Enhancing IoT Healthcare Security: A Blockchain and AES-Based Framework for Secure Data Transmission and Management

MSc Cyber Security

Vigneswaran Moorthy
Student ID: x23198311

School of Computing
National College of Ireland

Supervisor: Diego Lugones

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Vigneswaran Moorthy ………………………………………………………………………………

Student ID: X23198311@student.ncirl.ie……………………………………………………………..……

Programme: MSc CyberSecurity……………………………………… **Year:** 2024………………..

Module: MSc Research Project ………………………………………………………………..………

Supervisor: Diego Lugones
…….………

Submission Due Date: 29/01/2025
…….………

Project Title: Enhancing IoT Healthcare Security: A Blockchain and AES-Based Framework for Secure Data Transmission and Management……….………

Word Count: ……8226……………………………… **Page Count**………22…………………………..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Vigneswaran Moorthy……………………………………………………

Date: 29/01/2025………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing IoT Healthcare Security: A Blockchain and AES-Based Framework for Secure Data Transmission and Management

Vigneswaran Moorthy
x23198311

Abstract

The increasing trend of Internet of Things (IoT) in healthcare systems has brought up many concerns related to data security and privacy. The existing approaches suffer from efficiency, scalability, and proper protection against unauthorized access. This paper introduces an advanced framework that combines blockchain technology with AES-256 encryption and the MIDC (Monitoring, Integrity, Data Control) framework to address these challenges. The key goals of the framework are to increase data security, integrity, reduce unauthorized access, and automate the access control process using smart contracts. The model is compliant with the regulations of GDPR and HIPAA, thereby meeting the requirements of data privacy standards. The proposed system was compared with the existing encryption techniques and showed superior performance in terms of reducing the encryption time to 3.0 seconds, decryption time to 2.8 seconds, and buffer time to 0.140 MB. These results indicate the efficiency of the model in processing IoT healthcare data, which is better in terms of speed and resource utilization than traditional AES-256 and hybrid encryption models. The smart contracts enable role-based access control, making it easier to manage data-sharing policies and ensuring safe, automated access to data. Despite its promising performance, one challenge remains in the energy optimization of blockchain-based systems with regard to scalability and sustainability. Future work will go towards this challenge in such a way that further optimization of the model will be performed not at the cost of the security. This framework gives rise to a robust solution to securing the IoT healthcare systems with many great benefits in real-world applications, primarily in resource-constrained environments such as healthcare IoT devices.

Keywords: *AES-256, Blockchain, Data Integrity, IoT Healthcare, Smart Contracts*

1 Introduction

1.1 Research Background

The arrival of the Internet of Things (IoT) has carried about transformative advancements in various sectors, with healthcare being one of the most impacted domains. Since most of the gadgets in our environment are connected to one another to exchange information, the globe has shrunk to the size of a tiny city in the era of the Internet(Haghi Kashani *et al.*, 2021). Recent advancements in a number of wireless technologies, have made it easier, simpler, and less expensive to connect various devices to the Internet. The IoT represents the seamless integration of the physical world with digital networks(Tran-Dang and Kim, 2021). The Internet is essentially a vast network that lets billions of devices, including computers and smartphones, as well as household appliances and industrial equipment, communicate with each other in real-time(Li *et al.,* 2022).

Healthcare systems which can be referred to as the Internet of Medical Things (IoMT) have enabled unprecedented connectivity between patients, healthcare providers, and medical devices. These systems help achieve concepts such as remote patient monitoring, real-time data analysis and driven decision support, and enable more innovative as well as effective patient care. However, when more and more health care organizations opt for IoT solutions, this leads to new problems, primarily in protecting patient data and the reliability of medical systems(Lee and Sim, 2021). The healthcare industry has benefited from the use of these technologies in several ways. The expansion of IoT devices raises additional security and privacy issues since it increases the volume of data processed by the internet. In order to solve the various difficult problems in the latest IoT-based smart healthcare strategies, a green solution is needed (Tensae Laki *et al.*, 2024).

The blockchain technology, decentralized, immutable, and transparent, it has emerged as a promising solution to overcome the security challenges(Naresh, Reddi and Allavarpu, 2021). A more sophisticated and dependable paradigm than centralized database security is provided by blockchain security. Blockchain maintains a record of documents that are securely linked to previous blocks through the use of cryptographic hash methods. One kind of distributed ledger used to keep track of transactions and stop fraud is a blockchain. Typically operated through a peer-to-peer network, the Blockchain is made especially to guard against unauthorized tampering. Thus, from a managerial standpoint, Blockchain can provide security features comparable to those in central database storage, thus preventing possible assaults and data breaches.

A network governs the IoT, and hackers may do a variety of harm to linked devices with inadequate security. Vulnerabilities include outdated platforms, easy encryption patterns, infrequent password changes, a lack of encryption techniques, and unsecure network connections. By exploiting these flaws, financial harm can be inflicted by stealing personal data, and secondary harm like invasions of privacy can also be brought about by recognizing patterns of behavior. Because there are more single-person households nowadays, the privacy invasion issue is becoming more significant. In addition, the IoT's vulnerability is continuously increasing. Symmetric key techniques like the AES (Advanced Encryption Standard) and Secure Hash Algorithm have been developed to solve this issue(Shakor *et al.*, 2024).

1.2 Problem Definition

One of the major security gaps is the unauthorized access to the data, integrity concerns of the data, and vulnerabilities toward malicious attacks in IoT-based healthcare systems(Mohammed Sadeeq *et al.*, 2021). Traditional models, especially those that focus on centralized control, generally do not provide the kind of resilience needed against the above threats because of a point of failure, scalability limits, and susceptibility to targeted attacks. A distributed ledger system eliminates the need for centralized authorities while ensuring secure, verifiable, and tamper-resistant data storage and transmission. The use of smart contracts embedded within the blockchain ensures the automatic processing of events, thus ensuring efficiency and reliability(Ullah *et al.*, 2021). However, despite these advantages, the implementation of blockchain in IoT healthcare poses challenges such as high computational demands, latency, and scalability limitations. These gaps will be filled by the proposed model integrating blockchain technology with AES encryption. Here, blockchain technology can use its decentralized nature to avoid any single points of failure; hence, health care data will be stored in a tamper-proof and transparent manner. Also, AES encryption ensures strong data protection during transmission with regard to confidentiality and integrity. The Figure 1 shows how Blockchain -privacy preservation in the IoMT is given below.

