RESEARCH ARTICLE

A secure sharing model of environmental monitoring data for remote environmental pollution control

Yunzhu Liu*

School of Computer Information Engineering, Nanchang Institute of Technology, Nanchang, Jiangxi, China.

Received: April 15, 2024; **accepted:** June 11, 2024.

The rapid development of industrialization and urbanization has made the environmental pollution problem in remote areas more prominent. However, this problem is often overlooked. This study attempted to construct an environmental monitoring data security sharing model for remote environmental pollution control to address this issue. A novel environmental monitoring model was proposed by introducing blockchain technology and the concept of cloud storage. A new data sharing model was proposed by combining symmetric encryption and asymmetric encryption algorithms. The results demonstrated that the maximum total storage capacity of the alliance chain + cloud storage node was 8.96 gigabytes with the minimum daily storage capacity of a single node reaching 0.47 megabytes. The maximum data transmission error of the data sharing model did not exceed 1 unit. The maximum throughputs of the carbon monoxide index and chemical oxygen demand were 9,400 and 1,950 kilobytes, respectively. Its latency data could reach a minimum of 24,117 milliseconds with the transmission energy consumption reaching a minimum of 30.7%. The data security and data integrity could reach the maximum of 92.4% and 99.7%. The proposed model had demonstrated excellent data transmission and security performance, which could provide a new technical reference for environmental monitoring and data security sharing in remote areas.

Keywords: remote areas; environmental monitoring; data sharing; data security; encryption; pollution.

***Corresponding author:** Yunzhu Liu, School of Computer Information Engineering, Nanchang Institute of Technology, Nanchang 330000, Jiangxi, China. Email: nanchang2024@126.com.

Introduction

The accelerated pace of industrialization and urbanization has led to a rise in environmental pollution concerns globally, particularly in remote areas [1]. The control of environmental pollution in remote areas is a challenging task, as these areas often lack the appropriate infrastructure and resources. Nevertheless, with the advancement of modernity and the evolution of scientific and technological disciplines, environmental monitoring in remote regions of China has been progressively enhanced. The conventional approach to environmental monitoring relies primarily on technical means with database storage serving as the primary repository for data and complemented by collection and analysis [2]. Although significant progress has been made in environmental monitoring technologies such as sensor technology, remote sensing technology, and the Internet of Things (IoT) in recent years, these advances are mainly concentrated in urban and industrial areas, and environmental monitoring in remote areas still faces significant challenges [3]. Meanwhile, the secure sharing of environmental monitoring data (EMD) has also become an important issue, as the data may contain sensitive information such as the location and type of pollution sources, and its leakage may bring security risks [4]. Ullo *et al*. proposed an intelligent environmental monitoring system by combining IoT and modern sensor technology to explore a more efficient technology for detecting environmental data in remote areas. The system showed excellent performance in monitoring air quality, water quality, and radiation pollution, and had strong robustness [5]. Kumar *et al*. successfully proposed a new type of glacier area environmental monitoring model (EMM) by combining remote sensing technology and image supervised learning technology to detect the environmental quality of glacier covered areas. This model could smoothly monitor the glacier environment changes in Bhutan over the past 20 years with an accuracy rate of up to 94.3% [6]. Lechner *et al.* constructed a new type of environmental monitoring sensor model using multi-spectral and synthetic aperture radar to achieve intelligent monitoring of forest environment in remote mountainous areas in western China. This model had shown excellent performance and stability in environmental quality monitoring in western mountainous areas [7]. Akbar *et al*. found that non-invasive load monitoring still faced issues such as signal noise and data privacy security in the current environmental monitoring process. Therefore, they proposed a novel EMD model by combining neural network algorithms, which showed some hope in performance testing, greatly optimizing the classification and recognition efficiency of EMD through neural networks [8].

EMD often contains a lot of sensitive information, which is of great significance for national construction and security protection. Therefore, establishing a secure EMD sharing model has become the key to environmental pollution control in remote areas. Pirbhulal *et al*. proposed a new data resource allocation encryption model by combining IoT technology and time slice rotation method to enhance the transmission security of EMD. The energy optimization efficiency of this model had been improved by 15% compared to that of traditional allocation encryption models [9]. Safara *et al*. found that uploading EMD to cloud storage through IoT technology faced three major challenges including fault tolerance, security, and energy consumption. Therefore, a new path energy-saving encryption method was proposed by combining low-power lossy network routing protocols and asymmetric encryption algorithms. This method could significantly reduce the network overhead of data transmission and improve security [10]. Dhanvijay *et al*. found that existing environmental monitoring systems were vulnerable to network attacks. Therefore, they proposed an advanced encryption standard (AES) password feedback authentication algorithm in combination with the security aware mobile management protocol. The network delay and switching delay of this algorithm had been significantly optimized, and the total transmission delay had been reduced by about 32.4% [11]. To further enhance the privacy and security of EMD during transmission and sharing, Ma *et al*. proposed a new data encryption model by combining attribute cryptography mechanism and dual key algorithm. The data encryption and decryption time of this method was shorter, and the cost was reduced by about 14% [12].

