Heliyon 11 (2025) e39462

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

# Enhancing smart healthcare networks: Integrating attribute-based encryption for optimization and anti-corruption mechanisms

Yanzhao Zeng [a,1], Xin Guan [b], Jingjing Sun [c,1], Yanrui Chen [c], Zeyu Wang [c,1], Peng Nie [a,*]

[a] *School of Economics and Statistics, Guangzhou University, Guangzhou, 510006, China*
[b] *Guangzhou Xinhua University, Dongguan, 523133, China*
[c] *School of Public Administration, Guangzhou University, Guangzhou, 510006, China*

ARTICLE INFO

*Keywords:*
Smart healthcare networks
Attribute-based encryption
Data security
Data transmission speed
Anti-Corruption mechanisms

ABSTRACT

This study investigates the feasibility and effectiveness of integrating Attribute-Based Encryption (ABE) into smart healthcare networks, with a particular focus on its role in enhancing anti-corruption mechanisms. The study provides a comprehensive analysis of current vulnerabilities in these networks, identifying potential data security risks. An anti-corruption mechanism is designed to ensure data integrity and reliability. The ABE approach is then empirically compared to other prominent encryption algorithms, such as Identity-Based Encryption, Data Encryption Standard, Advanced Encryption Standard, and Rivest-Shamir-Adleman algorithms. These methods are evaluated based on access latency, data transmission speed, system stability, and anti-corruption capabilities. Experimental results highlight the strengths of the ABE algorithm, demonstrating an average access latency of 31.6 ms, a data transmission speed of 3.56 MB/s, and an average system stability of 98.74 %. Furthermore, when integrated into anti-corruption mechanisms, ABE effectively protects against data tampering and misuse, ensuring secure data transmission. Compared to alternative algorithms, ABE offers a more efficient, secure, and stable solution for data management within smart healthcare networks, supported by its robust anti-corruption capabilities. This positions ABE as an optimal choice for safeguarding the integrity and security of healthcare data.

## 1. Introduction

Recent advancements in information technology have significantly progressed smart healthcare networks, fundamentally transforming the healthcare system [1–3]. These networks utilize cutting-edge technologies, such as cloud computing and the Internet of Things (IoT), to digitize, network, and manage medical data intelligently. This enhances information exchange between medical professionals and patients, offering unprecedented convenience and efficiency [4–6]. However, the exponential growth of medical data has also increased vulnerabilities within these networks, exposing them to threats from external hackers, internal misuse, and other security risks, thereby raising concerns about data privacy and security [7,8]. As sensor technology, mobile health applications,

[*] Corresponding author.
*E-mail addresses:* zyzcl@e.gzhu.edu.cn (Y. Zeng), guanxin@xhsysu.edu.cn (X. Guan), sunjingj7966@gzhu.edu.cn (J. Sun), chenyanrui@e.gzhu.edu.cn (Y. Chen), theowang@gzhu.edu.cn (Z. Wang), niepeng@gzhu.edu.cn (P. Nie).
[1] These three authors considered as co-first authors: Yanzhao Zeng, Jingjing Sun and Zeyu Wang.

https://doi.org/10.1016/j.heliyon.2024.e39462
Received 27 March 2024; Received in revised form 4 October 2024; Accepted 15 October 2024
Available online 16 October 2024

and cloud computing platforms evolve rapidly, the generation and transmission speed of medical data have significantly accelerated, enabling extensive applications in personalized medicine, remote monitoring, and diagnostics. Yet, alongside these advancements, concerns about data security and privacy protection are becoming increasingly urgent [9].

Moreover, challenges related to corruption in the healthcare sector present urgent issues that require immediate attention [10]. Corrupt practices disrupt the equitable distribution of healthcare resources and negatively impact patients' experiences [11]. Therefore, establishing an effective anti-corruption mechanism is essential for optimizing smart healthcare networks [12]. By utilizing data analysis and early warning systems, corrupt activities can be identified and mitigated promptly, thereby enhancing transparency and integrity within the healthcare system [13]. In traditional medical information systems, data security primarily relies on conventional encryption technologies, such as symmetric and public key encryption. For instance, Indushree and Raj [14] developed a secure decentralized authentication framework using blockchain for remote healthcare information systems. Their findings demonstrate that the proposed framework ensures security, efficiency, and practical feasibility in healthcare applications. Another notable approach is presented by Rupa [15], who introduced a homomorphic encryption technique based on matrix transformations involving shifting, rotating, and transposing ASCII values of plaintext characters. This method aims to enhance data security through innovative encryption methodologies. Additionally, Man [16] explored the security vulnerabilities of cloud data and proposed an image encryption scheme that utilizes neural networks. Performance analysis revealed the robust security capabilities of this algorithm.