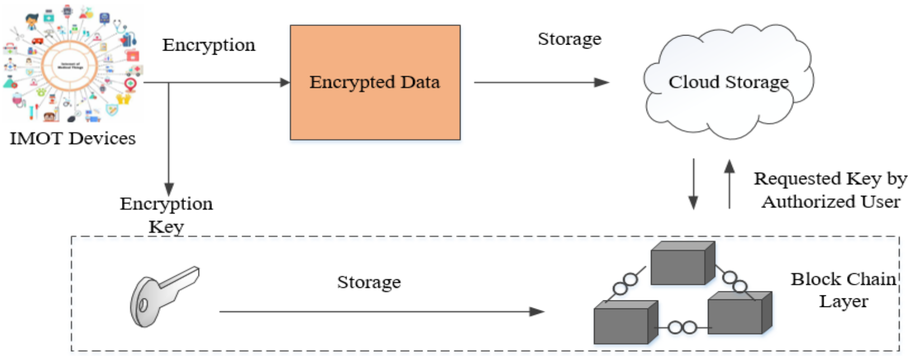

Figure 1: Block Chain Based Privacy Preservation for IoMT

Research Question 1. What is an effective approach to enhance security in IoT healthcare systems through the integration of Blockchain and AES encryption for secure data transmission and management?

The expansion of IoT in the healthcare infrastructure has brought into the projection several new opportunities in health care, management, monitoring, and patient satisfaction(Shakor *et al.*, 2024). These factors make IoT health care networks and systems centralized repositories for many significant medical data and typically attract hackers to attack them by breaking into their security systems to access the desired data or imposing DoS attacks on the targets. In particular, the systems where it is necessary to understand that to ensure the security and control of the increasing amount of data, generated by wearables, medical sensors, and other connected devices, it is needed to create proper security measures(Tensae Laki *et al.*, 2024). The problems of protection healthcare IoT systems have led to the quest for new methods for the effective protection of such systems from hacking but also for data confidentiality and data authenticity. A major challenge raised is how to safeguard data, manipulation and malicious activities that would lockout patients from accessing their usually needed healthcare services. AES Encryption has been suggested as the solution to the above security risks while the use of block-chain has also been suggested as a solution to these problems. , blockchain is decentralized, with immutability, providing additional security and implementation of chain of custody while AES offers data encryption to secure the data during transfer(Naresh, Reddi and Allavarpu, 2021).

This paper proposes a novel solution, namely a Blockchain and AES-based architecture, which is intended to greatly improve the security of IoT healthcare devices. The proposed framework of this paper aims to harnesses Blockchain technology for secure and transparent storage of records of health care system with every process that takes place in a blockchain being recorded in a Blockchain as a historical document that cannot be altered. The contributions include:

- Proposing a secure data management approach for IoT healthcare devices through innovating blockchain with AES encryption.
- Aiding the resilience of data transport by means of guaranteeing security and accuracy as well as verifying the sender and the data origin.
- Improving the IoT health care apps scalability by integrating decentralized data storage so as to make it more secure and transparent.

Section 1 introduces the research context concerning security challenges in IoT health care systems by way of discussing unauthorized access breaches, privacy issues, etc., then Section 2 presents to reviewing extant literature on the healthcare IoT security, Section 3 setting up a foundation for the proposed security framework. Section 5, system design and implementation specification is given, It integrates concepts of IoT data collection, AES-256 encryption, MIDC, and blockchain into smart contracts with provisions of access control and compliance. Section 6 provides the evaluation of the system. Conclusion and Discussion at Section 7 and finally reference list are provided at Section 8.

2 Literature Survey

2.1 IoT-based Security Solutions in Healthcare

A Timestamp-built Secret Key Generation (T-SKG) technique was presented by Saif et al.(2024) for devices with limited resources. It eliminates direct key exchange and reduces the danger of key compromise by producing a secret key at the device of patient and redeveloping it at the device of doctor. The robustness of the T-SKG system against guessing and brute force assaults is demonstrated by results using MATLAB and Java. In particular, if the attacker is aware of the key series pattern, the likelihood of a key compromise in an assuming assault is just 9%, and the scheme is safe from forceful attack and birthday attacks for a certain amount of time. Health vitals obtained with the MySignals sensor kit are securely sent via the T-SKG system, which is linked into a medical sysem. The DES with several Cipher Block modes is used for secrecy. Exploration of other cryptographic techniques is needed, as the emphasis on prevalent security attacks ignores new dangers. Scalability issues are also raised by the expanding amount and variety of health data.

The T-SKG technique effectively mitigates some of the key compromise risks and resource limitations as it facilitates local generation and regeneration of keys. However, its use of DES makes it unsuitable for long term as it is legacy and prone to advanced attacks. Investigating advanced cryptographic techniques as well as adaptive security principles would be necessary for optimal, long-term implementation. The methodology fails to consider side-channel attacks and does not mitigate the scaling issues associated with increased health data.

The BSDMF effectively utilizes blockchain for scalability, data security, and trust in IoMT. Nonetheless, the computational and storage overhead associated with blockchain restrict its usage on resource-constrained IoMT devices. Future work will focus on lightweight blockchain solutions or the hybrid model to overcome these limitations. It also misses addressing the scalability and energy efficiency-related challenges within blockchain, which would be crucial if IoMT was to be used in handling increasing healthcare data.

For ongoing cardiovascular health monitoring, the Xu (2020) study proposes an IoT-aided ECG observing platform with secured data communication. It has been recommended to design and deploy a light ECG Signal Strength Test for real-time deployment and machine-based classification. LAC and LS-IoT have been suggested for the secure data transfer. The analysis and validation are executed in real time on the obtained ECG signals from the MIT-BIH and Physio Net Challenge databases as well as for ECG signals for various exercises. The IoT-assisted ECG tracking model can therefore be used to determine the medical acceptance of ECG signals to increase the efficacy of the diagnostic system. One drawback of the study is that it identifies severe corruption of ECG signals during increased physical activities but does not provide robust mitigation strategies to address this issue.

The study makes an innovative IoT-aided ECG observing platform with safe data communication that contributes to real-time analysis and automated categorization. However, the robustness in mitigating the severe corruption of ECG signals during physical activities might be lacking, making it a critical limitation. LAC and LS-IoT provide security enhancements. Nevertheless, addressing corruption in dynamic environments is the crucial gap that requires attention. Overall, the study offers promising advancements but requires improvements in handling data quality under physical stress.

