant operations have been programmed, the programmers can compile them. The Ethereum blockchain may then be used to compile, run, and deploy them. JavaScript is used to implement Ethereum's Solidity language in the smart contract code.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

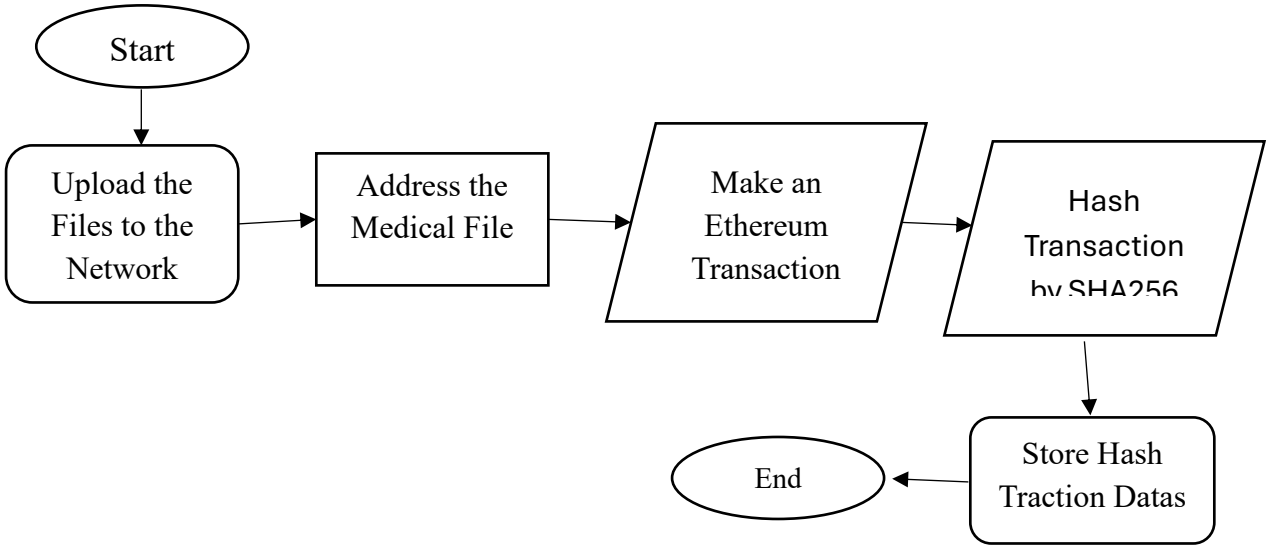

Fig 4: workflow diagram

Table 1: Description of the patient registration module.

INPUT	DESCRIPTION
Name	The patient's name that requires treatment is entered by the user.
Age	The patient's age in years.
Address	The patient's address
Mobile number	The patient's mobile number for communication.
Department referred	The patient is referred to the respective department based on the symptoms.
Gender	Gender of the patient (Male/Female/Other)

A number of nodes can join the network and securely exchange healthcare data thanks to the decentralised architecture. In general, errors and data loss are prevented by the suggested structure. In order to create a ledger of the previous transaction, nodes in the proposed architecture use the SHA256 cryptographic hash method, generate hashes, and need enough disc space to store hashes of all previous and subsequent transactions. The decentralised blockchain uses the secure hashing process.

Equation (1) describes the concept of One-way trapdoor functions are used to generate the hash value and are defined between two sets, such as X and Y. By dividing the power nth by the degree of a non-negative integer (n), this method finds the exponent (e) and the remainder of an integer base value (y).

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$f: x = y, with\ f(y) = x$

Where f is a trapdoor function that conceals some hidden information, and Equation (2) describes the function of hashing.

H=0,1^n, with H(P)

The blockchain algorithm combines transactions B with existing transaction blocks P using block hash (H). The computation and validation procedures for the transaction benefit from this method's assistance in maintaining track of previous transactions. Cloud management is used to save the EHR data in the cloud.

$a^3 = b^3 + ya + x$

The cryptographic technology ensures that only authorized nodes can share data because it is based on the hash value. Equation (4) has been applied to combine the hashes of the preceding and next blocks. The terms in the equations represent hash blocks that hold confidential data.

y=$((a_2 - b_2)/(a_1 - b_1) mod$

$x = (a_2 - b_2)/(a_1 - b_1) mod$

The network's necessary services are requested by the visiting nodes. Client node requests are managed by agent nodes, who also offer authentication services prior to acceptance. Nodes serving as coordinators verify approval and accept or reject requests for additional processing. Administrator nodes process transactions into frames after receiving authenticated requests from a number of coordinator nodes. They then forward the newly produced frames to contributors and coordinators in the vicinity for additional network distribution. The updated state is started across the network using this manner.

