https://doi.org/10.53964/jia.2024001

https://www.innovationforever.com

Journal of Information Analysis

ISSN 2959-1295 (Online)

Open Access

Research Article

Securing Medical Data: The Integration of Advanced Encryption Standard and Blockchain

Xiaomeng Hu[1,2*], Yaning Du[1,2]

[1]University of Science and Technology Liaoning, Anshan, Liaoning Province, China

[2]Institute of Applied Artificial Intelligence of the Guangdong-Hong Kong-Macao Greater Bay Area, Shenzhen Polytechnic University, Shenzhen, Guangdong Province, China

[*]**Correspondence to: Xiaomeng Hu,** University of Science and Technology Liaoning, No. 185, Qianshan Middle Road, Tiedong District, Anshan, 114051, Liaoning Province, China; Email: 1948492554@qq.com

Received: October 12, 2023 **Revised:** November 14, 2023 **Accepted:** December 8, 2023 **Published:** January 15, 2024

Abstract

Objective: The research is to ensure the security of medical data and prevent data breaches. To achieve this objective, An efficient solution was proposed - the integration of blockchain technology with Advanced Encryption Standard (AES) encryption techniques to provide medical data security.

Methods: The cryptography which served as the cornerstone of information security provides robust encryption and decryption methods to ensure data confidentiality and integrity. At the same time, the attributes of tamper-proof and decentralization in blockchain ensure the true validity and security of data. We utilized the AES encryption algorithm to secure data and integrate the encrypted data into the blockchain technology, providing a solid and reliable guarantee for medical data privacy.

Results: The AES encryption algorithm was apply to blockchain technology. With this integrated solution, the security of medical data and effectively prevent data leakage was ensured.

Conclusion: This solution not only addressed the issue of medical data leakage, but also provided a solid foundation for the future development of information security. Integrating blockchain technology with AES encryption provided a reliable solution for medical data security, giving both patients and medical professionals greater confidence in data security. At the same time, the combination of the AES encryption algorithm and blockchain technology is being widely applied in various other fields.

Keywords: AES encryption, blockchain, medical data

Citation: Hu X, Du Y. Securing Medical Data: The Integration of AES and Blockchain. *J Inform Anal*, 2024; 2: 1. DOI: 10.53964/jia.2024001.

1 INTRODUCTION

With the rapid advancement of big data technology, the healthcare industry is increasingly turning to electronic medical records for efficient data storage. While this transition has significantly improved medical services, it has also raised concerns about privacy and security risks[1-3].

At the same time, if electronic medical records are confined to a local database within a hospital, they struggle to reach their full potential and hinder the seamless sharing of medical data across multiple healthcare institutions. This results in redundant examinations and wasted resources. As a result, ensuring both the security and accessibility of medical data has become a pressing and widely discussed issue[4-6].

To address the security concerns surrounding medical data, we use the Advanced Encryption Standard (AES) encryption algorithm for data protection. The AES algorithm, proposed by Koç[7] in 2006, replaces Data Encryption Standard (3DES) to provide more efficient and secure encryption operations. Today, AES is one of the most widely used symmetric key encryption algorithms, which uses 128-bit block symmetric encryption, providing both exceptional security and efficient encryption speed.

In recent years, it has became clear that in-depth research on the AES algorithm is a crucial focus in the field of information security. Aleisa's research in 2015 conducted an in-depth comparison of AES and 3DES encryption algorithms, clarifying the significant advantages of AES in terms of security and efficiency, therefore was widely recognized as the preferred algorithm for providing higher security[8]. In addition, Devi and Kotha[9] detailed the key features of the AES algorithm and compares it to other algorithms, providing a solid foundation for further research. To improve data security and sharing, we adopt blockchain technology. With its characteristics of decentralization, anonymity, and immutability, blockchain provides a reliable foundation for medical data security[10]. The immutability and transparency of the data was ensured by storing medical data on the blockchain, effectively preventing unauthorized access and tampering. The integration of blockchain technology with encryption algorithms is also a prominent area of research. Sathya's research explored the application of advanced encryption technology to provide blockchain data security and ensure the secure transmission of information, providing important insights into the broad application and demand for blockchain technology[11]. Gabriel and Sengottuvelan[12] proposed using the AES encryption algorithm to protect data and storing the encrypted data on the blockchain to ensure the privacy and security of the information, underscoring the importance of data privacy.