Despite advancements in ensuring data confidentiality, traditional methods exhibit certain limitations, particularly regarding data access control and flexibility. With the expanding diversity and volume of medical data, along with increasing demands for efficient storage management, there is a critical need for smarter and more adaptable security solutions to address the complex challenges of data management in healthcare systems effectively. Moreover, issues such as medical data breaches, tampering, and misuse have become increasingly prevalent, posing significant threats to patient privacy and undermining trust in healthcare systems [17,18]. While traditional encryption algorithms provide some level of data protection, their security is vulnerable to evolving network attacks and sophisticated computational techniques [19–21]. As the complexity and sensitivity of medical data continue to rise, existing security mechanisms struggle to address these challenges effectively. The diversity and high value of medical data make it a prime target for attackers, while protecting patient privacy presents significant obstacles. Additionally, the efficiency of resource allocation and management within intelligent medical networks requires further optimization to meet the growing demands for data processing. Consequently, there is increasing interest in advanced Attribute-Based Encryption (ABE) as a crucial area of research [22]. ABE algorithms not only enhance the privacy of medical data but also provide flexible control over data access permissions, ensuring robust security even in situations where authorized access is permitted [23–25].

In this context, ABE technology emerges as an innovative encryption method that offers significant advantages in fine-grained access control and data protection. This technology has been successfully applied across various fields, particularly excelling in the management of highly sensitive and distributed data. The integration of ABE technology presents an effective solution for intelligent medical networks, enhancing system security and improving resource management efficiency. The primary objective of this study is to optimize intelligent medical networks through the incorporation of ABE technology while also introducing anti-corruption mechanisms to enhance system transparency and reliability. These improvements are intended to provide robust technical support for the development of intelligent medical networks, thereby facilitating the digital transformation of the entire healthcare industry.

The main contributions and innovations of this study are summarized as follows.

1) Optimization Method: This study proposes a method that combines cloud computing and edge computing to enhance the performance of intelligent medical networks. By leveraging the powerful computational capabilities of cloud computing alongside the low-latency characteristics of edge computing, this approach optimizes data processing and transmission efficiency. This hybrid architecture not only improves overall system response speed but also significantly reduces bandwidth requirements and latency during data transmission, thereby enhancing the adaptability of the medical network in complex environments.
2) Application of ABE Technology: This study innovatively applies ABE technology to intelligent medical solutions to address challenges related to data security and privacy protection. Unlike traditional encryption methods, ABE technology provides fine-grained access control and facilitates dynamic permission management based on user attributes. The introduction of this technology greatly enhances the security of medical data, ensuring confidentiality and integrity during transmission and storage, particularly in collaborative medical scenarios.
3) Anti-Corruption Mechanism: To combat data corruption and unauthorized access within medical systems, this research designs and implements a comprehensive anti-corruption mechanism. By integrating ABE technology, this mechanism can detect and prevent data tampering in real time while effectively blocking unauthorized users from accessing sensitive information. The design of this mechanism significantly enhances the transparency and reliability of medical systems, providing crucial technical support for building a more secure intelligent medical network.

The structure of this paper is organized as follows:

The first section serves as the introduction, presenting the research background, motivation, and main contributions of the study. The second section reviews relevant literature and technological background, focusing on the applications of cloud computing, edge computing, and ABE technology in intelligent medical networks. The third section elaborates on the research methods, detailing the optimization design of intelligent medical networks, the integration of ABE technology, and the implementation of the anti-corruption mechanism. The fourth section presents experimental results and discussions, evaluating the performance of the proposed methods and their potential for practical application. Finally, the fifth section summarizes the research findings and outlines future research directions.

## 2. Literature review

IoT technology facilitates real-time connectivity among various medical devices, enabling instant communication between patients, healthcare providers, and devices. However, increased awareness of security vulnerabilities during data transmission and storage has raised concerns. Wang [26] emphasized that the rapid advancement of communication network technologies, alongside the emergence of virtual communities, societies, and metaverses, has not only enhanced data accessibility and sharing but has also contributed to the proliferation of misinformation. Su [27] examined the significance of key attributes of medical data within social networks and introduced a greedy clustering algorithm to group data points based on the attributes and connection information of nodes already published in these networks.

Soni and Singh [28] proposed an innovative data communication scheme employing cost-effective encryption techniques capable of withstanding various security and privacy attacks while requiring minimal computational resources. Zhang [29] presented a privacy-enhanced optimization solution for neighborhood-based recommendation systems in medical diagnosis, ensuring secure and privacy-preserving recommendations without disclosing sensitive patient information. Praveen and Pabitha [30] introduced an enhanced Gentry-Halevi-based fully homomorphic encryption scheme for lightweight privacy-preserving user authentication. This scheme utilized integer matrix computation strategies to safeguard data computation, ensuring the privacy of medical data. Liu [31] proposed a fine-grained medical data sharing solution based on federated learning. This approach incorporated collaborative ABE techniques to formulate fine-grained access policies, allowing medical institutions or healthcare providers to decrypt data individually or collaboratively under specific conditions to accurately select the required medical data.

Almalawi [32] proposed the Lionized Remora Optimization-based Serpent encryption method, a novel approach designed to encrypt sensitive data and mitigate privacy leaks while thwarting network attacks by unauthorized users and hackers. Kumar [33] developed a blockchain-orchestrated deep learning framework for secure data transmission within IoT healthcare systems. Experiments demonstrated superior performance compared to state-of-the-art technologies in both blockchain and non-blockchain environments. Jaime [34] conducted a comprehensive analysis of intricate security challenges in IoT communication related to biomedical microelectromechanical systems. This research addressed vulnerabilities such as network threats, data manipulation, and communication interception. The integration of real-case studies elucidates the direct impacts of these security vulnerabilities on smart healthcare systems, emphasizing the need to safeguard patient safety and preserve the integrity of medical data.