Numerous studies have concentrated on the development of hierarchical monitoring data management architectures. Conversely, researchers have proposed data resource allocation encryption models, path energy-saving encryption methods, and other solutions for the protection of environmental data. These methods can indeed strengthen the reliability of the EMD transmission process, but there are still problems such as data silo problem, data leakage, transmission delay, and slow feedback. This study aimed to construct a secure EMD sharing model and apply it in remote areas to enhance the safety and sharing efficiency of EMD in remote areas to effectively support the governance of environmental pollution. A new EMM was constructed by introducing blockchain technology and cloud storage concepts followed by the construction of a new data sharing model with the combination of AES and Ron Rivest-Adi Shamir-Leonard Adleman (RSA) encryption algorithms. The proposed model would improve the sharing efficiency and data security of environmental monitoring in remote areas and provide technical support for environmental protection.

Materials and methods

EMM combined with blockchain technology

To solve the data transmission and security problems of environmental pollution management models in remote areas, the study introduced blockchain technology for model optimization. Blockchain technology, as a decentralized and secure distributed database technology, can be well adapted to solve the problem of poor information in remote areas [13, 14] and is formed by public, consortium, and private chains (Figure 1). Compared to public and private chains, consortium chains allow participants to share data and participate in consensus mechanisms, while retaining a certain degree of privacy and control, making them more flexible and trustworthy [15, 16]. Therefore, this study chose alliance chain as the main framework for subsequent environmental monitoring network models. The alliance chain was maintained by multiple pre-selected nodes, and during this process, hash values were calculated to ensure data integrity and immutability as follows.

$$H(D) = hash(D) \tag{1}$$

where *H* (*D*) was the hash value of data *D*. *hash* (_) was the hash function. *D* was EMD, such as air quality, water quality indicators, *etc*. To ensure the reliability and non-repudiation of the data source, each data or transaction needed to be digitally signed by the sender [17]. Through transaction signature verification, any participant could verify that the data had not been tampered with and the source was genuine. The calculation formula for transaction signature verification was as below.

$$V(S, PK, H(D)) = true\, or\ false \tag{2}$$

where *V* (_) represented the previous validation function to verify whether the data hash signature was valid. *S* was the signature of the data transaction. *PK* was the public key of the signer. After verification, the data hash value, transaction list, hash of the previous block, and timestamp were packaged into a new block, which was calculated as follows.

$$B_n = \{H(B_{n-1}), T_n, H(D_n), timestamp\} \tag{3}$$

where B_n was the *n*-th block. $H(B_{n-1})$ was the hash value of the previous block B_{n-1}. T_n was the list of transactions within the block. *H* (D_n) was the hash value of the data within the block. *timestamp* was generated by the block. The consensus mechanism was the core of maintaining network consistency and security in the alliance chain [18]. In the application of environmental monitoring, consensus mechanisms such as proof of computing power or authoritative voting could be used to achieve this and the process of proving computational power was achieved using equation (4).

$$(x \,||\, H(B_{n-1}) \,||\, T_n \,||\, H(D_n)) < target \tag{4}$$

where *x* was a random number that satisfied the condition [-∞, +∞]. *target* was the preset target value for the network. Proof of computing power relied on solving complex computational problems to validate new blocks, while authoritative voting relied on the voting of pre-selected nodes to determine the effectiveness of the blocks. The calculation for authoritative voting consensus was shown in equation (5).