In all, the integration of blockchain technology and AES encryption plays a critical role in securing medical information,which not only addresses information security concerns but also provides a reliable foundation for the digital advancement of the medical industry. This innovative solution plays an important role in current and future medical information systems, providing patients and medical professionals with more secure and reliable services.

2 METHODS

2.1 Integrating AES Encryption with Blockchain Technology

Blockchain technology offers an exceptionally secure means of data storage, which guarantees the permanent preservation and traceability of information supported by its immutable nature[13]. At the same time, blockchain achieved a decentralized trust framework that eliminates the necessity for intermediaries, significantly reducing transaction costs and associated risks. These transformative features are reshaping industries including finance and supply chain management.

The fusion of blockchain technology with the AES encryption algorithm is a critical advance in information security and privacy. It maintains both the integrity and confidentiality of data by effectively thwarting unauthorized access, theft or tampering which represents a significant step forward in enhancing data security and strengthening privacy measures. The role of the encryption algorithm in permitting only authorized individuals to decrypt data ensures both its confidentiality and integrity which also serves as a robust deterrent against malicious attacks and potential data breaches, thereby increases the overall security and stability of the system. Crucially, this technological integration establishes the foundation for a decentralized trusted digital economic ecosystem which offers more streamlined, transparent and secure solutions across multiple industries, which in turn encourages the widespread adoption and advancement of blockchain technology.

Uploading encrypted data to the blockchain is the key in the architecture (Figure 1). Storing encrypted data on the blockchain offers clear security advantages over storing unencrypted data directly. The approach involves encrypting the data before uploading to the blockchain, ensuring that only users with the correct decryption key can access and interpret it. This method ensures data privacy and security, effectively mitigating the risk of unauthorized access or tampering. Storing encrypted data on the blockchain also improves data traceability and transparency[14,15]. Blockchain technology is inherently immutable; once data is recorded, it remains unalterable and cannot be removed[16-18]. This characteristic, coupled with the storage of encrypted data, guarantees the integrity and authenticity of the information. Another notable benefit is increased control over data sharing, in which the encrypted data can only be accessed and leveraged by authorized users, giving data owners greater oversight and ensuring that information is only used by authorized personnel.

Based on the Figure 1, safeguarding the privacy of patient information and enabling the secure sharing of medical records is achieved through the following steps:

(1) The medical information of the patient is first

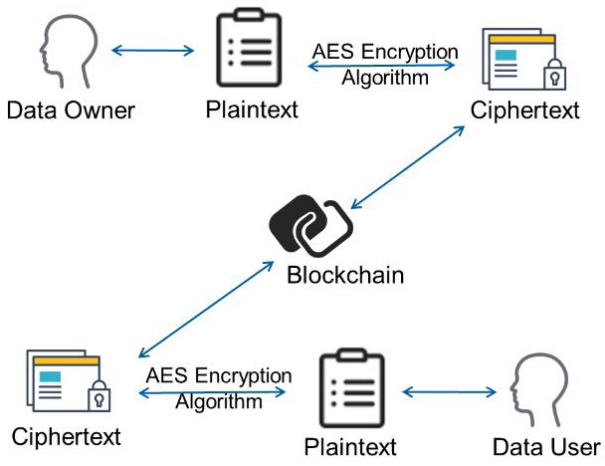

Figure 1. Architecture for uploading encrypted data to the blockchain.

encrypted using the AES algorithm, after which the encrypted data is securely stored on the blockchain. The decentralized and tamper-proof attributes of the blockchain guarantee the security and integrity of the data. It also generates new hash values to ensure the uniqueness of the information.