For instance, Namasudra and Roy [35] proposed a novel access control scheme for efficient data access. While this scheme performs exceptionally well in specific environments, its applicability and flexibility may be limited, particularly in addressing the complex data access requirements inherent in intelligent medical networks. Additionally, Elharrouss [36] conducted a comprehensive review of 3D point cloud tasks, classifying existing technologies based on algorithm characteristics, application scenarios, and objectives. Although this classification approach provides guidance for understanding and selecting appropriate algorithms, it primarily focuses on visual processing, which has limited relevance to medical data management.

Gupta and Namasudra [37] introduced a real-time migration optimization technique that effectively enhances system performance and reduces migration latency within trusted cloud computing environments. However, the direct application of this technique in intelligent medical networks remains unvalidated, particularly concerning the security and privacy requirements of medical data. Wang [9] optimized network systems through blockchain technology, employing smart contracts and risk association tree techniques for managing online public opinion. While this study emphasizes using blockchain to enhance the security and controllability of network environments, its primary focus on online public opinion management does not fully align with the encryption and transmission needs of medical data. Regarding anti-corruption mechanisms, Wang [38] enhanced the capacity of grassroots governments to prevent and combat corruption by introducing data platform management and a "5W" analytical framework. This research illustrates methods for optimizing government management through data analysis and public engagement, but its subjects and application domains are primarily centered on public administration rather than intelligent medical networks. Nonetheless, the presented study draws on the idea of evaluating system effectiveness through temporal frameworks and performance indicators, applying it to the assessment of security mechanisms in medical data management.

However, despite notable advancements in research, current studies exhibit several limitations. Firstly, existing research on the application of ABE algorithms primarily remains theoretical, with insufficient exploration of practical implementations within healthcare networks. Secondly, in the design of anti-corruption mechanisms, current methods may detect certain instances of corrupt behavior but often struggle to identify new and covert forms of corruption.

Numerous studies have examined the application of traditional encryption techniques for securing medical data; however, these methods face challenges when addressing complex access control requirements. For example, while symmetric encryption and public key encryption effectively safeguard data confidentiality, they are less effective in managing dynamic and fine-grained access control scenarios. Additionally, efforts to introduce ABE have largely remained theoretical, lacking substantial practical application and performance evaluation. This gap underscores the need for more empirical studies to validate the feasibility and efficacy of ABE technology within smart healthcare networks. Moreover, achieving a balance between security and performance presents a significant challenge that directly impacts the practicality of real-world implementations. Consequently, practical case studies are urgently needed to substantiate the feasibility and effectiveness of ABE technology in real-world healthcare contexts. Furthermore, integrating robust data integrity protection and anti-corruption mechanisms is essential for delivering comprehensive data security solutions. This study aims to bridge these research gaps by addressing the practical requirements of real-world healthcare networks. It proposes an optimization solution for intelligent healthcare networks based on advanced ABE algorithms and designs an efficient anti-corruption mechanism, providing a more pragmatic approach to enhancing the security and integrity of healthcare networks.

## 3. Research methodology

### 3.1. Optimization of smart healthcare networks based on cloud computing and edge computing

A multi-layered optimization strategy is implemented to enhance the performance and security of smart healthcare networks. Initially, an intelligent data distribution system is developed to allocate medical data between the cloud computing center and edge computing devices intelligently. This allocation is based on factors such as data type, urgency, and the status of the target device, aiming to minimize data transmission latency and ensure real-time data delivery. Furthermore, data compression and encryption technologies are introduced to optimize system efficiency and data security. Data compression reduces the volume of transmitted data, while an ABE algorithm ensures robust security during both transmission and storage phases. The selected ABE algorithm facilitates the creation of intricate access policies, enabling fine-grained control over data access. Upon data reception, corresponding decryption and decompression algorithms are designed to accurately restore and process the data, completing the secure and efficient data transmission cycle.

In addition, edge computing technology is introduced to significantly enhance the performance of the smart healthcare network. Lightweight computing modules are deployed on edge devices, equipping them with essential data processing and analysis capabilities. During data transmission, certain computational tasks are offloaded to these edge devices for processing, thereby reducing the load on the cloud computing center and minimizing data transmission latency. Moreover, an intelligent task allocation algorithm is designed to meet the specific requirements of the healthcare network. This algorithm distributes tasks to appropriate edge devices based on task complexity and device load, enabling real-time processing and analysis of medical data. The specific architecture of the smart healthcare network optimization system is illustrated in Fig. 1.