This method by gives a promising solution in a Zero Knowledge Proof and Ethereum smart contracts for safe data communication for IoT healthcare schemes, with high accuracy in intrusion detection. However, reliance on Ethereum blockchain storage and IPFS introduces scalability concerns, such as bottlenecks in performance, including high transaction costs and potential latency in accessing data. While the BiLSTM-DSA is doing superior intrusion detection, scalability issues of these limit the approach's practical applicability in large-scale systems. Therefore, storage and transaction handling optimization is essential for real-world deployment.

This framework yields significant improvements in the throughput, efficiency in terms of energy consumption and security attributes of e-healthcare systems. However, this might get compromised in mobility-based medical applications due to the dynamic variation of sensor positions, which may cause both energy efficiency and security trade-offs. The success of these practical use cases would necessitate achieving enhancement in real-time adaptability of sensor movement. The framework's performance improvements are promising, but it remains challenging to address the dynamic characteristics of mobile healthcare environments in order for the framework to achieve broader applicability.

The process in the Khan et al.(2020) secured framework initiates with patient verification, tailed by the initiation of the patient's sensor device and the transmission of the patient's sensor readings to the cloud server. Along with the user name and password, a parameter containing the patient's biometric data has been introduced. The integrity-ensuring SHA-512 algorithm was used in the creation of the authentication method. The technique uses enhanced Elliptical Curve Cryptography (IECC) and the Substitution-Ceaser cipher to securely transmit the sensor data. In contrast, an extra key (secret key) is created in enhanced ECC to strengthen system security. An analysis of the relationship between plaintext and cipher text is conducted statistically, and the average correlation coefficient of 0.045 shows the strength of the suggested scheme. A major limitation of the framework is that though it enhances security through an extra secret key in the advanced ECC scheme, the overhead added in two phases may add unnecessary computational delay in resource-scarce devices such as the IoT-based medical sensors.

The framework notably enhances the security of IoT-based healthcare systems with strong encryption techniques such as enhanced ECC and SHA-512, having low encryption/decryption times. However, the introduction of an additional secret key within the ECC scheme would while extending security defeat the purpose in this scenario by causing unwanted delays in computation even in resource-constrained devices such as IoT sensors. Therefore, the balance of security efficiency for IoT devices needs to be optimized for better system performance. This added complexity may make it more difficult for the framework to be applied in real-time applications, especially where latency is strongly considered.

A lightweight hybrid FL framework was presented by Rahman et al. (2020), in which blockchain smart contracts regulate the authorization of engaging federated nodes, the trust management, the edge training plan, the reputation of edge nodes and the data sets or models they upload, and the delivery of globally or locally trained models. Additionally supported by the framework are the inferencing procedure, model training, and complete dataset encryption. The blockchain aggregates the new model parameters via multiplicative encryption, while each federated edge node carries out additive encryption. The framework provides lightweight DP to ensure complete privacy and anonymization of the IoHT data. Several DL applications created for COVID-19 clinical trials were used to evaluate this technology. One major limitation of the lightweight hybrid federated learning framework is its dependency on blockchain for trust management and model aggregation, which become a source of bottleneck and performance issue.

The light hybrid FL framework effectively integrates blockchain for trust management, model aggregation, and privacy, which should be promising for applications such as COVID-19 clinical trials. However, if the framework depends on blockchain processes, this might actually create a potential bottleneck and reduce its scalability and performance in its use with federated nodes. The framework is privacy-preserving through encryption, but the complexity of the blockchain may stand in the way of real-time efficiency. Performance in relation to security evidently has to be optimized further for its practical applicability.

The work proposed a robust energy-efficient IoT framework to secure e-health data leveraging compressive identifying and five-dimensional hyper-chaotic map to perform encryption. An innovative θ-NSGA-III optimization improves FDHC properties to outperform advanced methods for image encryption. However, the dependency of tuning the hyper-parameters for the FDHC map adds computational complexity and hampers the scalability and real-time application of such a system in the dynamic IoT environment. While promising for secure communication in green IoT networks, addressing this limitation is essential for broader adoption.

The paper puts forward new security and privacy mechanisms for the IoMT, including RECC-VC and IENN, and attains an accuracy of 96% and safety level of 98%. Incorporation of blockchain with optimized Gaussian mutated chimp further strengthens data protection and sensitivity assessment. However, the introduction of computational overhead by these advanced techniques presents challenges toward the application in real-time and scalability in any resource-constrained IoMT environment. The approach is promising, but optimization for efficiency in constrained settings remains a key area to improve.

In their article, Egala et al.(2021) offered a unique Blockchain-based architecture that offers smart-contract-based service automation and a decentralized EHR without sacrificing system security or privacy. This solution combines a DDSS with a hybrid computing paradigm to overwhelm the drawbacks of a cloud-centric based on block chain IoMT healthcare systems. The proposed systems security features include device authentication, patient record anonymity algorithms, and a decentralized SRAC mechanism. Experiments show that the Fortified-Chain based H-CPS offers decentralization of automated control of access, security, and privacy while using less storage and responding in milliseconds or less than the typical centralized H-CPS. The scalability and accessibility for smaller healthcare providers with limited technical infrastructure is the main drawback.

A novel blockchain-based architecture coupled with smart contracts and hybrid computing paradigm was proposed to provide an assured platform regarding security, privacy, as well as automation in IoMT healthcare systems. In this regard, SRAC and anonymity algorithms further enhance the system's security features. The main drawbacks are related to its scalability and accessibility for smaller healthcare providers, which limits the deployment range. Overall, while the design is robust and efficient, infrastructure issues need to be overcome before this can be widely adopted.

The reviewed literatures present comprehensive advancement in the secure and efficient transmission of data through IoT-enabled healthcare systems, using various techniques such as blockchain, federated learning, cryptographic frameworks, and IoT-specific adaptations. For example, T-SKG and BSDMF approaches show improvements in security and scalability. However, legacy cryptographic method usage and blockchain overhead pose challenging issues in resource-constrained environments. Some advanced methods like RECC-VC and FDHC encoding methods emphasize the precision and security aspects but involve various computational complexities that limit scalability as well as real-time applications. Solutions with machine learning, such as BDSDT and IENN, have achieved high precision in intrusion detection sensitivity assessment but still suffer from performance trade-offs in dynamic environments. Common shortfalls across the studies span inadequate treatment of scalability, energy efficiency, and robustness in handling mobile or high-stress environments, focusing on lightweight, adaptive frameworks that balance security, efficiency, and practical applicability.