(2) When there is a subsequent need to access medical record data, users can locate the corresponding ciphertext medical record on the blockchain using the associated hash value. They can then utilize the corresponding key to decrypt the medical record and retrieve the original patient's medical information.

This approach offers a primary advantage that it not only safeguards patients' private information but also establishes a secure storage system for medical records on the blockchain. This enables multiple hospitals to seamlessly exchange medical record data, ultimately providing patients with more streamlined medical services. Additionally, owing to the inherent characteristics of blockchain, it acts as a safeguard against unauthorized access and tampering, further fortifying data security.

2.2 AES Encryption Algorithm

The AES algorithm is a block encryption algorithm whose basic unit is a 128-bit block , which emerges as the leading candidate to replace the DES algorithm due to its exceptional efficiency, computational simplicity, and robust security features. These blocks are organized in a 4×4 matrix configuration and together form the plaintext matrix. The AES encryption process is performed within a state matrix of the same size and arrangement, with the initial state matrix corresponding to the plaintext matrix. The AES algorithm provides flexibility with different key lengths, including 128 bits, 192 bits, and 256 bits. The use of a 128-bit key requires 10 rounds of encryption and decryption, a 192-bit key requires 12 rounds, and a 256-bit key requires 14 rounds. Increasing the key length inherently increases the number of encryption and decryption rounds, thereby increasing the overall security of the process.

This article applied the 128-bit AES encryption algorithm to ensure data security. The AES encryption algorithm is carefully programmed in C Programming Language and executed on the Central Processing Unit (CPU). It is important to emphasize that throughout this implementation process, we deliberately avoid the use of any external libraries, relying solely on the standard C language library. This deliberate choice not only serves to enhance the understanding of the structural principles underlying the AES encryption algorithm but also provides a robust foundation for potential future applications on CPUs. Figure 2A showed the flow chart of AES encryption process, which consists of ten rounds, with the first nine rounds following an identical sequence of operations and the final round excludes the column mixing operation. Each round includes four core operations: byte substitution, row shift, column mixing and round key addition.

2.3 Byte Substitution

A visual representation of the byte substitution process in the AES algorithm was shown in Figure 2B. Byte substitution involves mapping one byte of plaintext to another by means of an S-box. This is the single nonlinear transformation within the AES group of operations and maintains its reversible properties. The S-box essentially functions as a byte substitution table, performing byte-level operations using a predetermined substitution table. This step is intentionally included to increase the complexity of the algorithm and make it more resistant to encryption. Within the AES encryption process, byte substitution plays a pivotal role, significantly enhancing the security of the algorithm. Through the astute design of the S-box, the algorithm's resilience in maintaining encryption efficiency was strengthened. As such, byte substitution, a cornerstone of the AES algorithm, occupies an indispensable position throughout the encryption process.

2.4 Row Shift

A visual representation of AES row shifts was shown in Figure 2C. Row shift is a linear transformation stage within the AES encryption algorithm, primarily designed to spread the bytes within each row. In this process, the bytes are cyclically shifted according to certain rules, thereby improving the diffusion effect of the algorithm. In particular, the rowshift rules are as follows: the first row retains its original arrangement; the second row is shifted one byte to the left; the third row is shifted two bytes to the left; and finally, the fourth row is shifted three bytes to the left. The row shift operation effectively disperses the bytes within each row throughout the matrix, significantly increasing the algorithms ability to confuse. This strategic step is carefully designed to strengthen the security of the algorithm by thwarting potential cryptanalysis attacks. As a