In Fig. 1, the smart healthcare network optimization system is illustrated as a complex network structure comprising multiple key components designed to achieve real-time, secure, and efficient data transmission. The data generation and collection module is responsible for gathering information such as patient medical records and physician diagnosis records. The intelligent data distribution system serves as the core component, intelligently directing medical data to either the cloud computing center or edge computing devices based on factors such as data type, urgency, and the status of the target devices. The cloud computing center acts as a robust computational and storage hub, centralizing the processing of medical data. Within this center, data undergoes decryption, decompression, and processing, which includes data analysis and mining. Edge computing devices, lightweight computing modules situated at the periphery of the healthcare network, handle certain computational tasks. By delegating processing to these edge devices, the system alleviates the burden on the cloud computing center and reduces data transmission latency.

An intelligent task allocation algorithm assigns tasks to appropriate edge devices based on task complexity and device workloads, enabling real-time processing and analysis of medical data directly on these devices. This allocation enhances the system's

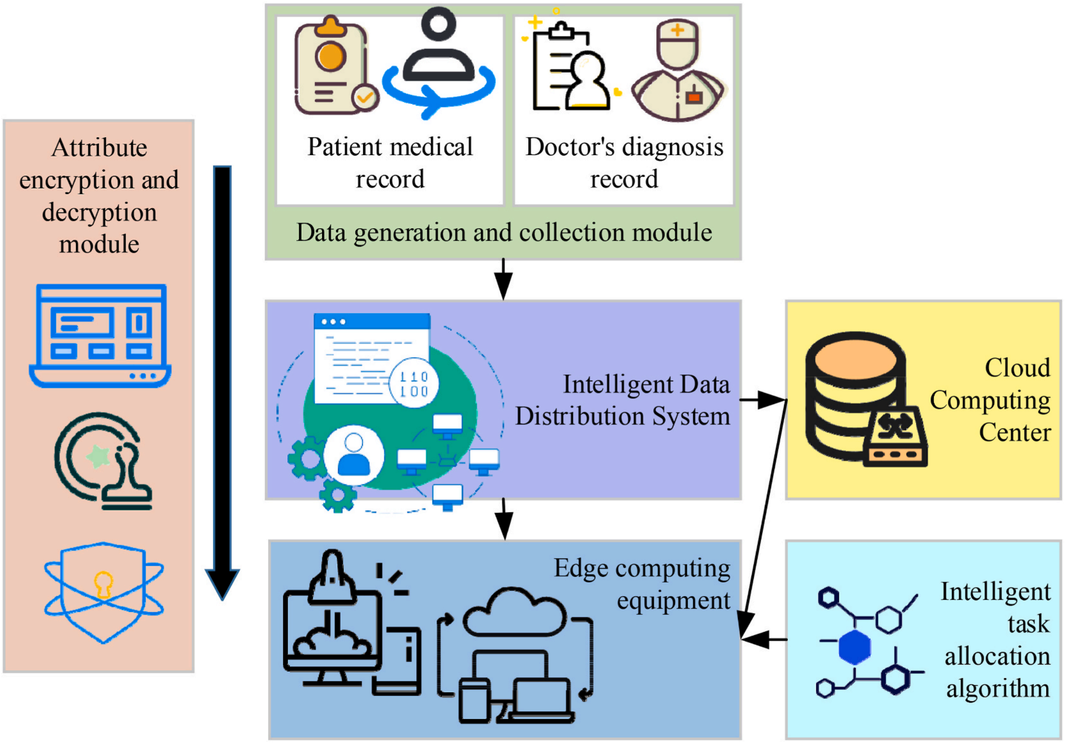
Attribute encryption and decryption module
Patient medical record
Doctor's diagnosis record
Data generation and collection module
Intelligent Data Distribution System
110
100
Cloud Computing Center
Edge computing equipment
Intelligent task allocation algorithm

**Fig. 1.** Architecture of the smart healthcare network optimization system.

responsiveness and efficiency. The attribute encryption and decryption module is responsible for ensuring data security during transmission. Medical data is encrypted to restrict access to authorized users only, with ABE algorithms managing data access rights based on specified policies, thereby safeguarding data privacy. The cohesive integration of these technological measures facilitates secure data transmission, real-time processing, and efficient distribution of medical data across the smart healthcare network.

### 3.2. *Attribute-based encryption for smart healthcare solutions*

The optimizations discussed in the previous section have improved the system's processing efficiency and response speed, establishing a solid foundation for the stable operation of the entire network. Building upon this optimization framework, ABE technology is employed to enhance data security and privacy protection. Ensuring the privacy and secure transmission of medical data is paramount within smart healthcare networks. While traditional encryption algorithms provide a level of data security, the medical field demands stringent requirements for fine-grained data access control and adaptability to dynamic needs. To address these challenges, ABE is introduced and seamlessly integrated into the smart healthcare network optimization solution. This innovative approach significantly enhances the protection of medical data privacy. Central to this solution is the key policy-based attribute encryption method for transmitting medical data, as illustrated in Fig. 2.

The application process of the ABE algorithm comprises three primary stages: key generation, encryption, and decryption. A detailed illustration of this process is presented in Fig. 3.