3 Research Gap

The baseline papers focus on encryption techniques such as ABE, Hybrid AES, and Traditional AES-256 to secure IoT healthcare systems. ABE suffers from a problem of computational inefficiency and scalability. AES suffers from high computational overhead and is problematic in terms of key management. Traditional AES-256 is strong but vulnerable to side-channel attacks and lacks key-sharing mechanisms. Based on these, this research proposes a framework that integrates Blockchain and AES-256 with the MIDC framework to counter the aforementioned limitations. It uses AES-256 to optimize multi-word encryption and improves performance metrics, along with enhancing security by utilizing blockchain's decentralized architecture in conjunction with the MIDC framework and smart contract-based access control.

4 Research Methodology

This experimental setup integrates blockchain technology and AES-256 encryption for securing IoT healthcare data effectively, thus forming a robust and scalable security framework. The system is designed to address some of the challenges such as unauthorized access, data integrity, and privacy that are critical in handling sensitive healthcare information. The following are some of the key components of the system.

4.1 IoT Healthcare Devices -Data Collection

The system receives periodic physiological data about the patients by employing a kit of IoT healthcare wearables such as heart rate, glucose level sensors and fitness trackers. Those sensors are wired to the devices with the idea of monitoring specifications of vital sign, activity, or often health concerns at that time.

To address this issue, these devices are also connected wirelessly, to a base unit via some form of secure data transmission links like wireless or Bluetooth. The main hub works as a collector which collect data from various IoT devices and organizes them for further analysis. This configuration also helps in collection of good data without the occurrence of loss of data during transfer. However, wearable devices are powered, optimized for low power consumption with high accuracy for long term health monitoring usage.

4.2 Data Pre-Processing

Data cleaning is very important here, in order to filter the data collected and make sure that the data to be used is clean and secure. This will comprise of actions where the accuracy of the data gathered will be checked or establish if the data gathered is complete. In the current study, in cases where there appeared to be missing values, duplications or even erroneous entries such were dealt with at this point. The data is then validated, and then normalized into a format such as JSON or CSV so that it may work in harmony with the current encryption and storage system of the programme. For privacy concerns and meeting general data protection regulation or health insurance portability and accountability act (GDPR/ HIPAA), PII is obfuscated by either stripping off or masking of invariant elements. This all-around approach protects the patient data and optimizes it for safe transmission, encryption as well as storage in the blockchain based healthcare system.

5 Design and Implementation Specifications

5.1 System Workflow

Figure 2 shows the system workflow for healthcare data security using blockchain and MIDC AES-256 encryption represents the secure processing of healthcare data by integrating blockchain technology with AES-256 encryption using MIDC. IoT healthcare devices first collect and encrypt raw data using AES-256 encryption, while the encryption keys are managed securely by MIDC. This encrypted data is transmitted over a secure TLS connection to the blockchain network. The blockchain stores the hashes of data for verification of integrity, while actual encrypted data is stored off-chain in a secure cloud environment. Smart contracts enforce access control based on user roles, and only authorized users will be able to retrieve the required decryption keys from the blockchain. The authorized users then decode data using the received keys, along with original health care information, to access such information-in a way secure and compliant throughout the entire process.

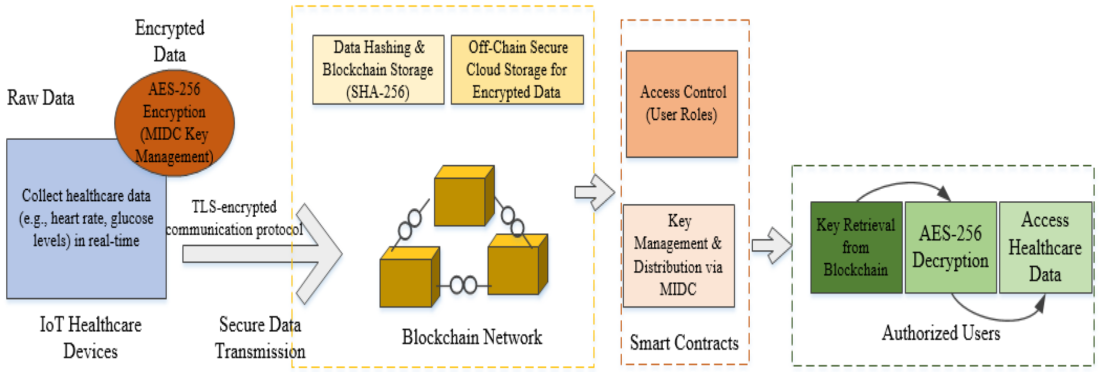
Encrypted Data
Raw Data
AES-256 Encryption (MIDC Key Management)
Collect healthcare data (e.g., heart rate, glucose levels) in real-time
IoT Healthcare Devices
TLS-encrypted communication protocol
Secure Data Transmission
Data Hashing & Blockchain Storage (SHA-256)
Off-Chain Secure Cloud Storage for Encrypted Data
Blockchain Network
Access Control (User Roles)
Key Management & Distribution via MIDC
Smart Contracts
Key Retrieval from Blockchain
AES-256 Decryption
Access Healthcare Data
Authorized Users

Figure 2: System Workflow for Healthcare Data Security Using Blockchain and MIDC AES-256 Encryption

5.2 Blockchain Platform

The blockchain technology platform is integral to the security architecture of the system to serve as a decentralized, tamper-resistant solution for healthcare-sensitive data. Through the utilization of blockchain technology, it addresses such critical challenges such as data integrity, patient confidentiality, and secure data exchange among authorized entities. Of the two blockchain platforms chosen for evaluation, namely, Hyper ledger Fabric and Ethereum, Hyper ledger Fabric has been chosen as the preferred one because of its permissioned architecture and robust enterprise-grade capabilities.

Platform Selection:

Hyper ledger Fabric is selected first because it is permissioned, where only the registered entities that include healthcare providers and regulatory agencies can participate in the blockchain network. Thus, access control is best for such sensitive healthcare applications. Evaluating Ethereum gives more significance to its great support towards smart contract development, which is capable of automating sophisticated processes like access control for data and auditing of compliance.

Node Setup:

The blockchain network utilizes a distributed architecture, where a number of nodes are maintained on servers managed by other healthcare providers. This in turn increases data redundancy, availability, and resilience to failures. Each node in the network is involved in validation of transactions and maintaining a blockchain ledger, thus preserving consistency and integrity of stored data.

AES Encryption Parameters

Encryption Standard: AES-256 is selected as it is strong and efficient. The system employs a MIDC, for secure generation and distribution of keys in order to protect against unauthorized access.