https://doi.org/10.53964/jia.2024001

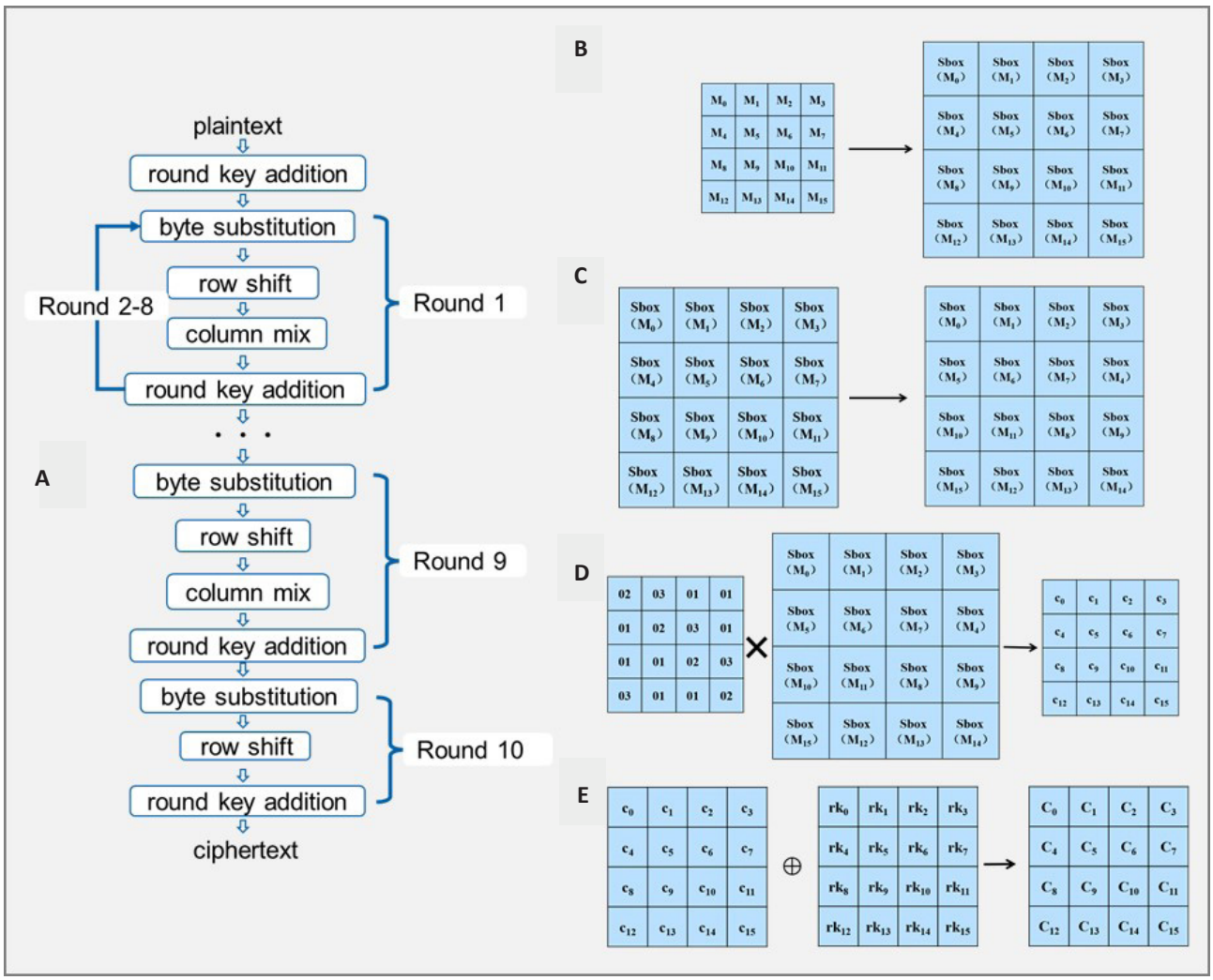

Figure 2. The schematic diagrams of AES encryption algorithm. A: AES encryption process; B: Byte Substitution; C: Row shift; D: Column Mix; E: Round Key Addition.

critical component within the AES algorithm, row shifting contributes significantly to its overall security posture. As a result, row shifting plays a critical role in the AES encryption process.