Algorithm 1 SHA256

1. Add a 64-bit length from the collected data until it reaches 512 bits, then raise the number of 0 bits in the data input until it reaches 448 bit.
2. Divide the 512 bit data into 16 groups after it has been merged : $M_O - M_{15}$
3. Set up the vectors $K_O - K_{65}$ and $h_O - h_7$
4. The following initial values: h0–h7
   Computation
5. Set t loop from 0 to 63, then update as follows : $B_{t+1} - A_t$

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

RESULTS AND DISCUSSION

A further decision will be made based on the patient's health condition. Numerous diseases are automatically detected and tracked using the classification models. When the sorts of data vary from patient to patient, the transfer-learning method is employed to ensure optimal performance.

Table 2: Security problems

Security problem	**%**
Authentication	81%
Communication	70%

Because it will take a lot of computing power to reverse, the hashing method and the compression feature will stop hackers from obtaining the data. The algorithm is also immune to the second-pre image. It will fail if the attacker attempts to substitute a valid value for the input after already obtaining it from the hash. Before the doctor begins creating a block, the system checks the patient's balance to make sure they have the money they stated.

Table 3: Transaction

User name	Wallet address	Balance
Name	**********	Rupees

The system generates the block and hashes it using the transaction's data and the previous hash when the doctor approves the transaction. The physician then begins responding to the patient.

Table 4: Receiving Transaction

User name	**Data sent**	**Offered money**	**User received**
Name	25 degree	Rupees	Doctor Name

It won't be possible to find a different input for the same hash. Given that the attacker is unable to distinguish between two unique or identical items in the hash, there are no collisions. There is no chance of getting duplicate inputs or two distinct inputs. A mixture of SHA-256 is computed intensively by the method.

Values, including the patient's insurance information, are entered into seven text boxes. Here, the value of one textbox is first converted to binary format and concatenated with the hashing constant; after the concatenation, the values of the other six cases are appended and entered into the compression function, which produces the final digest. The information is encrypted into a 256-bit hash value that can only be utilised for the private purposes of the healthcare system after it has been submitted into the text areas.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 5: Implementation of the SHA-256 algorithm

Details	
Name of the insurance	**********
Patient name	**********
Agent name	**********
Date of birth	**********
Policy no	**********
Validation	**********
Secured data	**********

All of the parameters are contained in the database as columns. The web application's data is linked to the database via a gateway. A stored procedure in the database is triggered when the web application's data arrives to the database server.

Secure Hash Algorithm-256 generates distinct hash values for sensitive data, ensuring the validity and integrity of the data in the proposed system. Secure Hash Algorithm-256 improves security by preventing unauthorised access or change and ensuring data integrity during transmission and storage. Integrating SHA reduces the possibility of unwanted access or alteration while protecting patient privacy and data integrity.The Secure Hash Algorithm-256 is a well-liked cryptographic hash function for data security and integrity. The suggested healthcare system improves security and privacy in wireless medical sensor networks by utilising distributed architecture and SHA-256, a specific form that produces a fixed-size 256-bit hash value, guaranteeing private data transit and storage.

Table 6: Parameters

Parameters	
Smart contract	Yes
Data secure	Medical data
Scalability	High
Level of decentralisation	High
Data privacy	Yes
Transaction details	Yes
Time complexity	n-1
Space complexity	n

For network monitoring and control, compile comprehensive information about every sensor node, including status and health data. Use decryption for statistical analysis after securely accessing and decrypting files from sensor nodes. To connect to nodes and servers in the wireless

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

medical sensor network, establish a secure link. Upload and Encrypt: To ensure integrity and confidentiality, divide sensor data, encrypt it using techniques, and then upload it safely to designated servers.

4.1. Performance measures

The parametric measurements that are used to confirm the performance results of the proposed blockchain technology employing a verified secure hash approach are block time and total execution time. The amount of time needed to mine data for each block is referred to as block time. Usually independent of the commencement time, but frequently dependent on the input data, the total execution time, also referred to as the CPU time, is the total amount of time required to complete the process.