In Fig. 3, the Key Generation stage involves the initial setup of parameters on the elliptic curve, including a large prime number $p$ and a generator $g$. When a medical institution or user registers, their corresponding user public key ($pk$) is generated based on specific attributes, which may include professional titles, departments, and medical permissions. The generation process of the user public key involves computations using system parameters and the user's attributes. Upon registration, the system administrator generates the user's private key ($sk$), which is then provided to the user. During the encryption stage, the data owner selects the medical data for transmission and establishes the corresponding access policy. This policy is converted into an access tree, where the nodes represent the conditions under which the data can be decrypted, constructed based on the user's attributes. A random encryption key $r$ is then selected. For each node in the access tree, the corresponding ciphertext fragments $C_1$ and $C_2$ are computed as follows:

$$C_1 \in g^r \tag{1}$$

$$C_2 = m \times e\left(g^{msk \cdot attr}, g^r\right) \tag{2}$$

Here, $m$ signifies the message to be encrypted, while $g$ represents the generator on the elliptic curve, typically used for computing group elements. The term $r$ refers to a randomly selected encryption key that contributes to the generation of the ciphertext. $e$ signifies the pairing operations on the elliptic curve, utilized to combine generated group elements and keys. The master key, indicated as $msk$, serves as the global key to the system during the encryption and decryption processes. Finally, $attr$ represents the attributes specified in

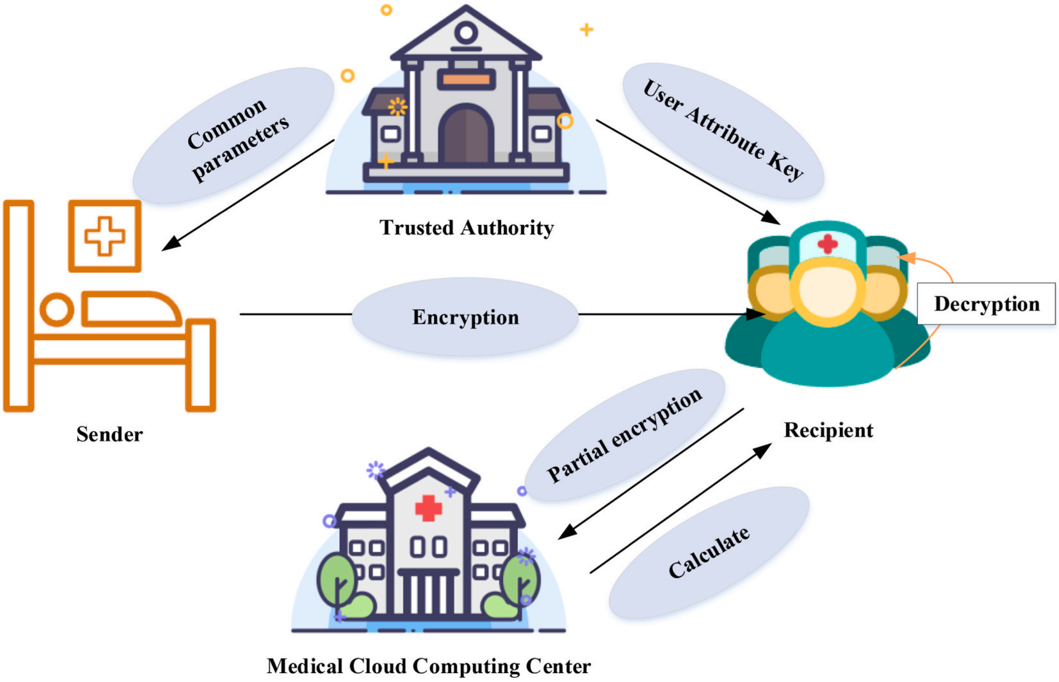

**Fig. 2.** Key policy-based attribute encryption for medical data transmission solution.

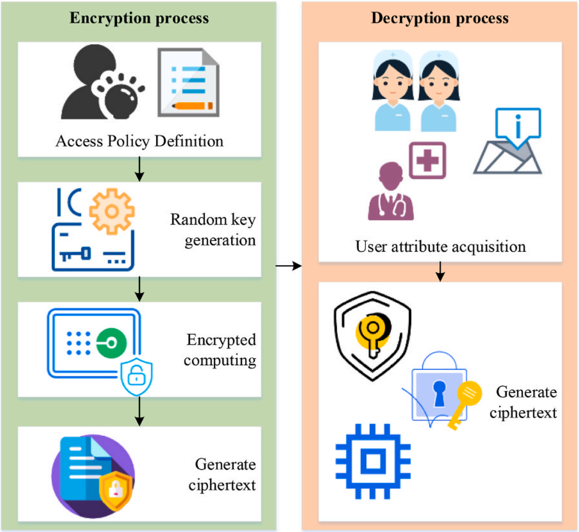

**Fig. 3.** ABE Algorithm process.

the access policy, which determine the users authorized to decrypt the message.