$$V_c = Majority(V_1, V_2, ..., V_m) \tag{5}$$

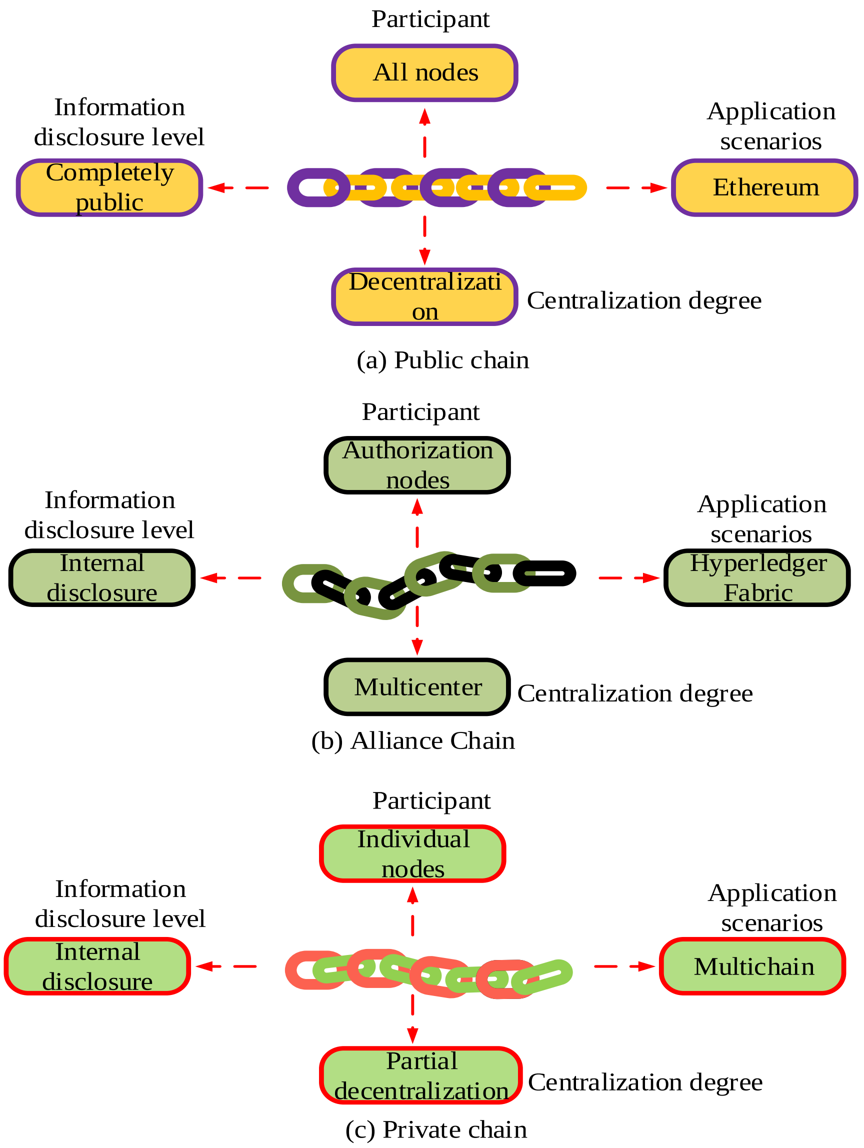


Figure 1. Classification of blockchain technology.

where V_c was the consensus result. *Majority* (_) was the majority voting function. V_m was the voting result of the *m*-th node. The privacy and security of data were controlled and ensured by setting data access permissions. The calculation of data access permissions was

$$Access(D_i, U_j) = true\, or\ \ false \tag{6}$$

where *Access* (_) was the access control function used to determine whether user U_j had access to data D_i. U_j was the *j*-th user or node. D_i was the *i*-th EMD. Through these mechanisms, this study attempted to establish a decentralized and trustworthy environmental data sharing platform, thereby promoting the efficiency and transparency of environmental protection and monitoring. The model of environmental monitoring in remote areas combined with alliance chain technology could be divided into pollution data collection layer (PDCL), environmental monitoring system combined with consortium chain (CCEMS), storage cloud (SC), and remote environmental monitoring scene

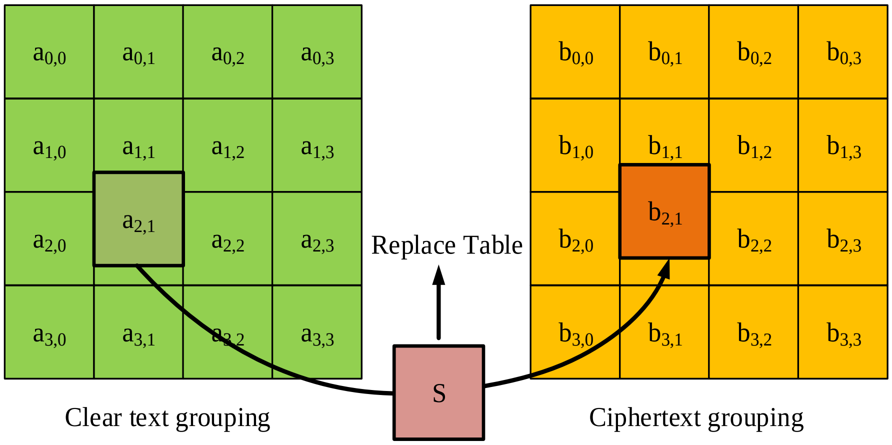

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
Replace Table
S
Clear text grouping
Ciphertext grouping

Figure 2. State matrix structure.

(REMS). PDCL was responsible for real-time data collection of multiple environmental indicators that included collection, transmission, and analysis functions. CCEMS was responsible for collecting EMDs from different deployment points and sending them to the blockchain for distribution arrangement. SC was responsible for storing fully arranged monitoring data in the blockchain including specific data and data sources. REMS was responsible for sharing the analyzed environmental data patterns among various departments, so that the data could be effectively utilized and used as a necessary condition to support decision-making.

EMD security encryption model based on AES-RSA

Due to the inevitable attacks and tampering of data during transmission, implementing data encryption is an indispensable means. Furthermore, considering the significant time and computational costs associated with this monitoring model, this study employed encryption algorithms from cryptography to optimize it. The existing more classical encryption algorithms can be categorized into symmetric and asymmetric encryptions. In symmetric encryption, the initial data is processed by the encryption algorithm and key to generate the ciphertext, and the receiver uses the same key for decryption. This method is fast, but the key transmission is not secure. In asymmetric encryption, the sender encrypts data using the receiver's public key, while the receiver decrypts it using a private key. Although the security of the system is assured, the speed of operation is somewhat slower. This study attempted to combine the advantages of symmetric encryption for data encryption and asymmetric encryption for optimizing the security of key transmission. AES is an efficient and secure symmetric encryption algorithm that is fast and suitable for encrypting large amounts of data [19, 20]. The state matrix was the core data structure of AES encryption, which could directly affect algorithm security and efficiency (Figure 2). Each element of the state matrix was a byte, which was 8 bits, totaling 16 bytes, arranged in column priority order. A replacement table was introduced to replace each byte of the input to increase confusion. Row shifting cyclically shifted each row of the state matrix to increase the complexity of encryption. Column mixing performed an obfuscation operation on each column of the state matrix to increase the strength of encryption. The round key plus put the current state matrix and the round key in an all-or-nothing operation (Exclusive OR, XOR) to increase the randomness and security of the encryption. The byte replacement was calculated using equation 7.