2.5 Column Mix

Column mixing transformation plays a key role in AES encryption and was shown in Figure 2D. The column mix transformation is a crucial phase within the AES encryption algorithm, which is performed through the operation of matrix multiplication. The state matrix, which has undergone a row shift, is multiplied by a predetermined constant matrix to achieve a diffusion effect across the columns. This step embodies a substitution transformation that further strengthens the security of the algorithm. The column mix transformation is a more complicated operation than other transformations within the AES encryption algorithm. Its core operation is a polynomial multiplication performed within the finite field GF(256). In principle, column mixing involves multiplying each element in the matrix by a predetermined polynomial. This method of processing significantly amplifies the algorithm's ability to obfuscate data, thereby strengthening the overall security of the encryption process. The column mix transformation in the AES algorithm conducts profound substitution and diffusion operations on the state matrix during each encryption round. This intricate process renders the alterations in each byte more intricate and unpredictable, providing a robust guarantee of the algorithm's security.

2.6 Round Key Addition

Round key addition shown in Figure 2E played a critical role in the AES encryption process. This operation involved performing an XOR operation on each column in the result of the column mixing with the corresponding column in the key. The original byte sequence was then replaced with the resulting values. This step integrates key information into the encryption process by performing an XOR operation with the key, thereby strengthening the security of the encryption algorithm. The inclusion of round key addition ensured that each encryption round possesses a unique quality, which made the algorithm significantly more resistant to decryption attempts. It is worth noting that in the

AES algorithm, round key addition is an iterative process, with each round employing an independent sub-key for encryption. This design choice provides a significant advantage: even if a portion of the key is known, it becomes difficult to deduce the complete key information, thereby strengthening the security of the encryption.

The key plays a critical role in the encryption process, acting as a password to protect the plain-text and ensure the confidentiality of the information. In symmetric encryption, the same key is used for both encryption and decryption. Therefore, key protection is paramount and requires secure negotiations between communicating parties in a protected environment. However, transmitting the key directly over the network is inadvisable due to the risk of interception by potential attackers. If compromised, the leaked key could be exploited to recover cipher-text and access sensitive data. To avoid this scenario, implementing a secure key exchange protocol, for instance leveraging public key encryption technology, is essential to maintain key security. In addition, regular key updates served as a standard security practice to mitigate potential threats.

As a symmetric encryption algorithm, AES leveraged a single key for both encryption and decryption, resulting in rapid processing speeds. In the key expansion process, each column within the key expansion matrix consists of four bytes, which together form an array referred to as W. The columns are labeled W[0] through W[3], corresponding to the first, second, third, and fourth columns of the matrix, respectively. The W array was then expanded, resulting in the addition of 40 new columns of bytes. This process culminated in an expanded key array with a total of 44 columns. This expanded key array plays a pivotal role in the encryption phase that follows, ensuring both the integrity and security of the key. Through this meticulous expansion process, we provide the AES encryption algorithm with robust keys capable of maintaining a high level of data security.

AES is a symmetric encryption algorithm that uses the same key for both encryption and decryption, ensuring rapid and efficient cryptography operations. AES excels at protecting sensitive information. When used to encrypt medical data, it provides reliable protection of privacy and sensitive patient information during storage and transmission, effectively thwarting unauthorized access and tampering. This technology provides a secure and reliable technical foundation for the medical industry, creating a secure service environment for both patients and medical staff.

3 RESULTS AND DISCUSSION

The efficiency of implementing 128-bit AES encryption and decryption using the C programming language was evaluated. The evaluation focuses primarily on the speed with which data can be encrypted and decrypted with a 128-bit key. Table 1 provided a breakdown of the time (measured in milliseconds) required for encryption and decryption operations for various input data sizes.