If the user's attributes satisfy the criteria of a given node, the public key information associated with that node is utilized for encryption. As a result, all ciphertext fragments collectively form the encrypted data, denoted as ciphertext *C*.

$$\mathrm{C} = (C_1, C_2) \tag{3}$$

During the decryption phase, when a user or doctor requests access to the encrypted data, the private key *sk*—generated based on the user's attributes and system parameters—is employed. By leveraging the user's private key *sk* and the access tree from ciphertext *C*, the system identifies the access path corresponding to the user's attributes. If the user's attributes fulfill the conditions specified in the access tree, successful decryption of the data occurs. The decryption process involves executing pairing operations between ciphertext fragments, ultimately retrieving the original medical data. Throughout this process, the authorizing entity utilizes the master key *msk* and the user's attribute set *attr* to compute a shared key *K*:

$$K = e\left(g^{msk \cdot attr}, C_1\right) \tag{4}$$

The plaintext is then calculated according to Equation (5).

$$m = \frac{C_2}{K} \tag{5}$$

In this context, $C_1$ is a component of the ciphertext generated during the encryption process, associated with the random key *r*. The pairing operation *e* on the elliptic curve is used to combine generated group elements and keys. The shared key *K* is computed and utilized to decrypt the ciphertext. $C_2$ is the other component of the ciphertext, containing the encrypted message and other encryption-related information tied to the master key. After decryption, the plaintext *m* represents the original message.

Several academic considerations support the use of ABE in smart healthcare networks.

1. Fine-Grained Access Control: ABE enables precise access control by defining policies based on user attributes. This allows for specific access scenarios, such as limiting access to certain medical records only to doctors with relevant qualifications, or granting access solely to patients and authorized physicians for specific diagnostic information.
2. Dynamic Access Policies: Medical data often requires real-time adjustments to access policies due to changing circumstances. ABE allows for flexible modification of access policies during data transmission and storage without the need for redistributing keys. For example, if a patient's condition changes unexpectedly, data owners can quickly update policies to ensure relevant healthcare providers have timely access to crucial information.
3. Simplified Key Management: Traditional encryption methods involve complex key management systems, whereas ABE simplifies this by generating keys directly from user attributes. This is particularly beneficial in medical environments, where users may not have extensive encryption expertise. ABE's approach provides a more intuitive method of managing data security operations.
4. Reduced User Burden: Many users in healthcare, including patients and physicians, are not familiar with encryption technologies. ABE minimizes the complexity for users, as they only need to consider their attributes and data access requirements, without navigating intricate key management systems. This streamlines access to medical data, making it more efficient for all parties involved.

To illustrate the application of ABE in smart healthcare networks, consider a case study involving a comprehensive hospital. This hospital manages patients' electronic health records (EHRs) and offers online consultations through a telemedicine platform. The medical team consists of doctors, nurses, and administrative staff, each requiring different levels of access to medical data. Additionally, the hospital collaborates with external research institutions, sharing anonymized patient data for research purposes.

In the context of EHR access control, a doctor records a patient's medical information during a visit. The data is stored in the hospital's EHR system, and ABE technology is used to encrypt it with an access policy, such as "only the attending physician and nurses in the department can access." This ensures that only individuals with these attributes can decrypt and view the medical records, protecting the patient's privacy. In the telemedicine consultation scenario, a patient uses the hospital's platform for an online consultation. To maintain confidentiality, the platform encrypts the consultation records with an access policy specifying "only the consulting doctor and the patient can access." The records remain encrypted during transmission and storage, ensuring only authorized individuals can access them, thus safeguarding data security. In the data sharing and research scenario, the hospital collaborates with external research institutions by providing anonymized patient data for cancer research. ABE technology encrypts the shared data, with an access policy allowing "only researchers involved in the project" to access the information. This ensures that only authorized researchers can view the data, protecting patient privacy while enabling valuable medical research. This case study highlights how ABE technology enhances data security and privacy protection in various healthcare scenarios, ensuring the safe management and sharing of sensitive medical information.

### 3.3. *Design of anti-corruption mechanism for medical systems*

The ABE technology not only offers fine-grained access control but also ensures data confidentiality and integrity during transmission and storage. With data security established, an anti-corruption mechanism is introduced to further safeguard the smart healthcare network. This mechanism addresses potential risks of corruption and misuse of medical data by focusing on four key dimensions: supervision, auditing, penalties, and incentives. The objective is to create a systematic and comprehensive framework that prevents unauthorized access and improper use of sensitive medical information. The detailed architecture of this anti-corruption mechanism is illustrated in Fig. 4.

As depicted in Fig. 4, the components of supervision, audit, penalties, and incentives work together to create an integrated system that ensures the security of medical data while promoting adherence to professional standards among healthcare providers. A dedicated supervisory body is tasked with real-time monitoring of medical data access activities, relying on data logs, access records, and other relevant information to regularly review compliance with established access policies. The audit component utilizes anonymous auditing techniques, such as zero-knowledge proofs, to conduct random checks on data access requests, validating the legitimacy of access without revealing the identities of healthcare professionals. This preserves privacy while confirming the legality of data access. The penalties aspect of the system provides a structured framework for addressing misconduct. Healthcare professionals who misuse their authority or exceed their access privileges face consequences according to institutional regulations, including fines, suspension of access rights, or legal actions. In contrast, the incentive component rewards those who consistently comply with data access regulations. Healthcare professionals may receive recognition through career advancements or enhanced reputations, fostering a culture of compliance within healthcare institutions.