Table 7: Block generation time

No. of blocks	Block chain memory (Mb)	Block generation time(sec)
50	0.281	0.92
100	0.283	1.97
200	0.288	2.64
300	0.284	5.98
400	0.285	7.93
500	0.286	9.96

From 50 to 500 blocks, the block creation time is represented graphically as varying linearly: when the blockchain memory is increased to 0.281Mb, the block generation time also increases to 9.96, indicating that the block generation time will increase if the number of blocks also increases.

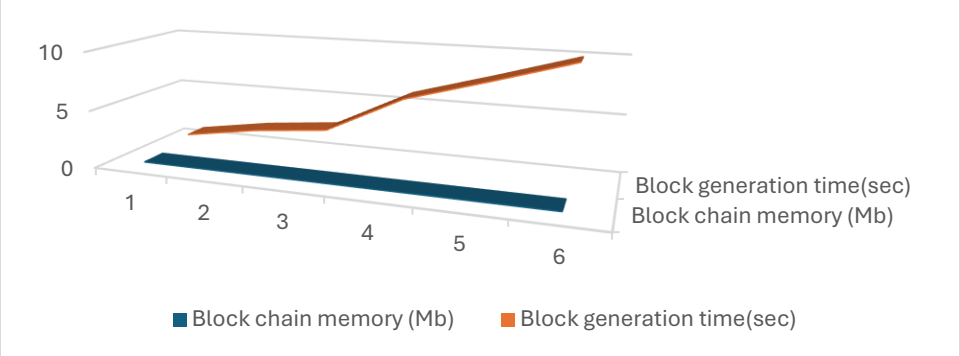

Fig 5: Graphical representation of block generation time

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The performance outcome of the suggested SHA256 algorithm with a verified secret key algorithm was measured in terms of total execution, block production, and blockchain memory. There are between 50 and 500 blocks, and when the number of blocks changes, more data will be embedded, increasing the blockchain's memory.

Table 8: No. of blocks with respect to total execution time

No. of blocks	Total Execution Time(Sec)
50	58.96
100	61.88
200	63.84
300	64.85
400	69.85
500	74.91

As the number of blocks increases, so does the system's overall execution time. The overall execution time, expressed in seconds, varies from 58.96s to 74.91s as the number of blocks increases from 50 to 500.

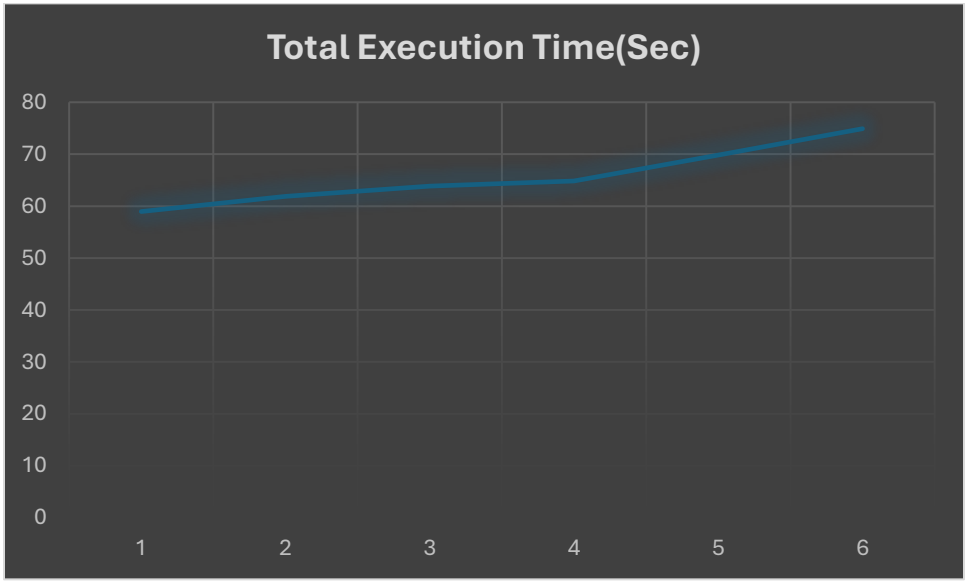

Fig 6: Graphical representation of Total Execution Time

The quantitative analysis of the suggested SHA 256 cryptographic scheme is displayed in Table 8 as a number of blocks divided by the total execution time (secs).

