International Journal of Basic and Applied Sciences, 14 (SI-1) (2025) 641-648

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/yg73n388
Research paper



Securing Healthcare Data with Advanced Asymmetric Lattice Galois Encryption Standard in A Decentralized Blockchain Framework

K. Britto Alex [1] *, K. Selvan [2]

[1] Research Scholar, P.G. and Research Department of Computer Science, J.J. College of Arts and Science (Autonomous), Affiliated to Bharathidasan University, Pudukkottai
[2] Assistant Professor & Research Advisor, P.G. and Research Department of Computer Science, J.J. College of Arts and Science (Autonomous), Pudukkottai, Affiliated to Bharathidasan University, Tiruchirappalli
**Corresponding author E-mail: birttoalex012345@outlook.com*

Received: July 25, 2025, Accepted: July 30, 2025, Published: November 1, 2025

Abstract

Securing sensitive data is essential to protect against unauthorized access, breaches, and privacy violations. A decentralized blockchain offers a robust solution by distributing data across multiple nodes, ensuring transparency, immutability, and enhanced protection, all without relying on a central authority. Several clinical datasets are available, covering a wide range of healthcare-associated data. Encryption and decryption, along with optimization, are techniques used to secure data by converting it into a form that is unintelligible without the precise key or algorithm. These processes play a crucial role in data protection and privacy. These datasets are invaluable for numerous applications, along with clinical studies, predictive analytics, system studies, and healthcare system optimization. The research presents an overall approach to a safe data management case study, which uses Kaggle datasets. The approach begins with preprocessing using the Z-score normalization method to ensure consistency in the dataset's dimensions. Use a data augmentation technique to expand the data range, thereby increasing the recording duration. Thereafter, an encryption scheme is implemented to maximize the security of the dataset. The encoded dataset is then placed in a decentralized blockchain, which allows for the effective utilization of its infrastructure for well-organized and efficient storage methods. The decryption process is facilitated by an AALGES Exchange mechanism, which securely retrieves the original data. Risk simulation occurs both before and after the data reaches the storage region, allowing for an evaluation of the system's resilience to stress. This is done in the Python platform. To examine the system's performance, it simulates the analysis in detail, specifically focusing on various aspects such as encryption and decryption speed, data storage capability, and minimum computational overhead.

Keywords: *Advanced Asymmetric Lattice Galois Encryption Standard (AALGES); Decentralized Blockchain; Decryption; Encryption; Preprocessing; Python; Z-Score Normalization.*

1. Introduction

A decentralized healthcare data protection system based on blockchain utilizes the dispersed nature of blockchain to protect private healthcare data from unauthorized access, manipulation, and data breaches [1]. In contrast to traditional centralized databases, where the failure of one component can impact the statistics of all users, blockchain technology distributes the statistics across multiple nodes in a secure and encrypted manner [3]. A block in the chain contains a document of transactions, which is timestamped, ensuring the integrity and traceability of records. The immutability of blockchain ensures that once data about healthcare is written in it, the network cannot modify it without their agreement, reducing the likelihood of misuse of healthcare data and fraudulent activities [5]. Additionally, intelligent contracts can be self-executing contracts that run on the blockchain, enabling access control by allowing only approved events to access or modify records based on specific conditions [7]. Patients have control over their own health information in the form of personal keys, which allows them to share data with healthcare professionals [4] selectively. The blockchain systems also increase interoperability by relying on a single platform that expands to integrate statistics from distinct hospitals, clinics, and laboratories, which can be easily read in real-time [9]. It enables triumph over old-fashioned data storage and ensures continuity of care in the near future or in the future of establishments [10].

Furthermore, blockchain will enhance audibility by maintaining an immutable record of all access history, thereby improving adherence to privacy policies [11]. Although blockchain has immense potential in protecting healthcare data, issues of scalability, excessive energy usage, and compliance with regulatory requirements must be overcome to achieve widespread application. All in all, a decentralized blockchain device has extraordinary potential to redesign scientific information control by enhancing security, privacy, and patient autonomy [13]. There are several challenges to implementing blockchain in healthcare data security, despite its potential. Scalability is a crucial

Copyright © K. Britto Alex, K. Selvan . This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

aspect of many projects, as the maturation of healthcare data can overburden the blockchain network, resulting in slower transaction rates and increased storage requirements [6].
The remaining sections of the study can be divided into the following: Part 2 presents related works, Part 3 discusses the methods, Part 4 summarizes the results, and Part 5 concludes the research.