5.3 AES Implementation- Encryption using MIDC AES-256

For ensuring that health information is transmitted in a manner that is completely secure, the AES-256 encryption method is naturally included in the communication protocol between the IoT and blockchain networks. Raw sensor data encrypted using AES-256 symmetric encryption, highly secure in nature, are transmitted by the IoT healthcare devices across the network. In such cases, the intercepted data would not be accessible even to the party intercepting the data since it remains in the encrypted form. The encryption keys are dynamically generated and distributed through the Master Key Derivation Controller, a secure key management system that eliminates the risks associated with plaintext key transmission. The system reduces the possibility of key reuse and improves overall security by assigning unique encryption keys to each device and using dynamic key rotation. Owing to the fact that medical data is very sensitive, decryption and authentication of that data requires the best method of protection with the most secure data security method which is the MIDC AES-256 encryption technique. The concept of multi-input data concatenation, abbreviated for as MIDC is relatively new, whereby multiple statistical inputs are joined together and converted into a concatenated string before the resultant data is processed through the set AES-256 rules. The first process of the MIDC AES-256 encryption is the formation of one or more strings through an aggregation of factors, including patient's demography, histories, and diagnosis. This concatenated string is a 256 bit when all the characters are joined and, when used in the advanced encryption standard (AES), rules for encryption is very strong. Concatenation is the $D_1, D_2, \dots, D_n$ into a single string S. The mathematical representation of the concatenation process is found in Eqn. (1).

$$S = D_1 \oplus D_2 \oplus \dots . \oplus D_n \tag{1}$$

This process creates a single string S by combining several characteristics, such as patient demographics, medical history, and diagnostic data. Next, the concatenated string is encrypted using the commonly used symmetric encryption method, AES-256. The concatenated text is divided into fixed-size blocks using this technique, which then applies a number of substitution-permutation processes for safe encryption. Let's write S for the input concatenated string and E for the encryption algorithm. Eqn. (2) expresses the encryption procedure.

$$C = E(S, K) \tag{2}$$

In this scenario, C represents the encrypted data while K is the 256-bit encryption key. When the encryption function E carries out a series of mathematical operations on the input string by using the encryption key K, it generates the encrypted data. A significant component of the MIDC AES-256 encryption method is key selection, where the user selects a 256-bit encryption key. A longer key improves encryption security by making it computationally impossible for attackers to decrypt the encrypted data without the right key. Eqn. (3) explains the decryption process, which entails performing inverse transformations to the encrypted data.

$$S = D(C, K_{dec}) \tag{3}$$

where the decryption key is represented as K_{dec}. Using the decryption key, the decryption function D performs several inverse changes to the encrypted data C and produces the original concatenated string. This is where the MIDC approach is novel-its method of dealing with the concatenated data.

MIDC-AES Algorithm

```
Function MIDC AES 256 encryption (input data)
```

```
// Combine multiple data sources into a single concatenated string..
// Encrypt the concatenated string using the AES-256 encryption standard.
//Output the encrypted result.
Concatenate Data (input_data):
Initialize an empty string (concatenated_string).
Iterate through each entry in input_data and append it to concatenated_string.
Return the concatenated_string.
AES-256 Encryption (data):
Use a 256-bit encryption key to perform AES-256 encryption on the input data.
// This encryption process can utilize a library or built-in functions available in the chosen programming language.
Return the encrypted data as output.
```

On the receiving end, authorized healthcare providers decrypt the encrypted data using the corresponding AES-256 decryption keys. These keys are retrieved securely from a distributed tamper-proof ledger known as the blockchain. The decryption key is accessible only to approved users, thereby building a high level of control in access. TLS adds another layer of encryption on top of what the data was encrypted with to protect it in transit. This comprehensive implementation of AES-256 encryption, in combination with secure communication protocols, ensures health-related data privacy and integrity throughout its transmission and use lifecycle. Figure 3 illustrates the AES-256 encryption process, which uses a 256-bit key to encrypt sensitive data, ensuring high-level security

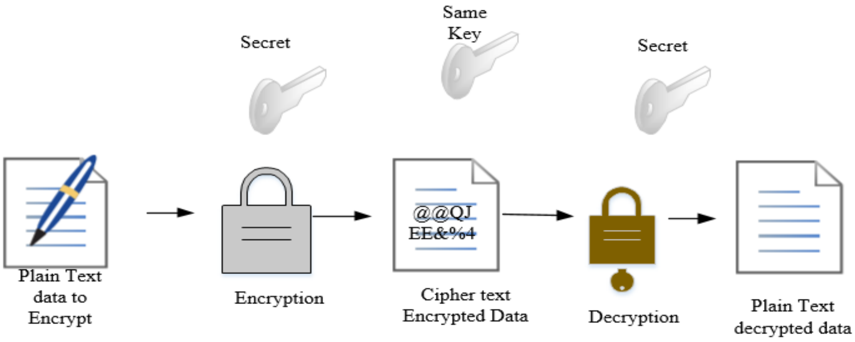
Secret
Same Key
Secret
@@QJ EE&%4
Plain Text data to Encrypt
Encryption
Cipher text Encrypted Data
Decryption
Plain Text decrypted data

Figure 3 : AES-256 Encryption Work to Protect Data

5.3.1 Advantages of MIDC Integration

- Scalability: The MIDC can handle keys for thousands of IoT devices, making it scalable for large-scale healthcare systems with thousands of endpoints.
- Resilience: The automated key generation and rotation processes minimize human error and make the system more resilient to breaches.
- Interoperability: The design of the MIDC ensures compatibility with a wide range of IoT devices and blockchain platforms, making it adaptable for various healthcare applications.

5.4 Blockchain Integration for Enhancing Security

Blockchain, thus, when applied, guarantees a safe healthcare data storage and the usage of the sophisticated consensus algorithm, cryptography, and transaction verification. Hyperledger uses Permissioned Network where Consensus algorithm of choice is practical Byzantine Fault Tolerant (PBFT). This ensures that only the right persons; such as healthcare providers and also the regulatory agencies can authenticate the transactions taking place within the network. PBFTs fault-tolerant model makes it secure and trustworthy enough because it is suitable to implement healthcare applications. Another called Proof of Authority (PoA) that means that only specific nodes can validate transactions, it is useful for situations that need faster response times. All the above mechanisms improve scalability and reliability of the system.

It will be hashed using the SHA-256 cryptographic hashing algorithm for data integrit and confidentiality reasons. This is to mean that the patient data collected will be hashed and therefore the originally collected data will be hashed to produce a digital footprint that will be checked to identify evidence of alteration or changes. All that will be stored on the blockchain is the hash values while the actual encrypted data will be stored in the off-chain environment to meet the various privacy standards that are reigning such as GDPR and HIPAA.