$$b' = S(b) = A \cdot (b^{254}) \oplus v \qquad (7)$$

where b was the original byte. b' was the replaced byte. b^{254} was the inverse element calculation of b, which was equivalent to b^{-1}. A was the replacement table used for the transformation. v was the fixed vector added in the replacement. The expression of round key addition was as below.

$$a_{i,j}^{'} = a_{i,j} \oplus k_{i,j} \tag{8}$$

where $a_{i,j}$ and $a_{i,j}^{'}$ were the current state and the bytes in row i and column j after the operation, respectively. $k_{i,j}$ was the byte in row i and column j of the round key. $\oplus$ was displacement. RSA is mainly used for encrypting and decrypting information in asymmetric encryption algorithms, especially suitable for symmetric encryption algorithms. The key steps of the RSA algorithm involved key generation, encryption, and decryption. The private key expression of RSA was equation 9.

$$d = e^{-1} mod \cdot \phi(n`) \tag{9}$$

where d was the private key index, which was used to decrypt data. e was the public key index. $\phi(n)$ was the Euler function. $n`$ was the modulus of public and private keys. The encryption process was then expressed in equation 10.

$$C = M^{e} mod(n) \tag{10}$$

where C was the encrypted ciphertext. M was the original plaintext message. The RSA algorithm relied on a pair of public and private keys with the public key used to encrypt data and the private key used to decrypt data. Assuming K_{AES} was the key of the AES algorithm, RSA public keys e and $n`$ were used for encryption optimization. The RSA encryption of AES keys was expressed in equation 11.

$$C_{K_{AES}} = K_{AES}^{e} mod(n) \tag{11}$$

where $C_{K_{AES}}$ was the AES key encrypted using the RSA public key. The process of decrypting AES keys using a private key was shown in equation 12.

$$K_{AES} = C_{K_{AES}}^{d} mod(n)d \tag{12}$$

where all algebraic explanations were consistent with the previous ones. The calculation for encrypting data using the optimized AES key was shown in equation 13.

$$C_{Data} = AES_{Encrypt}(K_{AES,} Data) \tag{13}$$

where $Data$ was the original data. C_{Data} was the data encrypted using AES key. $AES_{Encrypt}$ was the AES encryption function. By combining RSA and AES algorithms, AES keys could be securely exchanged to ensure the security of data transmission.

Model processing

The process of this model was mainly divided into data front-end collection, data encryption, data cloud storage, data decryption, data request, consensus detection, and consortium chain (Figure 3). The data storage tests for one of the blockchain + cloud storage models were conducted, while comparing with Blowfish algorithm (BA), RSA, and AES algorithms. The AES-RSA algorithm was then subjected to a series of tests to assess its multi-indicator performance. Finally, the shared model was tested in a practical setting to verify its viability for use. The hardware used for this study was Intel Core^{TM}i7-9700 CPU@3.00 GHz, 16 GB RAM, NVIDIA® GeForce® GTX 1660 SUPER™. The University of California, Irvine Machine Learning Repository - Air Quality Data Set (UIC-AQD) (https://archive.ics.uci.edu/dataset/360/air+quality) and Water Quality Data Set (WQDS) (https://archive.ics.uci.edu/ml/datasets/Water+Quality) were used as data sources. UIC-AQD contains air quality monitoring data from multiple remote cities including time series data of multiple indicators such as carbon monoxide

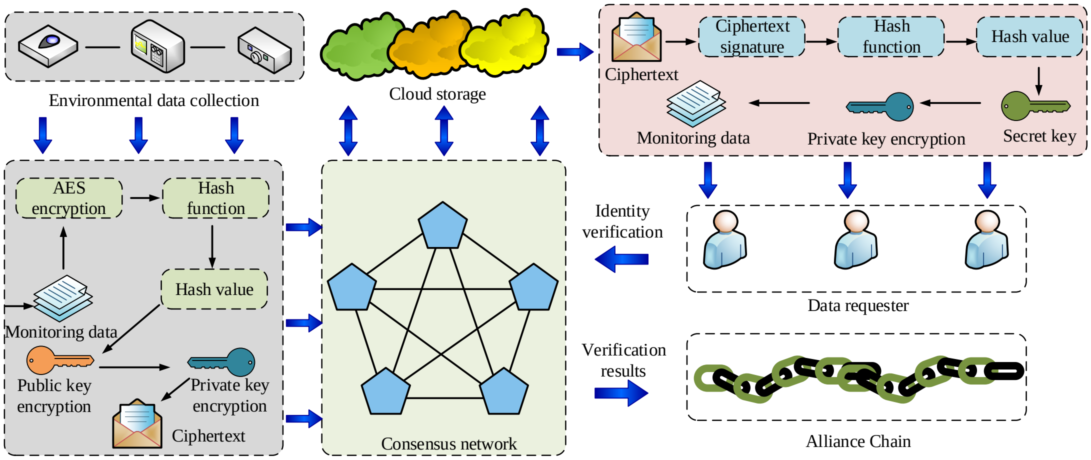


Figure 3. New environmental monitoring data security sharing model process.