## 4. Experiment design

A series of experiments are conducted to evaluate the effectiveness of the proposed smart healthcare network optimization solution. The initial step involved creating a simulation environment to replicate the data transmission and processing procedures typical of a real healthcare network. The specific parameter configurations are detailed in Table 1.

The hardware platform for the experimental environment consists of a computer with an Intel Core i7 processor and 16 GB of RAM, running on Ubuntu 20.04. The encryption algorithm used is ABE, and the dataset contains 1000 entries to simulate the typical volume of medical data. To ensure both security and computational efficiency during encryption, secp256k1 elliptic curve parameters are employed, reflecting real-world medical network scenarios.

Key performance metrics—such as access latency, data transmission speed, and system stability—are evaluated throughout the

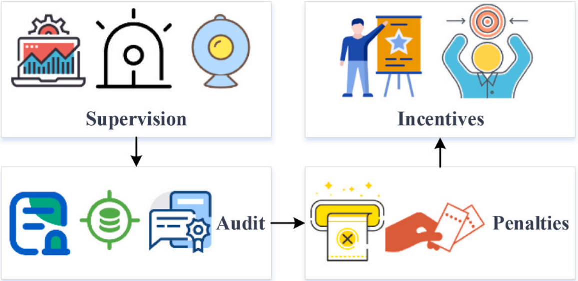

**Fig. 4.** Design of an anti-corruption mechanism in the medical system.

**Table 1**
Parameter settings.

| Parameter | Value |
|---|---|
| Encryption algorithm | ABE |
| Data volume | 1000 items |
| Access policy complexity | medium |
| Encryption key length | 256 bit |
| Elliptic curve parameters | secp256k1 |

experiments. These metrics are measured before and after the integration of ABE technology and compared against the performance of traditional encryption algorithms. Additionally, simulated corrupted data is introduced to test the accuracy and responsiveness of the anti-corruption mechanism, allowing the system's ability to detect and correct data tampering to be assessed.

The experiments also involve testing access control policies with varying levels of complexity to evaluate the ABE algorithm's performance in handling more sophisticated policies. The system's scalability is tested by gradually increasing the number of data entries, providing insights into its behavior under large-scale data loads. Multiple runs ensure that the results are stable and reproducible. The experiments comprehensively assess the applicability of the proposed method to intelligent medical networks, confirming its effectiveness in improving data transmission efficiency, reducing access latency, and enhancing system stability.

## 5. Results and discussion

### 5.1. Experimental results

The access latency, data transfer speed, and system stability of the ABE algorithm when applied to actual medical data are depicted through Fig. 5 to Fig. 7

Fig. 5 illustrates the consistently low access latency achieved by the ABE algorithm across multiple experiment runs, with latency ranging between 30 ms and 41 ms and an average of 35 ms. This performance highlights the ABE algorithm's ability to quickly respond to user requests within the smart healthcare network, which is critical for both patients and medical professionals requiring timely access to vital information. In emergency medical situations, the low-latency response enhances the efficiency of medical decision-making. Additionally, the stable low-latency results demonstrate the algorithm's scalability in managing a large volume of concurrent requests, ensuring reliable data delivery even under increased system load.

Fig. 6 showcases the impressive data transfer speed achieved by the ABE algorithm. The experimental results consistently demonstrate data transfer speeds ranging from 3.1 MB/s to 3.7 MB/s, with an average of 3.56 MB/s. This highlights the algorithm's efficiency in transmitting medical data, supporting large-scale data exchanges within intelligent healthcare networks. High data transmission speed is essential for applications such as real-time monitoring and remote diagnostics, which depend on fast and reliable data delivery. Additionally, the improved transmission speed reflects the ABE algorithm's effective utilization of network bandwidth, reducing transmission latency and further enhancing the system's real-time performance and reliability.

Fig. 7 illustrates the exceptional system stability of the ABE algorithm across various experimental runs. The results consistently show system stability ranging from 98.2 % to 98.9 %, with an average of 98.74 %. This high level of stability indicates that the ABE algorithm reliably delivers robust performance within intelligent healthcare networks, ensuring secure transmission and reliable storage of medical data. Such stability is crucial for preventing data loss, maintaining data consistency, and preserving the overall functionality of the healthcare network. Additionally, this level of stability suggests that the ABE algorithm exhibits strong resilience and fault tolerance in the face of potential network disruptions or malicious attacks, providing a secure and reliable encryption solution