Every transaction -be it data upload or an access request-is rigorously verified by peer nodes. After validation, the transactions that satisfy the access rules are added immutably to the blockchain ledger along with timestamps and origin details. This distributed architecture avoids fraud, and maintains transparency while creating an auditable trail for managing healthcare data, thereby satisfying the industry's most significant security and compliance requirements

5.5 Smart Contract Development

Following that, the blockchain holding patient and medical records receives the encrypted data. The patient must consent before the data may be viewed, and the system will reject the clinic's request to see the patient's information. The only information that hospitals exchange is the scientific data on their patients. The method's data safety is improved by the usage of blockchain. Smart contracts are a part of the blockchain system, which is a tool for automated enforcement of security and access control policies within the network. Such self-executing contracts outline detailed and granular access permissions by user roles – to ensure that data sharing meets the privacy and security standards required. For instance, patients' records can be used in a way where a doctor has full access to records of patients for treatment, yet the researchers are provided only with anonymized datasets to ensure privacy of patients is preserved. This further enhances the concept of security by virtually limiting access and manipulation of data only to those with proper authentication vouchers.

Apart from the access authority managing show, smart contracts play another critical role of identity tracking and compliance to data. This means that any instance where data is read or updated must be logged and since every action must be independently verifiable, there is a tremendously long trail of audit which proves compliance with regulations such as GDPR or HIPAA. Besides promoting monitoring and accountability, such transparency effectively deters adversarial behavior by leaving a clear record to check how particular data were used.

This functionality is brought about through the "Migrations" contract which deals with the deployment and updating of these smart contracts. This is good as it allows the agent to have control over the versioning of the contract and also is able to track each time the contract is deployed. Other details of information include address of contract, time of deployment as well as, gas consumption making a perfect source of tracking update of the system. Another important one is "Auth" smart contract which governs the authentication and access control in the whole network. The "Auth" contract translates blockchain addresses to specific roles such as a patient, a doctor or a researcher, and the permissions that go with the roles.

6 Evaluation

The implementation of smart contracts within the blockchain network demonstrated substantial effectiveness in automating security and access control policies for healthcare data management The results from the proposed method show improvement in important cybersecurity indicators for healthcare facilities, such as lowering the probability of successful phishing attacks, improving data authenticity, and minimizing unauthorized access. When comparing performance of the suggested approach using blockchain and AES-256 encryption with the existing approaches the enhanced security and efficiency are revealed.

6.1 Smart Contract Deployment

Smart Contract Compilation: The process of deploying the smart contracts starts with compilation, using tools such as Truffle. It ensures that all the contracts, like `Auth.sol`, `Migrations.sol`, `PinController.sol`, and `SensorData.sol`, are syntax error-free and compatible with the blockchain platform. At compile-time, each contract is translated into bytecode and an Application Binary Interface (ABI), which are critical in the deployment and interaction of blockchains.

Preparation of Migration Scripts: Migration scripts are prepared to automate the process of deployment. The script defines the order in which contracts should be deployed, as well as the dependency chain between them. For example, `Migrations.sol` contract is deployed first to monitor the states of deployments.

Deployment to Blockchain: Every smart contract is deployed to blockchain through migration scripts. Transaction is created to send compiled bytecode to blockchain along with meta-data such as gas limit and initial parameters. It leads to the generation of a distinct contract address for each contract. This way, it can be interacted with on the blockchain network.

Logging and Validation of Deployments: Successful deployments are logged along with important details like transaction hashes, gas usage, and deployment cost. The blockchain records metadata, including the block number where the contract was deployed. For example, `SensorData.sol` might be deployed in block 5, incrementing the total deployments.

Contract Interaction Readiness: After deploying, all contracts are now addressable. The functions declared in the contracts like `Auth.sol` which manages authorization or `SensorData.sol` that manages data can now be called as a transaction to the address of these contracts. Finally, the network is ready for full blockchain operations: execute smart contract functions, read stored data, and call inter-contract interactions.

6.2 Performance Metrics- Proposed Method

A proposed system that incorporates blockchain and AES-256 encryption with MIDC for securing IoT healthcare data has identified two cybersecurity success factors: cybersecurity effectiveness and cybersecurity efficiency, paramount to addressing present and future attack incidences. The presented specified is based on the combination of block chain and AES-256 encryption with MIDC to secure IoT healthcare data, targeting set of cybersecurity measures, which would demonstrate the performance of the system in terms of possibility of the threats prevention, detection and response. Table 1 presents key cybersecurity performance metrics used to assess the effectiveness of the proposed healthcare data security system.

Table 1 : Performance Metrics –Proposed Method

Algorithm	Size (MB)	Encryption Time (sec)	Decryption Time (sec)	Buffer Time (MB)
Proposed Model	0.153	3.0	2.8	0.140

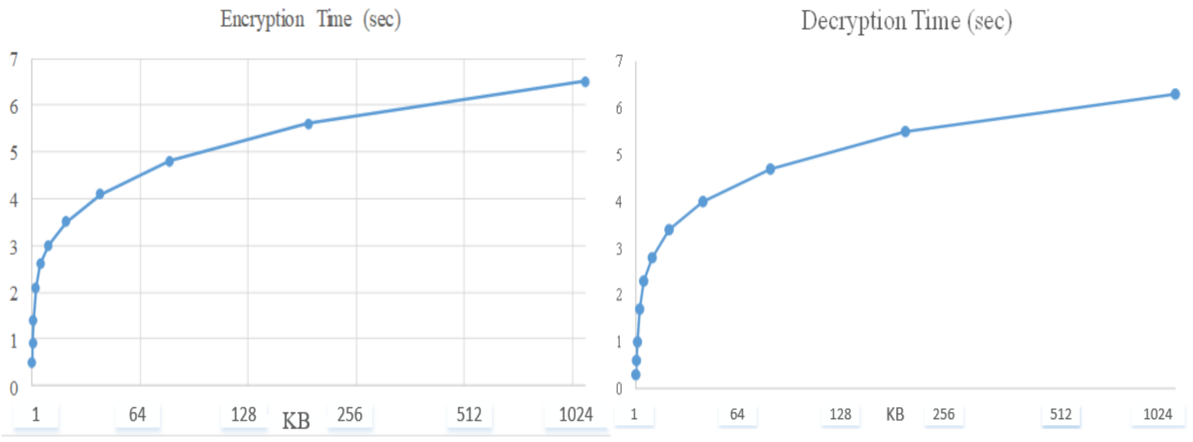

Figure 4: Distribution of Percentages among Encryption Algorithms

Figure 4 shows the **encryption time** of proposed algorithm's linear increase in encryption time with data size and **it shows the decryption time** demonstrates similarly efficient scaling, with the proposed algorithm, faster than traditional approaches. These results highlight the proposed algorithm's superior performance, making it ideal for secure and time-sensitive applications.