(CO), non-methane hydrocarbons (NMHC), nitrogen oxides (NOx), ozone (O_3), with a total of about 50,000 pieces. WQDS contains water quality monitoring data from multiple rivers in Brazil including time series data on multiple water quality indicators such as pH value, dissolved oxygen (DO), chemical oxygen demand (COD), and total solid content (TSS) with a total of over 40,000 pieces of information. The EMD of each point was collected by the data front-end, encrypted and uploaded to the consensus network for verification and detection, and then stored in the consortium chain. Similarly, another part of the collected data was encrypted and uploaded to the cloud storage end. If there was a data request, the corresponding data was decrypted and then verified and detected through a consensus network. The consortium chain sent the corresponding matching data file to the data requester, and finally completed the EMD sharing operation.

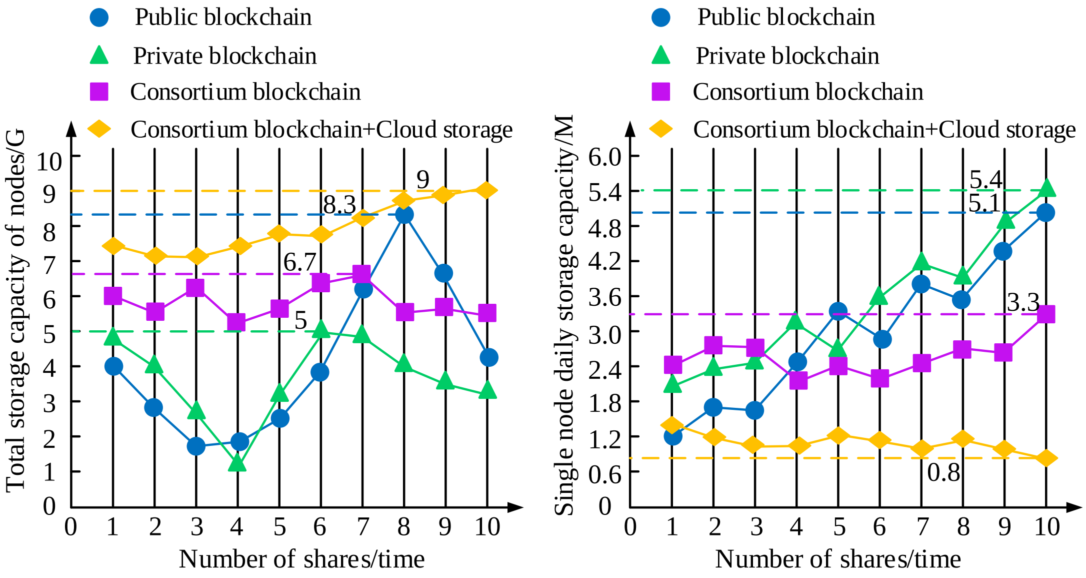
Results and discussion

Performance testing of EMD security encryption model

All data was run and implemented on Ubuntu (https://ubuntu.com/). This study first conducted comparative tests on the use of public chain, private chain, consortium chain, and consortium chain + cloud storage. Under the three different EMD quantities provided by the two types of datasets, as the initial data volume increased, the total storage capacity of nodes under the four storage technologies from public chain to private chain, consortium chain, and consortium chain + cloud storage continued to increase (Table 1). The results demonstrated excellent data resource storage capabilities with the maximum total storage capacity of the alliance chain + cloud storage node being 8.96 G. The minimum daily storage capacity of a single node in alliance chain + cloud storage was 0.47 M, which was significantly lower than that of the other three blockchain technologies. The reason behind this was that the combination of consortium chain and cloud storage could effectively alleviate the data storage pressure of individual environmental monitoring points, upload more data to the cloud, and optimize the performance of the entire environmental monitoring system. This study continued to test storage stability and examined the performance effects of four storage technologies under different data sharing frequency backgrounds (Figure 4). The results of the changes in total node storage and daily single node storage with the number of shares for the four technologies showed that the data performance of the alliance chain was relatively stable with a storage range of no more than 2 G. The maximum storage capacity of

Table 1. Capacity testing results of different data storage technologies.