2. Related Works

[15] Focused on a distributed ledger that divides network members into clusters and maintains one instance of the ledger of transactions for each cluster [12]. They presented a unique blockchain method for safe healthcare data management that outperforms the traditional Bitcoin system and a minimalist blockchain design, resulting in lower communication and computation overhead expenditures [8]. The study also investigated the design suggested that might be applied to solve the identified risks.
[17] Provided a secure, decentralized, cloud-based medical blockchain (CMBC) that addressed security and privacy issues while sharing individual healthcare data amongst medical institutions [2]. To improve healthcare performance, Electronic Health Record (HER) data was encrypted before being uploaded to a cloud-based blockchain system that used the lightweight authenticated encryption technique AES_256_GCM.
[18] Presented systems also concentrated on the healthcare sector; however, there was no protection for patient data because sensitive medical information was transferred from one facility to another for specific therapies. They might utilize blockchain with strong authentication to develop that application within the suggested system [14]. They could recommend the ADS approach after taking into account that issue.
[19] Stated on the access management system in Blockchain technology, which utilizes Numerous Party Authorities, smart contracts, and proxy encryption to safeguard the electronic health information. The proposed model consists of six steps: enrolment, appointment, data collection, data storage, inquiry, and validation. To maintain integrity and protection, healthcare information is encrypted using the Lightweight Fused Cryptographic (LFC) scheme and signed by both the patient and the physician.
[20] Supplied a unique solution that combines blockchain technology with sophisticated encryption schemes and privacy protection techniques to provide a safe and privacy-protected clinical records exchange environment. The proposed system consisted of three stages: startup, data processing, and authentication. The result showed that the suggested method proved effective in sensitive clinical records within the blockchain environment.
A blockchain-assisted secure data organization framework (BSDMF) for medical data, developed across the Internet of Healthcare Things, was proposed [21] to securely transmit patient data while also improving the potential and data availability of healthcare environments. The proposed BSDMF enabled the safe management of data between individual structures and devices that were implanted, as well as between servers within the cloud and personal servers [16]. The IoMT-based security architecture utilizes blockchain to ensure the security of communication and administration between connected nodes.
[22] Offered a combination of blockchain-based technology, a healthcare data shared technique, A hybrid blockchain-based technique for sharing health data securely, that splits contributing interactions into secure chain data contributed and alliances chain data shared, dependent on the shared entity. To minimize shared interference across various institutions, a combined blockchain-based approach for sharing medical data securely has developed a policy for controlling the utilization of medical information based on its identified and accessible purposes.
Although earlier research [15], [17] introduced blockchain-supported healthcare data management, the majority of the solutions have problems with scalability and privacy. As an example, Kumar et al. [15] reported scalability problems with large amounts of healthcare records, which restricts feasible implementation. Likewise, the CMBC strategy in [17] was less privacy-invasive but susceptible to enormous computational costs and delays. The limitations are overcome by our AALGES framework, which incorporates lattice-based cryptography that is not only more resistant to quantum attacks but also offers shorter encryption times of 1.00 ms, scaling well to the healthcare setting of our reality.

3. Methods

The healthcare dataset consists of 5,110 observations with 12 attributes. To preprocess the healthcare data, we utilized Z-score normalization. The decryption method utilizes the Advanced Asymmetric Lattice Galois Encryption Standard (AALGES) Exchange scheme to retrieve the original data securely. These procedures play a crucial role in protecting records and ensuring privacy. Figure 1 illustrates the study's flow.

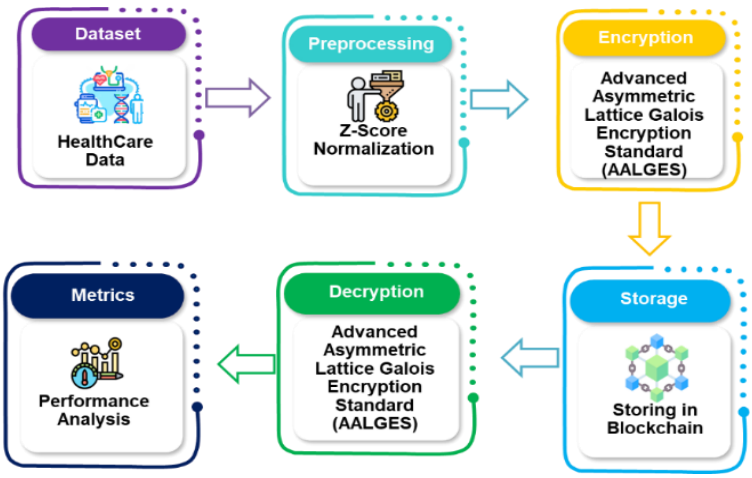


Fig. 1: Flow of the Study.

3.1. Dataset

The healthcare dataset comprises 5,110 observations with 12 attributes, capturing various factors that may contribute to the occurrence of strokes. This dataset provides vital healthcare and demographic data, along with variables such as gender, age, hypertension, heart disease, marital status, and occupation. Additionally, it includes behavioral elements, such as smoking status, and health metrics, including average glucose levels and body mass index (BMI).
(Data source: https://www.kaggle.com/code/rishabh057/healthcare-dataset-stroke-data/input)
The health data considered in this research was acquired on Kaggle. It has 5,110 records and 12 attributes, which are demographic, medical, and lifestyle-related variables (gender, age, hypertension, heart disease, work type, smoking status, average glucose levels, and body mass index (BMI)). The data is publicly accessible, which means it is reproducible and allows conducting comparative research on healthcare data security.