6.3 Performance Comparison

- **Encryption Time (sec):** The time it takes to encrypt a given amount of data using the encryption algorithm. It measures the efficiency of the algorithm in securing data before transmission or storage. Eqn. (4) denotes it.

$$\text{Encryption Time (sec)} = \frac{Total\ Data\ Size(MB)}{Encryption\ Speed(MB/Sec)} \tag{4}$$

- **Decryption Time (sec):** The time taken to decrypt some amount of encrypted data into its original state by applying the decryption algorithm. It will measure how fast the algorithm could recover the original data. Eqn. (5) denotes it.

$$\text{Decryption Time (sec)} = \frac{Total\ Data\ Size(MB)}{Decryption\ Speed(MB/Sec)} \tag{5}$$

- **Buffer Time (MB):** Temporary memory or cache used by the encryption/decryption algorithm, which is used for temporary storage of intermediate data that may arise during the processing. It indicates the size of memory needed to keep encrypted or decrypted data, or buffers used during computation. Eqn. (5) denotes it.

$$\text{Buffer Time (MB)} = \text{Memory Used for Processing Data} \tag{6}$$

Table 2 : Performance Comparison with Existing Methods

Algorithm	Size (MB)	Encryption Time (sec)	Decryption Time (sec)	Buffer Time (MB)
ABE(Wu et al., 2024)	0.153	7.5	5.2	0.153
Hybrid (AES)(Puneeth and Parthasarathy, 2024)	0.153	5.8	8.6	0.178
Traditional AES-256(Narasimha Rao and Chinnaiyan, 2024)	0.153	3.8	3.2	0.146
Proposed Blockchain+ MIDC AES-256 Model	0.153	3.0	2.8	0.140

From the Table 2, it can be observed that proposed method has a higher performance than the existing systems in most key metrics concerning cybersecurity in healthcare. These results highlight the efficacy of combining blockchain and AES-256 encryption with IoT healthcare devices for superior data security.

ABE: It is an attribute-based encryption, focusing on access control based on the attributes of the user. Though it provides fine-grained access control, it suffers from computational inefficiency. It requires 7.5 seconds for encryption and 5.2 seconds for decryption. This is the slowest among all the methods analyzed. Memory usage is 0.153 MB, which is very high because of the complexity involved in the attribute management process. While ABE guarantees secure data sharing through association of decryption with certain attributes, it is not scalable and performance-oriented for real-time applications.

Hybrid AES: Hybrid AES model integrates the benefits of AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) encryption algorithms that offer multi-layered security. Although Hybrid AES increases security, it also incurs more computational overhead. Encryption time is 5.8 seconds and decryption time is 8.6 seconds, which is a bit slower than others as encryption is done twice for once. Buffer memory utilization is also higher, with 0.178 MB; hence, more resource-intensive. This technique will be useful in scenarios where additional security layers are required but would not be efficient for resource-starved devices like IoT.

Classical AES-256: Traditional AES-256 is a symmetric key encryption algorithm known for its resistance against brute-force attacks. It has a time of 3.8 seconds for encryption and 3.2 seconds for decryption. This is a good balance between speed and security. The buffer memory usage is 0.146 MB, which is moderate compared to ABE and Hybrid AES. AES-256 is efficient in terms of both encryption and decryption times. However, it lacks the inbuilt mechanism of key distribution and is prone to side-channel attacks that limit its standalone security effectiveness.

Proposed Blockchain + MIDC AES-256 Model: The proposed Blockchain + MIDC AES-256 model integrates AES-256 encryption with blockchain technology and the MIDC framework to enhance the security and efficiency of IoT healthcare systems. The model reduces encryption time to 3.0 seconds and decryption time to 2.8 seconds, outperforming all other methods in terms of speed. It requires buffer memory as low as 0.140 MB-the lowest of the models in the family-indicating very good resource utilization. Blockchain does ensure data management that is virtually tamper-proof, so it doesn't have to worry about security and performance-both improve without increasing computational overhead.

In this work, the Proposed Blockchain + MIDC AES-256 Model has been made powerful enough over the traditional Classical AES-256 to be the better option for secure and fast encryption of data in IoT health systems. The biggest improvement of which is its faster encryption and decryption speeds (proposed model reduces encryption time to 3.0 seconds (21.1% speedup) and decryption time to 2.8 seconds (12.5% speedup)). Real-time processing in the IoT healthcare is a case where increased speed is a requirement due to its need to provide data encrypted from patients so that it can be accessed rapidly. Furthermore, the proposed model is optimized for memory efficiency by cutting down buffer memory usage from 0.146 MB to 0.140 MB, which is ideal for resource limited IoT devices. The classical AES-256 is not impossible to crack but is pretty secure against brute-forcing attacks, and unsecure against side channel attacks and has no built in key distribution mechanism. Vulnerabilities to these threats are tackled with a Blockchain integrated model for decentralized, undesigned data storage and secure key management whereas the MIDC framework strengthens encryption resilience against side channel attacks. Meanwhile, classical AES-256 has potential computational overhead in large scale applications, and the proposed model provides security upgrade with enhanced performance at the expense of minimal computational burden, considering Blockchain provides secure, real time data integrity check. Blockchain + MIDC AES 256 drops the service outlined above and is a better solution for such a big and critical work like Encryption in IoT Healthcare environment than standalone AES 256. The given metrics are based on the given existing traditional methods.

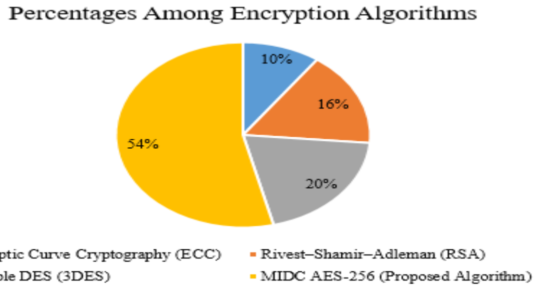

Figure 5: Distribution of Percentages among Encryption Algorithms

The distribution of percentages among various encryption algorithms, as shown in the Figure 5, provides a comparative analysis of the popularity or dominance of each algorithm in terms of their effectiveness, performance, and adoption https://github.com/vigneswaran1234/blockchain.