Data set	Monitor data (K)	Total storage capacity of nodes				Daily storage capacity of nodes			
		Public blockchain (G)	Private blockchain (G)	Consortium blockchain (G)	Consortium blockchain + cloud storage (G)	Public blockchain (M)	Private blockchain (M)	Consortium blockchain (M)	Consortium Blockchain + cloud storage (M)
UIC-AQD	1.86	1.73	1.83	2.41	4.02	2.02	2.05	1.15	0.58
	3.54	3.02	2.94	3.25	6.52	3.68	3.84	1.68	0.64
	5.53	5.21	5.17	5.54	8.96	5.69	5.69	2.58	0.97
WQDS	1.86	1.62	2.23	2.47	4.98	2.12	2.10	1.13	0.47
	3.54	3.01	2.76	2.89	5.52	3.74	3.27	1.87	0.68
	5.53	5.14	5.03	5.44	8.07	5.87	5.61	2.89	1.02



(a) Changes in total storage capacity of nodes

(b) Changes in daily storage capacity of a single node

Figure 4. Comparative testing of total node and individual node storage capacity for different technologies.

nodes in the alliance chain + cloud storage was 9 G, and it was steadily increasing. In addition, apart from the alliance chain and cloud storage technologies, the daily storage volume of a single node was on the rise, indicating that the workload of a single node was relatively heavy, and the operating pressure was high. The combination of alliance chain and cloud storage showed a low storage capacity and a stable downward trend with a minimum daily storage capacity of 0.8 M per node, indicating that this combination could provide lower storage consumption and faster storage response speed. After comparing several popular encryption storage technologies using latency as the testing metric, the results showed that, as the amount of EMD increased, the latency of BA and RSA algorithms could reach up to 7×10^5 ms and 1×10^5 ms, respectively. The encryption processing effect of AES was slightly better than that of the first two algorithms with a maximum latency of 7×10^4 ms. AES-RSA showed the best latency effect with a maximum latency of only 6×10^3 ms and a minimum latency of 4×10^2 ms (Figure 5). In addition, for processing the same amount of environmental data, the number of nodes

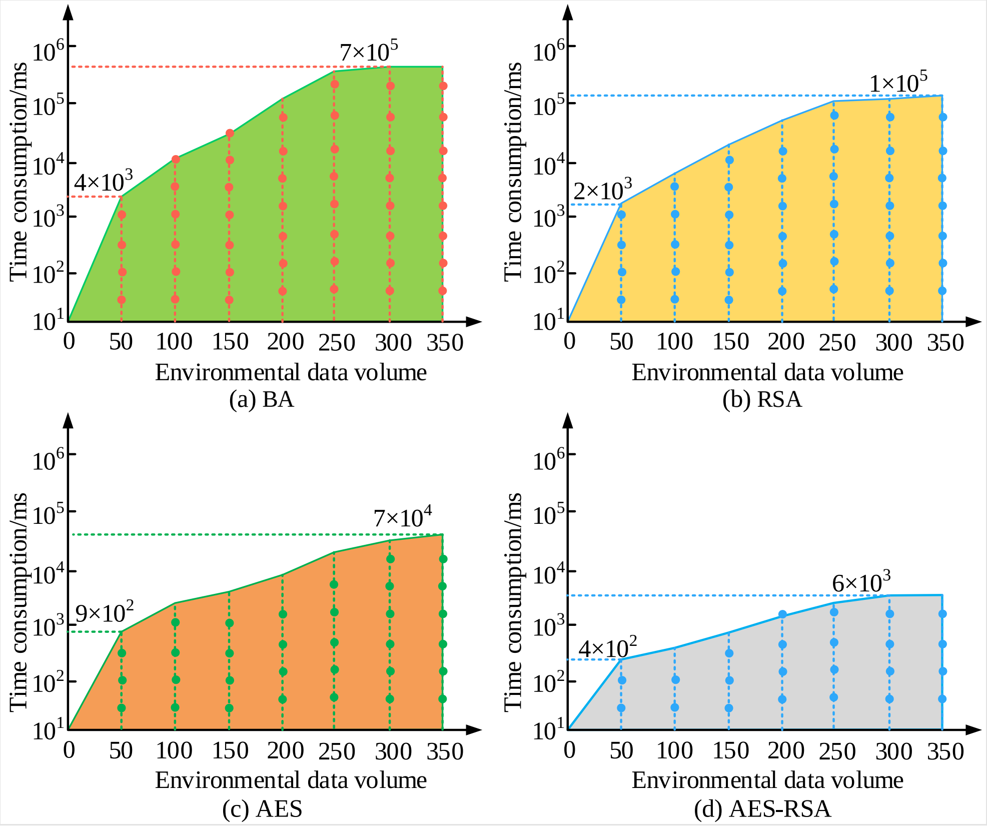


Figure 5. Delay test results of different encryption algorithms.

required for BA, RSA, and AES was significantly lower than that of AES-RSA with two nodes being the least. The results indicated that the proposed model had certain encryption advantages with AES encrypting data at a faster speed and RSA only being used for encrypting and decrypting AES keys that did not require operations on the entire data.