As shown in the Table 1, there was a proportional increase in the time required for both encryption and decryption as the data size escalates. However, the overall performance remained highly efficient.

Figure 3 showed the encryption and decryption timefor data sizes ranging with 1KB-100KB and 1MB-100MB.We incrementally encrypt data from 1 to 100KB and 1 to 100MB in equal increments of 5KB and 5MB, which followed an incremental rule. It is evident that as the data size increases, the time required for both AES encryption and decryption also increases. This correlation underscores the direct impact of data size on encryption and decryption speed. As a result, the AES algorithm may take longer to process larger data sets. This trend underscored the importance of considering data size and encryption time in practical applications to ensure system efficiency and stability when handling large data loads. These experimental results served as a reference in refining and tuning the encryption system for optimal performance.

Eencryption operations were performed on the Ubuntu operating system, which significantly improved encryption efficiency by optimizing the encryption algorithm and reducing the iteration process. When the data size was 1MB, the encryption time on the Ubuntu operating system was only 73.3ms, which was significantly shorter than the encryption time of 80ms[19]. As the data size increased, the efficiency advantage became more significant. When the data size increases to 5MB, 10MB and 20MB respectively, our encryption times are 348.93ms, 697.05ms and 1389.35ms, while the corresponding times of Panda's research were 376.1ms, 897.5ms and 1844.5ms, which indicated that our system was more efficient at these respective data scales[19]. Rihan et al.[20] implemented the encryption algorithms AES and DES on both Windows and Mac platforms. In particular, the execution time for AES outperforms DES on both platforms. For data sizes of 15KB, 30KB and 45KB, the encryption times in this study were 1.22ms, 2.27ms and 3.3ms respectively. In contrast, the corresponding times reported by Rihan et al.[20] were 3.8s, 7.5s, and 8.5s. Comparing these experimental results, it was clear that our implementation was significantly more efficient. Kawle et al.[21] presented a lightweight AES encryption algorithm that takes only 51.093ms to process 16 bytes of data. In contrast, the AES encryption algorithm implemented in this article processes 1KB of data in 0.224ms. In terms of encryption efficiency, the algorithm used in this article clearly demonstrated its superior performance.

https://doi.org/10.53964/jia.2024001

Table 1. AES Encryption and Decryption Time

Data Size	Encryption (ms)	Decryption (ms)	Data Size	Encryption (ms)	Decryption (ms)
1KB	0.223845	0.214328	1MB	73.3	71.67
5KB	0.507862	0.489646	5MB	348.93	341.06
10KB	0.867006	0.848359	10MB	697.05	680.6
15KB	1.2214	1.1913	15MB	1,043.48	1,014.68
20KB	1.588526	1.541575	20MB	1,389.35	1,351.36
25KB	1.895507	1.847659	25MB	1,730.87	1,686.6
30KB	2.269815	2.20535	30MB	2,079.59	2,026.66
35KB	2.620276	2.559176	35MB	2,432.12	2,468.53
40KB	2.966584	2.883019	40MB	2,767.86	2,695.04
45KB	3.303858	3.200095	45MB	3,127.52	3,048.21
50KB	3.642491	3.567363	50MB	3,448.26	3,372.68
55KB	4.012924	3.918011	55MB	3,796.96	3,711.43
60KB	4.35138	4.24262	60MB	4,149.86	4,040.9
65KB	4.784489	4.669884	65MB	4,489.23	4,383.96
70KB	5.03948	4.90229	70MB	4,839.79	4,715.65
75KB	5.396649	5.264079	75MB	5,210.76	5,084.85
80KB	5.673797	5.554643	80MB	5,537.69	5,394.93
85KB	6.078595	5.845474	85MB	5,864.03	5,713.49
90KB	6.46806	6.302645	90MB	6,207.37	6,021.93
95KB	6.82987	6.641852	95MB	6,558.06	6,379.55
100KB	7.155401	7.00467	100MB	6,890.13	6,710.3