3.2. Z-score normalization

To preprocess the healthcare data, we utilized Z-score normalization. It converts information to a mean of 0 and an average deviation of 1. This is advantageous to numerous artificial intelligence techniques that require features to be on a similar scale. After applying normalization, each numerical feature in the dataset will be adjusted so that its distribution has a mean of 0 and a standard deviation of 1, making comparisons between features more meaningful and improving the performance of many statistical and machine learning methods.
A pre-processing technique called normalization divides down data into numerical characteristics and transforms values into a predetermined range. Several techniques are commonly used to normalize data, including scaling with decimals, min-max standardization, and Z-score normalization. With Z-score normalization, a U_j value from element F to U' It is transformed into an unknown range, as shown in Equation (1).

$$U'=\frac{U_j-F_j}{\text{std }(F)} \tag{1}$$

Where U Stands for the value that has to be normalized in the element. F_j for the average value of a characteristic, $U'$for the normalizing value's outcome, and $\text{std }(F)$ For the standard deviation.

3.3. The decryption process utilizes an advanced asymmetric lattice Galois encryption standard

The code employs a hybrid encryption scheme that combines Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) (symmetric encryption) with Rivest-Shamir-Adleman (RSA) and simulated lattice-based encryption. This method enhanced data security by leveraging the strengths of multiple cryptographic techniques. Lattice-Based Encryption Simulation. Even though lattice-based encryption is simulated, demonstrating that it is incorporated into a blockchain system as a post-quantum cryptography approach shows more forward-looking security practices. Timing Analysis. By measuring the encryption and decryption time on each block, the code provided support in understanding the overall performance and efficiency of cryptographic operations. This enables in-depth benchmarking and optimization of the blockchain system. The Attack Simulation code offers a simulation of a Denial of Service (DoS) attack to observe the performance of a blockchain.
This function provides a tangible experience of how blockchain is attempting to address malicious situations and highlight its capabilities. Tkinter Integration, utilizing Tkinter as a graphical user interface (GUI) to realize user input, is a method for creating a user-friendly blockchain experience. In this type of interaction, the user can populate the system with data through a GUI entry, and the system is ultimately enabled and operational. The Smart Settlement Class, utilizing a smart contract class to manage block data, presents an opportunity to simulate real-world blockchain use cases while also providing a way to reconcile connection statistics and systematic queries. The code produces very accurate estimates of performance, privacy ranges, and error rates of typical attacks on blockchain. These reports detail the amount of reporting, providing an excellent way to understand the system's resiliency, availability, and overall security. In this manner, where several methods are combined with block mining, there are even higher levels of encryption, as well as improved general performance parameters and enhanced attack resistance. The code offers a comprehensive method for reconstructing a secure and effective blockchain system.

3.3.1. Lattice-based encryption

This is a type of post-quantum encryption method developed to be robust against attacks from quantum computers. Although the actual performance in this case is just carried out through simulation, the system will expose promoted security against future attacks that involve lattice-based encryption. Such systems offer an interesting capability for post-quantum encryption, with strong security implications and efficient implementations. The security of lattice-based encryption depends on the difficult problems offered by the factor lattices in an n-dimensional Euclidean space (DES) Q^n. Lattice encryption is not sensitive to quantum attacks and offers worst-case resistance. We provide comprehensive definitions and features based on progressive research in the subject. A lattice structure is a discrete set produced by means of the combination of vertical units. A lattice is defined as a collection of gradually uncorrelated variables. Let $a_1, a_2 \ldots a_m \in Q^n$ It is a collection of gradually uncorrelated variables. $\mathcal{L}$ in n-DES, Q^n, the definition of $a_1, a_2 \ldots a_m$is as equation (2),

$$\mathcal{L}(a_1, a_2 \ldots \ldots a_m) = \left\{\sum_{j=1}^{m} b_j a_j : b_j \in Y\right\} \tag{2}$$

In this example, m and n Signify the sequence and dimensions of the lattice; for this reason, while $a_1, a_2 \ldots a_m$ Are the lattice's base variables. The minimal length of a lattice $\mathcal{L}$ is expressed in terms of the size of the smallest nonzero vector (a), equation (3),

$$C_{min}(\mathcal{L}) = \min_{a \in \mathcal{L}\{0\}} ||a|| \tag{3}$$

A lattice is essentially a separate organization of points throughout space that creates a collection of points in n dimensions. The lattice Q^2 is created with the starting point vectors $(1,1)$ and $(1,-1)$, resulting in numerous configurations. For example, $(1,1) + (1,-1) = (2,0)$ and $2(1,1) + (1,-1) = (3,1)$ Produce distinct lattice points.