EMD security encryption model simulation test

The concentrations of CO and DO were taken as the test objects in this study for the performance comparison with popular data transmission models of the same type such as Peer-to-Peer model (P2P), Message Queue model (MQ), Cellular Network model (CN). The individual computers of P2P were directly connected to each other and shared resources and information without relying on a central server. MQ allowed applications to exchange data by queuing and processing messages asynchronously, thereby decoupling and increasing the scalability and reliability of the system. CN was a wireless communication network that enabled wide-area user equipment by dividing a geographic area into a number of cellular cells, each of which was covered by a communication base station [21-23]. The comparison curves of CO and DO transmission results obtained from four models were shown in Figure 6. The monitoring concentration data changes of AES-RSA were most consistent with the actual changes of CO and DO concentrations with both maximum errors in the trend data not exceeding 1 unit. Therefore, AES-RSA had a certain data transmission efficiency, which could ensure the authenticity and integrity of data. In addition, this study continued to test the above four methods using system throughput under different air and water quality indicators. The AES-RSA models all showed significant throughput advantages with the maximum throughputs of 9,400 KB in CO

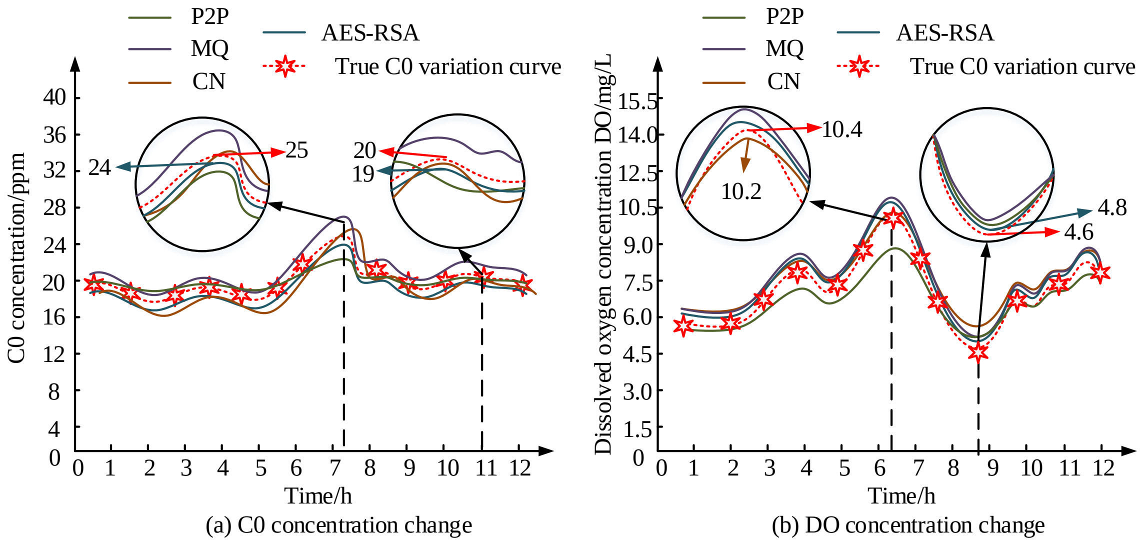


Figure 6. Performance test results of different data transmission models. The actual changes of CO and DO concentrations followed the r ed curve.

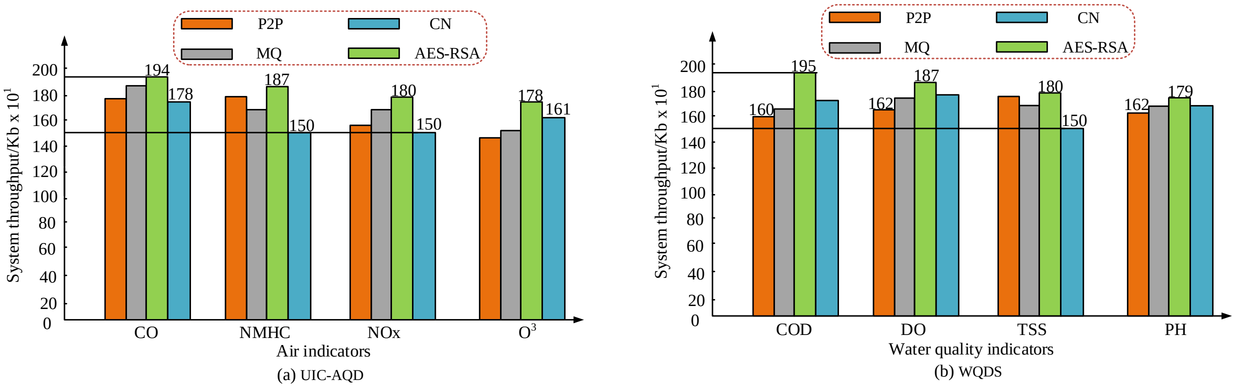


Figure 7. Test results of model throughput under two types of environmental indicators.

detection in air index testing and 1,950 KB under COD in water quality testing, which was much higher than that of the other three methods (Figure 7). Therefore, the AES-RSA model had a certain degree of robustness in existing EMD transmission tasks and could adapt to efficient data transmission in different environments. The four methods were then compared on data transmission delay, transmission energy consumption, data security, and data integrity. The results demonstrated that both P2P and MQ showed significant transmission delays of 157,966 ms and 120,447 ms, respectively. For both datasets, the AES-RSA model showed the lowest latency data of 24,117 ms (Table 2). In addition, in the energy consumption test during EMD transmission, the AES-RSA model reached a minimum of 30.7%, while the P2P model reached a maximum of 57.6% with a difference of 26.9%. Meanwhile, AES-RSA had a data security of up to 92.4% and data integrity of up to 99.7%.