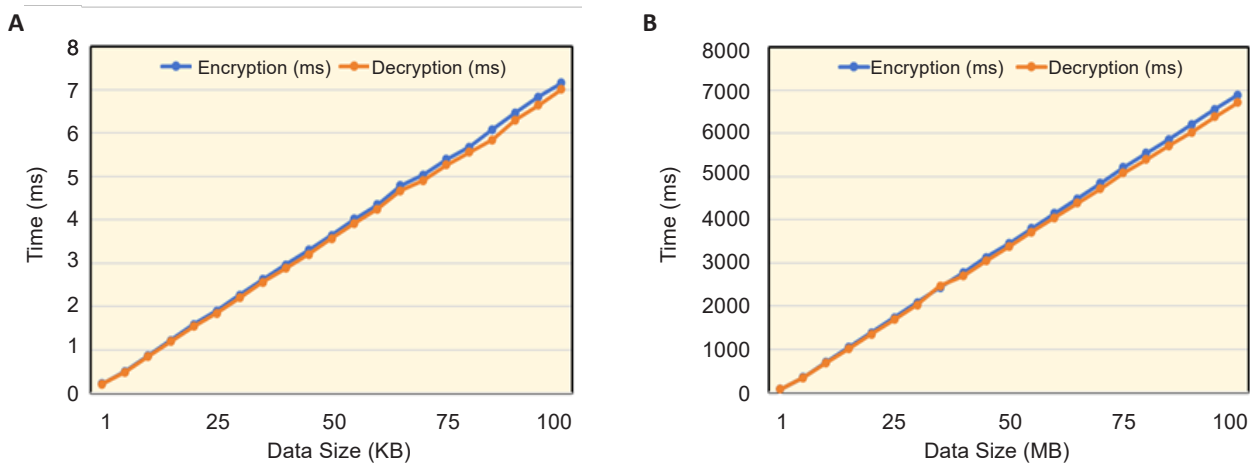

Figure 3. The encryption and decryption timefor data sizes ranging with 1KB-100KB and 1MB-100MB. A: 1-100KB AES encryption and decryption time comparison; B: 1-100MB AES encryption and decryption time comparison.

This comparison showed that the encryption scheme in this study was more efficient when processing data with different sizes. By implementing optimizations and reducing iteration processes on the Ubuntu operating system, encryption times were significantly reduced. These improvements were not only reflected in small data, but also showed significant advantages when processing large data. A more reliable solution was provided by AES encryption algorithm, which enabled the secure encryption of medical records. The fusion of the AES encryption algorithm with blockchain technology would provide a double layer of protection for medical record data, ensuring the confidentiality of patients' sensitive information during both storage and sharing.

4 CONCLUSION

The paper dissected various facets of the AES algorithm, including byte substitution, row shift and column mix. At the same time, the benefits of the storage of encrypted data on the blockchain were emphasized. The 128-bit

AES encryption algorithm to encrypt data and conducts experiments on the Ubuntu operating system was applied, which focused on reducing the number of iterations to improve calculation efficiency. A comparative analysis of the experimental results showed that the text encryption scheme provided significant efficiency advantages, indicating the integration of blockchain technology with the AES encryption algorithm is a widely recognized and powerful solution that provides a robust framework for strong information security.

The extensive research addressedthe innovative fusion of the AES encryption algorithm with blockchain technology, reaffirming the privacy and security of medical data. The patient's private information was effectively protected through the encryption of their medical records with the AES algorithm and subsequent storage on the blockchain. The validate efficiency and security of the AES algorithm in the field of information security was conducted. This result serves as a valuable reference for related fields. As this technology matures and evolves, its potential extension to broader domains promises to provide data security assurances to a wider audience, thereby catalyzing the continuous advancement of information security.