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CONCLUSION

By safeguarding patient privacy and enhancing security against insider attacks in wireless medical sensor networks, this research offers a fresh approach to healthcare. The user-friendly interfaces, smooth networking, and efficient data management enable the balanced solution that enhances security without sacrificing usability, which in turn enhances patient care and the efficacy of healthcare. A feasible approach that allows one to build upon standardized auditing, certain defined contracts for data access, and SHA256 cryptographic techniques to ensure data integrity is the proposed Blockchain-based solution. The recommended SHA 256 was suitable for healthcare systems that use EHRs since it provides superior security and efficient protection compared to other related schemes like Smart-Contract Ethereum and Searchable Encryption. One benefit of the recommended SHA 256 technique is that it uses a verifiable key, which makes it challenging for hackers to decipher the contents from the hash result.

REFERENCES

1. Wijesekara, Patikiri Arachchige Don Shehan Nilmantha, and Subodha Gunawardena. "A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges." *Network* 3, no. 3 (2023): 343-421.
2. Guo, Hao, Wanxin Li, Mark Nejad, and Chien-Chung Shen. "A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms." *IEEE Transactions on Network and Service Management* 20, no. 2 (2022): 1759-1774.
3. Upadrista, Venkatesh, Sajid Nazir, and HuagloryTianfield. "Secure data sharing with blockchain for remote health monitoring applications: a review." *Journal of Reliable Intelligent Environments* 9, no. 3 (2023): 349-368.
4. Jabbar, Rateb, Eya Dhib, Ahmed Ben Said, Moez Krichen, Noora Fetais, Esmat Zaidan, and Kamel Barkaoui. "Blockchain technology for intelligent transportation systems: A systematic literature review." *IEEE Access* 10 (2022): 20995-21031.
5. Javed, Mannan, Noshina Tariq, Muhammad Ashraf, Farrukh Aslam Khan, Muhammad Asim, and Muhammad Imran. "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework." *Sensors* 23, no. 23 (2023): 9372.
6. Qi, Minfeng, Ziyuan Wang, Qing-Long Han, Jun Zhang, Shiping Chen, and Yang Xiang. "Privacy protection for blockchain-based healthcare IoT systems: A survey." *IEEE/CAA Journal of Automatica Sinica* (2022).
7. Issa, Wael, Nour Moustafa, Benjamin Turnbull, Nasrin Sohrabi, and Zahir Tari. "Blockchain-based federated learning for securing internet of things: A comprehensive survey." *ACM Computing Surveys* 55, no. 9 (2023): 1-43.

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

8. Demirbaga, Umit, and Gagangeet Singh Aujla. "MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem." *IEEE Transactions on Network and Service Management* 19, no. 4 (2022): 3896-3907.
9. Bamakan, Seyed Mojtaba Hosseini, Najmeh Faregh, and Ahad ZareRavasan. "Di-ANFIS: an integrated blockchain–IoT–big data-enabled framework for evaluating service supply chain performance." *Journal of Computational Design and Engineering* 8, no. 2 (2021): 676-690.
10. Irshad, Reyazur Rashid, Zakir Hussain, Ihtisham Hussain, Shahid Hussain, Ehtisham Asghar, Ibrahim M. Alwayle, Khaled M. Alalayah, Adil Yousif, and Awad Ali. "Enhancing cloud-based inventory management: A hybrid blockchain approach with generative adversarial network and elliptic curve diffiehelman techniques." *IEEE Access* 12 (2024): 25917-25932.
11. Omondi, Alan Odhiambo, Erick Oteyo Obare, and Samuel Oonge. "Adaptive Fuzzy Logic Risk-Based Access Control Model for Smart Contract Execution on Block Chain Systems."
12. Lopez, Leonardo Juan Ramirez, David Millan Mayorga, Luis Hernando Martinez Poveda, Andres Felipe Carbonell Amaya, and Wilson Rojas Reales. "Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review." *Computers* 13, no. 6 (2024): 152.
13. Venkatesan, K., and Syarifah Bahiyah Rahayu. "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques." *Scientific Reports* 14, no. 1 (2024): 1149.
14. Alqbaishi, Arwa A., and Alaa ES Ahmed. "Reputation evaluation using fuzzy logic for Blockchain-Based access control in an IoT environment." *IEEE Access* (2024).
15. Wijesekara, Patikiri Arachchige Don Shehan Nilmantha, and Subodha Gunawardena. "A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges." *Network* 3, no. 3 (2023): 343-421.

Received: August 03, 2025