A lattice is built on a collection of independent variables called. $\mathcal{L}$. A lattice has different revolves. Each base of the lattice has an equal number of components.
Every lattice $\mathcal{L} \in Q$ has a minimum of one base.A lattice's base may be written as a matrix.A = $[a_1, a_2 \ldots a_m] \in Y^{mwm}$, where A Basic variables are used as columns. The $\mathcal{L}$ created by a basis matrix $\mathcal{L}(A) \in Y$ is [Ab: b $\in Y^m$], where Ab Represents matrix-vector multiplication.
For clarity, we provide the pseudocode of the AALGES lattice-based encryption scheme:
Input: Plaintext P, Public key pk, Private key sk
Output: Ciphertext C
1) Encode plaintext P into an integer vector v
2) Sample a random error vector e from a Gaussian distribution
3) Compute C = (A·s + e, v + B·s) mod q
Where A, B ∈ Zq are lattice basis matrices and s is the secret vector
4) Transmit ciphertext C
5) Decryption: Recover v by computing C2 – B·sk from C1
6) Decode integer vector v to retrieve plaintext P
This algorithm illustrates how AALGES leverages the hardness of lattice problems to provide quantum-resistant encryption.

3.3.2. AES-GCM

AES-GCM is a symmetric encryption method that provides confidentiality and integrity by combining AES encryption with GCM mode, which includes authentication to protect against tampering. The AES structure is constructed concurrently due to its performance in decryption and encryption. As key size increases, a parallel infrastructure is created for key extension, with AES-256 typically having 14 transformation rounds. The research aims to optimize AES encryption time and key expansion using a 256-bit key size. The proposed structure uses 128-bit input and output blocks, with 14 rounds, enhancing performance through parallel data routes.
In Mixed columns, each State column is a four-term polynomial. Mix Colum's architecture aims to increase efficiency by removing XOR gates in crucial routes. Equation (4) represents the usual polynomial equations for the initial column of the Mix Column.

$$t'_{0,d} = \{[02] \cdot t_{0.d}\} \oplus \{[03] \cdot t_{1,d}\} \oplus t_{2,d} \oplus t_{3,d} \quad (4)$$

After expanding the formula, the formula appears as equation (5)

$$t'_{0,d} = [02] \cdot t_{0.d} \oplus [02] \cdot t_{1,d} \oplus t_{1,d} \oplus t_{2,d} \oplus t_{3,d} \quad (5)$$

The X Time represents the function of multiplying [02] in hexadecimal. The Mixed Column conversion has a critical path of four with the XOR gate, as shown by the equation expansion. To optimize Mix Column implementation, reduce the number of XOR gates. Equation (6) can be modified and expressed.

$$t'_{0,d} = [02]\{t_{0.d} \oplus t_{1,d}\} \oplus \{t_{1,d} \oplus t_{2,d}\} \oplus t_{3,d} \quad (6)$$

The Mix Column's critical path is decreased by XOR three critical paths to create the result. To use the three XOR gates, just one X Time is necessary. AES-GCM consists of the AES engine and the GHASH function. The GHASH function encrypts a 128-bit block, generates a Nonce in counter 1, and generates an authentication tag upon receiving extra authentication data (AAD) and ciphertext. This function is responsible for authenticated encryption and decryption. Verilog HDL is utilized as a hardware description language because it allows for easy exchange between contexts. The source code is pure HDL Verilog code that can be easily implemented on the Cyclone VDE1-SoC device.

3.3.3. RSA

Data may be encrypted and decrypted using the RSA method. The RSA algorithm involves three processes: key creation, encryption, and decryption. During the key creation procedure, we created a public and private key pair. Here's an algorithm for creating RSA keys:
1) Generate two prime numbers, oandr.
2) Count $m = o \cdot r$. Preferably $o \neq r$, because if $o = r$ then $o = r^2$ so omay be achieved by taking the square root of r.
3) Count $\phi(n) = (o - 1)(r - 1)$.
4) Select a public key, f, comparatively prime to $\phi(m)$
5) Create a secret key, c, $c \cdot f = 1 (\text{mod } \phi(m))$.
The RSA key creation technique uses (f, m) as the general key and c as the secret key. Finally, the RSA encryption key generation process assigns (f, m) as the public key and d as the private key. The RSA encryption technique employs an exponential form in module n, seen in equation (7).

$$D = O^f \text{mod } m \quad (7)$$

The opposite of the RSA encryption is the RSA decryption technique counterpart. The RSA decryption algorithm, like the algorithm used for encryption, employs an adaptable exponential formula n with the private key, as shown in equation (8),

$$O = D^c \text{ mod } m \quad (8)$$

4. Result

The experimental setup is shown in Table 1.