This study introduced blockchain technology to facilitate the monitoring and deployment of information in remote areas and AES and RSA encryption algorithms to encrypt and safeguard the EMD. The proposed new EMD sharing model with security showed excellent performance in terms of data storage capacity, storage stability, transmission delay, transmission energy

Table 2. Test results of indicators for different data transmission guarantee models.

Data set	Model	Transmission delay (ms)	Transmission energy consumption (%)	Data security (%)	Data integrity (%)
UIC-AQD	P2P	157966	57.6	78.4	97.4
	MQ	120447	48.9	82.5	96.2
	CN	94287	40.2	80.2	98.4
	AES-RSA	45776	37.2	90.4	99.4
WQDS	P2P	135529	54.8	82.9	97.8
	MQ	108879	46.9	85.4	98.1
	CN	62589	39.2	87.3	98.6
	AES-RSA	24117	30.7	92.4	99.7

consumption, data security, and data integrity. However, the stability and scalability of the research results in extreme environments need to be further verified. Future work can focus on the adaptability of the model in a wider range of application scenarios, as well as enhancing the comprehensiveness of the study.

References

1. Kaplan G, Rashid T, Gasparovic M, Pietrelli A, Ferrara V. 2022. Monitoring war-generated environmental security using remote sensing: A review. Land Degrad Dev. 33(10):1513-1526.
2. Durairaj UM, Selvaraj S. 2022. Two-level clustering and routing algorithms to prolong the lifetime of wind farm-based WSN. IEEE Sens J. 21(1):857-867.
3. Lapworth L. 2022. Parallel encryption of input and output data for HPC applications. Int J High Perform Comput Appl. 36(2):231-250.
4. Fang D, Qian Y, Hu RQ. 2020. A flexible and efficient authentication and secure data transmission scheme for IoT applications. IEEE Internet Things J. 7(4):3474-3484.
5. Ullo SL, Sinha GR. 2020. Advances in smart environment monitoring systems using IoT and sensors. Sens. 20(11):3113-3114.
6. Kumar M, Al-Quraishi AMF, Mondal I. 2021. Glacier changes monitoring in Bhutan High Himalaya using remote sensing technology. Environ Eng Res. 26(1):190-255.
7. Lechner AM, Foody GM, Boyd DS. 2020. Applications in remote sensing to forest ecology and management. One Earth. 2(5):405-412.
8. Akbar MK, Amayri M, Bouguila N. 2024. A novel non-intrusive load monitoring technique using semi-supervised deep learning framework for smart grid. Build Simul. 17(3):441-457.
9. Pirbhulal S, Wu W, Muhammad K, Mehmood I, Li G, Albuquerque VHC. 2020. Mobility enabled security for optimizing IoT based intelligent applications. IEEE Network. 34(2):72-77.
10. Safara F, Souri A, Baker T, Al Ridhawi I, Aloqaily M. 2020. PriNergy: a priority-based energy-efficient routing method for IoT systems. J Supercomput. 76(11):8609-8626.
11. Dhanvijay MM, Patil SC. 2021. Optimized mobility management protocol for the IoT based WBAN with an enhanced security. Wirel Netw. 27(1):537-555.
12. Ma H, Zhang Z. 2020. A new private information encryption method in Internet of Things under cloud computing environment. Wireless Commun Mobile Comput. 2020(6):1-9.
13. Wang Y, Wang J, Chang S. 2021. Classification of street tree species using UAV tilt photogrammetry. Remote Sens. 13(2):216-217.
14. Chung D, Lee S, Choi D, Lee J. 2022. Alternative tower field construction for quantum implementation of the AES S-Box. IEEE Trans Comput. 71(10):2553-2564.
15. Bandewad G, Datta KP, Gawali BW, Pawar SN. 2023. Review on discrimination of hazardous gases by smart sensing technology. Artif Intell Appl. 1(2):86-97.
16. Shen J, Yang H, Vijayakumar P. 2021. A privacy-preserving and untraceable group data sharing scheme in cloud computing. IEEE Trans Dependable Secure Comput. 19(4):2198-2210.
17. Tan L, Yu K, Shi N. 2021. Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach. IEEE Trans Network Sci Eng. 9(1):271-281.
18. Narayanan U, Paul V, Joseph S. 2022. A novel system architecture for secure authentication and data sharing in cloud enabled big data environment. J King Saud Univ - Comput Inf Sci. 34(6):3121-3135.
19. Cui J, Ouyang F, Ying Z. 2021. Secure and efficient data sharing among vehicles based on consortium blockchain. IEEE Trans Intell Transp Syst. 23(7):8857-8867.
20. Feng C, Yu K, Bashir AK. 2021. Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach. IEEE Network. 35(1):130-137.
21. Miao L, Lin M, Wei W. 2023. Peer regulation in a peer-to-peer business model. J Hosp Tour Res. 47(5):908-926.
22. Maharjan R, Chy MSH, Arju MA. 2023. Benchmarking message queues. Telecom. 4(2):298-312.
23. Sajan B, Mishra VN, Kanga S. 2022. Cellular automata-based artificial neural network model for assessing past, present, and future land use/land cover dynamics. Agron. 12(11):2772-2773.