Acknowledgements

The authors sincerely thank the University of Science and Technology Liaoning and Shenzhen Polytechnic University for providing a quality learning environment. At the same time, the authors would like to thank all the collaborating partners for their support and cooperation.

Conflicts of Interest

The authors declared no conflict of interest.

Author Contribution

Hu X completed the experimental work and drafted the article. Both Hu X and Du Y reviewed and contributed to the content of the article.

Abbreviation List

AES, Advanced Encryption Standard
CPU, Central Processing Unit
DES, Data Encryption Standard

References

[1] de Moraes Rossetto AG, Sega C, Leithardt VRQ. An Architecture for Managing Data Privacy in Healthcare with Blockchain. *Sensors*, 2022; 22: 8292.[DOI]

[2] Mokhamed T, Talib MA, Moufti MA et al. The potential of blockchain technology in dental healthcare: a literature review. *Sensors*, 2023; 23: 3277.[DOI]

[3] Han Y, Zhang Y, Vermund SH. Blockchain Technology for Electronic Health Records. *Int J Env Res Pub He*, 2022; 19: 15577.[DOI]

[4] Gabriel SJ, Sengottuvelan P. An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System. 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2021: 400-405.[DOI]

[5] Sun J, Yao X, Wang S et al. Blockchain-based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. *IEEE Access*, 2020; 8: 59389-59401.[DOI]

[6] Puneeth RP, Parthasarathy G. Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System. *Int J Eng*, 2023, 36: 925-933.[DOI]

[7] Koç ÇK. About Cryptographic Engineering. In: Cryptographic Engineering. Springer: Boston, USA, 2009.[DOI]

[8] Aleisa N. A Comparison of the 3DES and AES Encryption Standards. *Int J Sec Appl*, 2015; 9: 241-246.[DOI]

[9] Devi SV, Kotha HD. AES encryption and decryption standards. Journal of Physics: Conference Series. Andhra Pradesh, India, 27-28 December 2018.[DOI]

[10] Jena AK, Dash SP. Blockchain technology: introduction, applications, challenges. Blockchain Technology: Applications and Challenges. Cham: Springer International Publishing, 2021: 1-11.[DOI]

[11] Sathya AR, Banik BG. A comprehensive study of blockchain services: future of cryptography. *Int J Adv Comput Sc*, 2020; 11: 279-288.[DOI]

[12] Gabriel SJ, Sengottuvelan P. An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System. 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2021: 400-405.[DOI]

[13] Fadlil A, Riadi I, Nugrahantoro A. Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology Modification. *Lontar Komputer Jurnal Ilmiah Teknologi Informasi*, 2021.[DOI]

[14] Jiang Y, Sun G, Feng T. Research on Data Transaction Security Based on Blockchain. *Information*, 2022; 3: 532.[DOI]

[15] Yaga D, Mell P, Roby N et al. Blockchain technology overview. arXiv preprint arXiv: 1906.11078, 2019.[DOI]

[16] Wang Q, Su M. Integrating blockchain technology into the energy sector-from theory of blockchain to research and application of energy blockchain. *Comput Sci Rev*, 2020; 37: 100275.[DOI]

[17] Rajasekaran AS, Azees M, Al-Turjman F. A comprehensive survey on blockchain technology. *Sustain Energy Techn*, 2022; 52: 102039.[DOI]

[18] Alqahtani AM, Algarni A. A Survey on Blockchain Technology Concepts, Applications and Security. I*nt J Adv Comput Sc*, 2023; 14: 841-847.[DOI]

[19] Panda M. Performance analysis of encryption algorithms for security 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). IEEE, 2016: 278-284.[DOI]

[20] Rihan SD, Khalid A, Osman SEF. A performance comparison of encryption algorithms AES and DES. *IJERT*, 2015; 4: 151-154.

[21] Kawle P, Hiwase A, Bagde G et al. Modified advanced encryption standard. *Int J Soft Comput Eng*, 2014; 4: 21-23.