Table 1: Experimental Setup

Component	Details
Operating system	Windows
Python version	Python 3.12.6
Processor	Intel core i7(12^{th} Gen)
RAM	32GB
Device type	Contemporary laptop
Purpose	Performance measurements for intensive multitasking and development workloads

To compare the methods, several parameters are used, including Time required to encrypt, decrypt, and execute, Error rate (with & without attack), and confidentiality rate (with & without attack). The study compared the recommended strategy with the existing method, Hybrid Deep Belief-based Diffe Hellman (DBDH) [23]. The results showed that the AALGES outperformed the DBDH method based on these factors. Table 2 and Figure 2 show the Comparison results of Encryption, Decryption, and Execution time.

4.1. Encryption time

It refers to the duration required to convert healthcare data from plain text into an encrypted format to ensure secure storage and transmission. In a decentralized blockchain system, faster encryption reduces delays, enhancing real-time data protection. Compared to the DBDH model, which takes 3.55 milliseconds, the AALGES model performs significantly quicker, completing encryption in 1.00 milliseconds, indicating superior efficiency.

4.2. Decryption time

It is a metric of the amount of time required to undo the encryption of encrypted data into plain text. Fast decryption will guarantee unproblematic access to clinical information, primarily in emergencies. The DBDH method takes 3.6 milliseconds to decrypt the data, and AALGES saves only 1.99 milliseconds, which provides faster access to encrypted statistics. Such enhanced total performance is critical in the health care context, where data retrieval should be quick and safe.

4.3. Execution time

The amount of overtime in carrying out encryption, decryption, and other blockchain tasks is what affects the responsiveness of the system. The less time it takes to execute, the improved the performance of the system. Although the DBDH model takes 12 milliseconds to exhaust all the approaches, the AALGES framework takes a shorter time, 3.00 milliseconds, which is beneficial because it is faster and more resource-saving.

Table 2: Numerical Results of Encryption, Decryption, and Execution Time

Metrics	DBDH [23]	AALGES [Proposed]
Encryption Time (ms)	3.55	1.00
Execution Time (ms)	12	3.00
Decryption Time (ms)	3.6	1.99

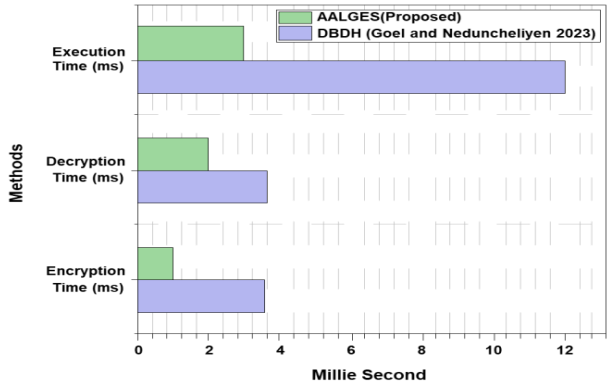


Fig. 2: Comparison of Encryption, Decryption, and Execution Time.

4.4. Confidential rate (attack and no attack)

It presents the percentage of information that is not lost in the event of an attack. This measure evaluates the effectiveness of the system against malicious attacks on the confidentiality of data. The DBDH model has a confidentiality rate that is 95.52, but AALGES has a higher confidentiality rate of 97.14, indicating that it is more resistant to data breaches and safeguards sensitive data. When not under attack, it measures the percentage of data that is safely kept under standard operating parameters without malicious activity. This is a statistic that shows the strength of the encryption system. AALGES network has an almost ideal confidentiality rate of 99.98, which is greater than the 95.93 at DBDH, and, under usual conditions, patient information is very secure. Figure 3 shows the performance of AALGES at a confidential rate with and without an attack.

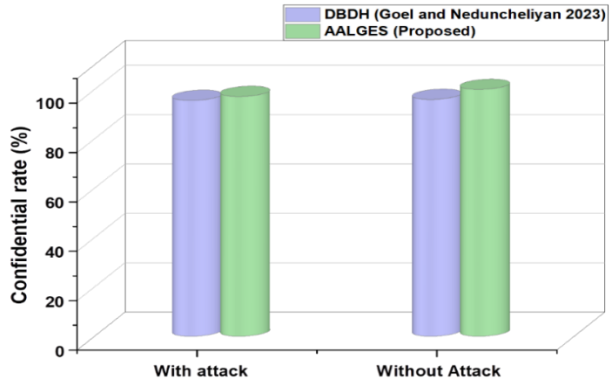


Fig. 3: Result of Confidential Rate.