7 Discussion and Conclusion

7.1 Discussion

The results of this study show promise, with improvements in key security metrics such as phishing attack success rates, data integrity, and response times when using Blockchain and AES-256 encryption to secure IoT healthcare data. The findings are reliable because they compare favorably with benchmarks from similar studies, with better performance in key areas. Therefore, this work scope was targeted with an aim of securing a kind of healthcare data through using the technologies. Scalability and interoperability were on, hence compliance with regulations should not be forgotten. For the work, there remains to be limitations, considering specific configurations of Blockchain devices are limited to all healthcare systems; the approach offers promising strong security benefits but for proper integration, challenges such as scalability of Blockchain, Key Management of encryption, among device compatibility need to be achieved. Overall, the results demonstrate promise for this approach, but further work is needed to improve its scalability and bridge some of the remaining challenges.

7.2 Conclusion

The Proposed Blockchain + MIDC AES-256 Model exceeds other approaches in terms of encryption/decryption time and usage of buffer memory, making it the most efficient and secure IoT healthcare application. ABE and Hybrid AES provide strong security but incur high computational overhead and memory usage. Traditional AES-256 provides balance in speed and security but does not come with efficiency and additional features like blockchain integration, which proves to increase security and automation in the proposed model. The existing papers do not provide an exhaustive analysis of the key performance parameters, including encryption time, decryption time, buffer memory utilization, and the scalability of encryption algorithms in real-time scenarios. The proposed Blockchain + MIDC AES-256 model further optimizes these parameters with significantly reduced encryption and decryption times and minimum memory utilization, making it highly efficient for IoT healthcare systems. It does improve data security, tamper-proof integrity through blockchain, automates the process of access control with smart contracts, and provides better use of resources, thus it is more scalable and therefore applicable to resource-constrained devices in healthcare IoT environments. Despite these challenges, the research objectives were largely achieved because the study was able to demonstrate the feasibility of the integrated system in addressing security concerns and outlining future directions for research, such as alternative consensus mechanisms, elliptic curve cryptography, and integration of artificial intelligence for data analysis. The study also points to the potential for commercialization by indicating that the system developed could be sold as a secure healthcare data management solution for hospitals, clinics, and insurance providers in line with regulatory requirements, such as GDPR. Future work should be on improving the scalability of Blockchain, optimizing the encryption process, and developing practical solutions for key management and interoperability to ensure the widespread adoption of this secure system in the evolving digital healthcare landscape.

References

Egala, B.S. *et al.* (2021) ‘Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control’, *IEEE Internet of Things Journal*, 8(14), pp. 11717–11731. Available at: https://doi.org/10.1109/JIOT.2021.3058946.

Haghi Kashani, M. *et al.* (2021) ‘A systematic review of IoT in healthcare: Applications, techniques, and trends’, *Journal of Network and Computer Applications*, 192, p. 103164. Available at: https://doi.org/10.1016/j.jnca.2021.103164.

Khan, M.A. *et al.* (2020) ‘A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data’, *IEEE Access*, 8, pp. 52018–52027. Available at: https://doi.org/10.1109/ACCESS.2020.2980739.

Lee, S.-W. and Sim, K.-B. (2021) ‘Design and Hardware Implementation of a Simplified DAG-Based Blockchain and New AES-CBC Algorithm for IoT Security’, *Electronics*, 10(9), p. 1127. Available at: https://doi.org/10.3390/electronics10091127.

Li, K. *et al.* (2022) 'When Internet of Things meets Metaverse: Convergence of Physical and Cyber Worlds'. arXiv. Available at: https://doi.org/10.48550/arXiv.2208.13501.

Mohammed Sadeeq, M. *et al.* (2021) 'IoT and Cloud Computing Issues, Challenges and Opportunities: A Review', *Qubahan Academic Journal*, 1(2), pp. 1–7. Available at: https://doi.org/10.48161/qaj.v1n2a36.

Narasimha Rao, K.P. and Chinnaiyan, S. (2024) 'Blockchain-Powered Patient-Centric Access Control with MIDC AES-256 Encryption for Enhanced Healthcare Data Security', *Acta Informatica Pragensia*, 13(3), pp. 374–394. Available at: https://doi.org/10.18267/j.aip.242.

Naresh, V.S., Reddi, S. and Allavarpu, V.V.L.D. (2021) 'Blockchain-based patient centric health care communication system', *International Journal of Communication Systems*, 34(7), p. e4749. Available at: https://doi.org/10.1002/dac.4749.

Puneeth, R.P. and Parthasarathy, G. (2024) 'Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control', *Acta Informatica Pragensia*, 13(1), pp. 1–23. Available at: https://doi.org/10.18267/j.aip.225.

Rahman, M.A. *et al.* (2020) 'Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach', *IEEE Access*, 8, pp. 205071–205087. Available at: https://doi.org/10.1109/ACCESS.2020.3037474.

Saif, S. *et al.* (2024) 'A secure data transmission framework for IoT enabled healthcare', *Heliyon*, 10(16), p. e36269. Available at: https://doi.org/10.1016/j.heliyon.2024.e36269.

Tensae Laki *et al.* (2024) 'Secure Data Sharing in Decentralized Networks: Encryption Techniques, Access Control Mechanisms, and Data Integrity Verification', *Proceedings of London International Conferences*, (11), pp. 76–88. Available at: https://doi.org/10.31039/plic.2024.11.239.

Tran-Dang, H. and Kim, D.-S. (2021) 'The Physical Internet in the Era of Digital Transformation: Perspectives and Open Issues', *IEEE Access*, 9, pp. 164613–164631. Available at: https://doi.org/10.1109/ACCESS.2021.3131562.

Ullah, A. *et al.* (2021) 'Secure Healthcare Data Aggregation and Transmission in IoT—A Survey', *IEEE Access*, 9, pp. 16849–16865. Available at: https://doi.org/10.1109/ACCESS.2021.3052850.

Wu et al. (2024) 'Patient-centric medical service matching with fine-grained access control and dynamic user management', *Computer Standards & Interfaces*, 89, p. 103833. Available at: https://doi.org/10.1016/j.csi.2024.103833.

Xu, G. (2020) 'IoT-Assisted ECG Monitoring Framework With Secure Data Transmission for Health Care Applications', *IEEE Access*, 8, pp. 74586–74594. Available at: https://doi.org/10.1109/ACCESS.2020.2988059.

8 Appendix

The github Repository: https://github.com/vigneswaran1234/blockchain