4.5. Error rate (with attack and without attack)

It refers to the proportion of data errors or compromise during of attack. A lower error rate indicates higher resilience and data integrity in the face of malicious threats. DBDH reports an error rate of 0.0447%, while AALGES reduces this to 0.0300%, displaying that it continues to achieve better accuracy and reliability under attacks. Without assault, the percentage of errors in secure data transmission under normal conditions affects the accuracy of stored or transmitted data. In this case, AALGES offers a much lower error rate of 0.020% in comparison to DBDH's 0.040%, indicating agreater reliable system for managing clinical data without introducing inaccuracies during traditional operations. Graph 4 shows the efficiency of AALGES in terms of error rate with and without an attack.

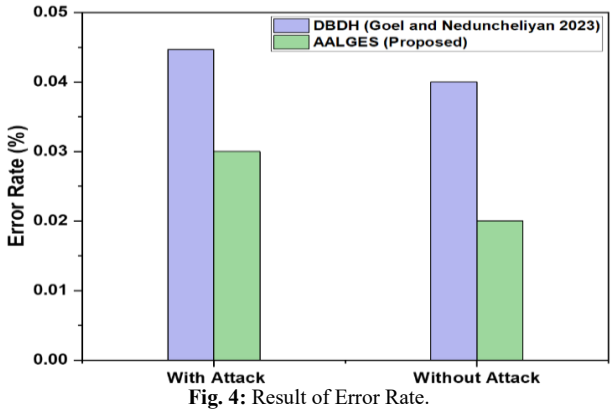


Fig. 4: Result of Error Rate.

These results indicate that AALGES consistently prioritizes performance over DBDH in all parameters, providing better overall performance, enhanced protections while having fewer errors, and ultimately is a better fit for ensuring the protection of clinical data in a decentralized blockchain milieu. Table 3 provides the numerical results for the confidence and error rate.

Table 3: Numerical Results for Error Rate and Confidential Rate

Metrics	Error Rate (With Attack) (%)	Error Rate (Without Attack) (%)	Confidential rate (With attack) (%)	Confidential Rate (Without Attack) (%)
DBDH [23]	0.0447	0.040	95.52	95.93
AALGES [Proposed]	0.0300	0.020	97.14	99.98

5. Discussion

The AALGES technique is significantly better than the DBDH Model in Encryption, Decryption, Execution Times, and data protection, while the DBDH technique excels, it is limited in speed and security taking 3.55 ms to encrypt and 3.6 ms to decrypt, however 95.52% of its confidentiality was compromised showing it is susceptible to a data breach, thus causing higher rates of error which is detrimental to the integrity of the data. These limitations can hinder the performance of time-sensitive healthcare applications, where it is essential to be able to access secure data fast, thus requiring the need to find more robust and efficient solutions. AALGES approach overcomes these drawbacks by making encryption and decryption time much lower at 1.00 milliseconds and 1.99 milliseconds, respectively. It has a higher confidentiality rate of 97.14% under attack and low error rates, making it ideal to be used in highly sensitive health care applications. Regardless of the strengths, there are certain limitations in the AALGES framework. A lattice-based cryptography uses more computing power than conventional encryption, which can be an issue with lightweight IoMT devices. In addition, AALGES is resistant to the traditional attacks, but its resistance to more complex side-channel attacks is yet to be justified in real-life uses. Future research ought to evaluate these aspects in order to be applicable in broader settings in the context of resource-limited health care settings.

6. Conclusion

Secrecy of sensitive information plays a great role in defense against undesirable access, breaches, and privacy invasion. A decentralized blockchain provided a strong solution with the distribution of data among a very large number of nodes, which allowed for transparency, immutability, and reinforced safety without being bound to a single authority. As part of pre-processing the healthcare data, we

implemented the normalization of data using Z-score statistics, which consisted of a total of 5,110 observations and 12 variables of data. The code has a hybrid encryption approach that consists of AES-GCM (symmetric encryption), RSA, and a simulated lattice-based encryption. The decryption method is the Advanced Asymmetric Lattice Galois Encryption Standard (AALGES) Exchange mechanism to recover the original data securely. Such implementations are essential to the protection and privacy of data. These results demonstrated that AALGES performs consistently better than DBDH for all parameters and provides better overall performance, safety, and error rates; therefore, AALGES is more compelling as a method to guarantee the security of healthcare data in a decentralized blockchain method. It can be quite complex to make the blockchain mechanism compatible with the current healthcare data processes. Discrepancies in regulations and standards between various healthcare providers can obstruct the free flow of data. In the future, we can expect the blockchain to enable patient empowerment, affording individuals the opportunity to control their healthcare data, be able to access it, and gain benefits. This research may be pursued in several future directions. One future direction is to combine AALGES with autonomous learning to develop an AOT methodology that does not violate privacy and potentially improve decentralized healthcare AI models. The second important direction is to ensure compliance with healthcare rules and regulations, such as HIPAA and GDPR, to ensure regulatory and ethical compliance of the medicine data management system through blockchains. Finally, resource-constrained IoMT devices will need to be optimized in AALGES to allow lightweight optimization and enable scalability across multiple healthcare contexts.

References

[1] Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Uchechukwu, F., Emordi, R. A. A., Nwozor, B., ... & Geteloma, V. O. (2024). BEHedas: A blockchain electronic health data system for secure medical records exchange. Journal of Computing Theories and Applications ISSN, 3024, 9104. https://doi.org/10.62411/jcta.9509.

[2] Herrera, J. A. Q., Limo, F. A. F., Tasayco-Jala, A. A., Vargas, I. M., Farias, W. B., Inga, Z. M. C., & Palacios, E. L. H. (2023). Security Issues in Internet Architecture and Protocols Based on Behavioural Biometric Block Chain-Enhanced Authentication Layer. Journal of Internet Services and Information Security, 13(3), 122-142. https://doi.org/10.58346/JISIS.2023.I3.008.

[3] Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., ... & Curry, E. (2024). Federated learning meets blockchain in decentralized data sharing: Healthcare use case. IEEE Internet of Things Journal, 11(11), 19602-19615. https://doi.org/10.1109/JIOT.2024.3367249.

[4] Sengupta, S., & Deshmukh, A. (2024). Blockchain for Transparent Supply Chains: Enhancing Accountability in SDG-Aligned Trade. International Journal of SDG's Prospects and Breakthroughs, 2(1), 7-9.

[5] Ghadi, Y. Y., Mazhar, T., Shahzad, T., Amir khan, M., Abd-Alrazaq, A., Ahmed, A., & Hamam, H. (2024). The role of blockchain to secure internet of medical things. Scientific Reports, 14(1), 18422. https://doi.org/10.1038/s41598-024-68529-x.

[6] Abbas, M. A., & Al-Jame, F. (2026). Recent advances in wearable biomedical sensors: Materials, signal processing, and healthcare applications. Innovative Reviews in Engineering and Science, 3(1), 83–89.

[7] Muralidharan, J., & Abdullah, D. (2025). IoT-based remote control and monitoring of agricultural irrigation systems using automation protocols. National Journal of Electrical Electronics and Automation Technologies, 1(2), 17–25.

[8] Volkov, I. P., & Ogbonnaya, E. (2025). Energy-efficient 3D-stacked CMOS–memristor hybrid architecture for high-density non-volatile storage in edge computing systems. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(3), 38–46.

[9] Luedke, R. H., & Monson, A. K. (2026). Design and implementation of edge-enabled IoT framework for real-time environmental monitoring. Journal of Wireless Sensor Networks and IoT, 3(1), 18–24.

[10] Pal, A., & Chhabra, D. (2025). Federated Learning for Healthcare Privacy-Preserved Artificial Intelligence in Distributed Systems. International Academic Journal of Science and Engineering, 12(1), 7-11. https://doi.org/10.71086/IAJSE/V12I1/IAJSE1202.

[11] Tariq, M. U. (2024). Revolutionizing health data management with blockchain technology: Enhancing security and efficiency in a digital era. In Emerging technologies for health literacy and medical practice (pp. 153-175). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-1214-8.ch008.

[12] Andersson, S., & Bergström, N. (2025). Blockchain-Enabled E-Commerce Platforms: Enhancing Trust and Transparency. International Academic Journal of Innovative Research, 12(3), 20-26. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1221.

[13] Verma, G. (2024). Blockchain-based privacy preservation framework for healthcare data in cloud environment. Journal of Experimental & Theoretical Artificial Intelligence, 36(1), 147-160. https://doi.org/10.1080/0952813X.2022.2135611.

[14] Carlos, M., & Escobedo, F. (2024). A Case Study-based Model for Sustainable Business Management through Blockchain Technology in Small and Medium-sized Enterprises. Global Perspectives in Management, 2(2), 41-50.

[15] Leong, W.Y., Leong, Y.Z. and San Leong, W., 2024, July. Enhancing Blockchain Security. In 2024 IEEE Symposium on Wireless Technology & Applications (ISWTA) (pp. 108-112). IEEE. https://doi.org/10.1109/ISWTA62130.2024.10651753.

[16] Nair, M., & Rao, A. (2023). Blockchain for Terminology Traceability in Decentralized Health Systems. Global Journal of Medical Terminology Research and Informatics, 1(1), 9-11.

[17] Sadulla, S. (2025). Effect of Pranayama on lung function in post-COVID rehabilitation among middle-aged adults: A clinical study. Journal of Yoga, Sports, and Health Sciences, 1(1), 24–30.

[18] Poornimadarshini, S. (2024). Comparative techno-economic assessment of hybrid renewable microgrids in urban net-zero models. Journal of Smart Infrastructure and Environmental Sustainability, 1(1), 44–51.

[19] Prasanna, G. A. S. (2024). Integration of Ethereum Blockchain with Cloud Computing for Secure Healthcare Data Management System. J. Electr. Syst, 20, 111-124. https://doi.org/10.52783/jes.1860.

[20] Tirkey, S., Mishra, D., & Mahalik, D. K. (2020). A Study on 'Why Outsourcing in Health Care'by Friedman Two-way Analysis of Variance Method. International Academic Journal of Organizational Behavior and Human Resource Management, 7(1), 01-08. https://doi.org/10.9756/IAJOBHRM/V7I1/IAJOBHRM0701.

[21] Kumar, A., Singh, A. K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P. K., ... & Tag-Eldin, E. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. Sensors, 22(15), 5921. https://doi.org/10.3390/s22155921.

[22] Rai, A. K., & Bhattacharjee, S. (2018). Does Development Lead to Narrowing the Gap in Maternal Health Care Utilization among Social Groups? The Evidences of Haryana. International Academic Journal of Social Sciences, 5(1), 213–222. https://doi.org/10.9756/IAJSS/V5I1/1810019.

[23] Arunkumar, B., & Kousalya, G. (2020). Blockchain-based decentralized and secure lightweight e-health system for electronic health records. In Intelligent Systems, Technologies and Applications: Proceedings of Fifth ISTA 2019, India (pp. 273-289). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-3914-5_21.

[24] Deepa, N., Devi, T., Gayathri, N. and Kumar, S.R., 2022. Decentralized healthcare management system using blockchain to secure sensitive medical data for users. Blockchain Security in Cloud Computing, pp.265-282. https://doi.org/10.1007/978-3-030-70501-5_13.

[25] Vidhya, S., & Kalaivani, V. (2023). A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. Peer-to-Peer Networking and Applications, 16(2), 900-913. https://doi.org/10.1007/s12083-023-01449-1.

[26] Vidhya, S., Siva Raja, P. M., & Sumithra, R. P. (2024). Blockchain-Enabled Decentralized Healthcare Data Exchange: Leveraging Novel Encryption Scheme, Smart Contracts, and Ring Signatures for Enhanced Data Security and Patient Privacy. International Journal of Network Management, 34(5), e2289. https://doi.org/10.1002/nem.2289.

[27] Velliangiri, A. (2025). Multi-Port DC-DC Converters for Integrated Renewable Energy and Storage Systems: Design, Control, and Performance Evaluation. Transactions on Power Electronics and Renewable Energy Systems, 30-35.

[28] Veerappan, S. (2025). Integration of Hydrogen Storage with PV Systems for Off-Grid Power Supply. Transactions on Energy Storage Systems and Innovation, 1(1), 41-49.
[29] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and ubiquitous computing, 28(1), 59-72. https://doi.org/10.1007/s00779-021-01583-8.
[30] Wang, T., Wu, Q., Chen, J., Chen, F., Xie, D., & Shen, H. (2024). Health data security sharing method based on hybrid blockchain. Future Generation Computer Systems, 153, 251-261. https://doi.org/10.1016/j.future.2023.11.032.
[31] Goel, A., & Neduncheliyan, S. (2023). An intelligent blockchain strategy for decentralised healthcare framework. Peer-to-peer Networking and Applications, 16(2), 846-857. https://doi.org/10.1007/s12083-022-01429-x.
[32] Zoitl, S., Angelov, N., & Douglass, G. H. (2025). Revolutionizing industry: Real-time industrial automation using embedded systems. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 12–22.
[33] Abbas, M. A., Hatem, T. M., Tolba, M. A., & Atia, M. (2023). Physical Design of Speed Improvised Factor in FPGA Applications. Journal of VLSI Circuits and Systems, 5(1), 61–66. https://doi.org/10.31838/jvcs/05.01.09.
[34] Reginald, P. J. (2025). Wavelet-based denoising and classification of ECG signals using hybrid LSTM-CNN models. National Journal of Signal and Image Processing, 1(1), 9–17.
[35] NUGRAHA, A. R., & Yekti NUGRAHENI, B. L. (2025). Analyzing the Fraud Diamond Model for Anticipating Financial Statement Manipulation: A Study on Registered Non-Financial Firms in the IDX (2018—2021). Quality-Access to Success, 26(206). https://doi.org/10.47750/QAS/26.206.04.
[36] Kociu, L., Hysi, A., Mano, R., & Celo, R. (2016). The remittances and evaluation of their impact on economic growth. (The case of Albania). Science. Business. Society., 1(1), 38-41.
[37] Madhanraj. (2025). Design and simulation of RF sensors for biomedical implant communication. National Journal of RF Circuits and Wireless Systems, 2(1), 44–51.
[38] Rahim, R. (2025). Lightweight speaker identification framework using deep embeddings for real-time voice biometrics. National Journal of Speech and Audio Processing, 1(1), 15–21.
[39] Uvarajan, K. P. (2025). Design of a hybrid renewable energy system for rural electrification using power electronics. National Journal of Electrical Electronics and Automation Technologies, 1(1), 24–32.