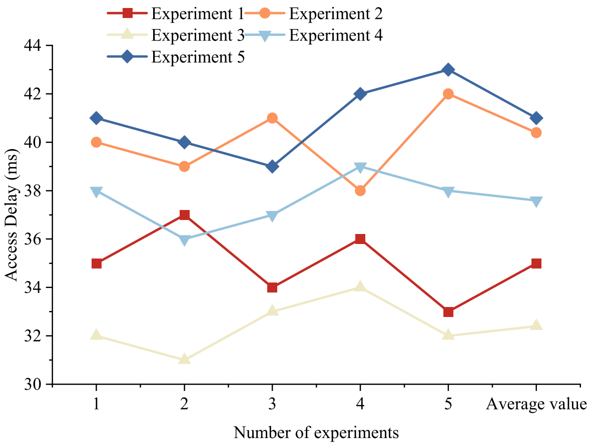

**Fig. 5.** Access latency (in milliseconds).

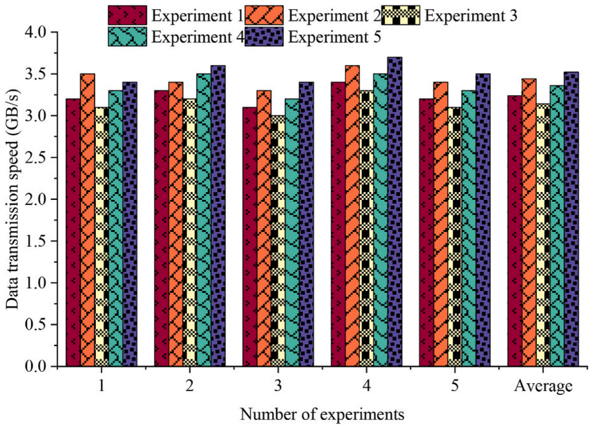

**Fig. 6.** Data transfer speed (in megabytes per second).

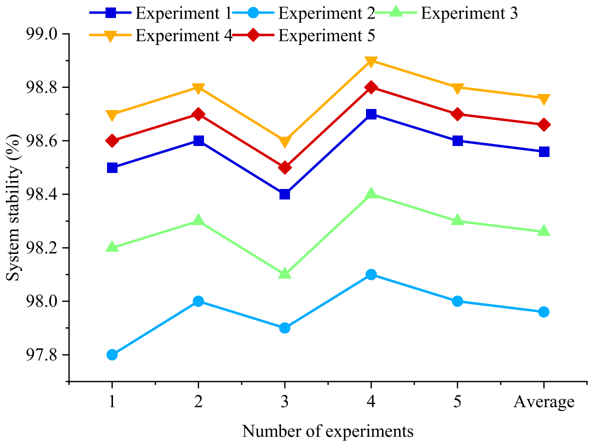

**Fig. 7.** System stability (in percentage).

for intelligent healthcare networks.

### 5.2. *Comparison with other similar algorithms*

To assess the performance of the ABE algorithm, a comparative analysis is conducted against traditional encryption algorithms, including Identity-Based Encryption (IBE), Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-

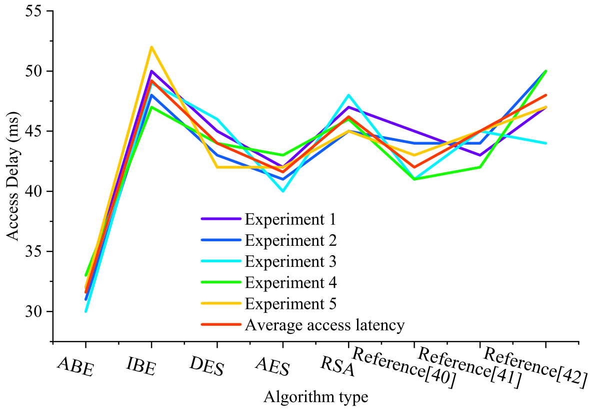

**Fig. 8.** Comparison of access delays of different algorithms (measured in milliseconds).

Adleman (RSA). Additionally, comparisons are made with various hybrid encryption algorithms as referenced in Refs. [39,40], and [41]. The results are illustrated in Fig. 8 to Fig. 10

Fig. 8 illustrates significant performance disparities among various encryption algorithms concerning access latency, as indicated by the experimental results. The ABE algorithm consistently achieves an average access latency of 31.6 ms across all experimental runs, notably outperforming other algorithms such as IBE, DES, AES, and RSA. This finding highlights the ABE algorithm's ability to provide rapid data access within smart healthcare networks, ensuring timely access to essential information for patients and healthcare professionals.

Furthermore, the ABE algorithm's performance is compared with hybrid encryption algorithms referenced in Refs. [39–41]. Although hybrid encryption algorithms can enhance encryption strength in certain contexts, they exhibit significantly higher access latency compared to the ABE algorithm. This increased latency may affect the real-time accessibility of medical data in practical applications. While hybrid encryption algorithms demonstrate robust security performance, their higher access latency limits their applicability in medical scenarios that require rapid responses. In contrast, the ABE algorithm not only ensures comparable security but also substantially reduces access latency, thereby improving overall system performance. It is evident that the ABE algorithm maintains high security standards while effectively optimizing system performance, particularly in smart healthcare networks that demand swift data access. These comparisons reveal a distinct advantage for the ABE algorithm in terms of access latency, significantly enhancing the response time of smart healthcare networks. This capability ensures that patients and healthcare professionals can quickly access critical medical information, ultimately improving the efficiency and quality of healthcare services.

Fig. 9 illustrates the outstanding performance of the ABE algorithm regarding data transfer speed. Across various experimental runs, the ABE algorithm consistently achieved an average data transfer speed of 3.56 megabytes per second, surpassing the averages of other algorithms, including IBE, DES, AES, and RSA. This performance highlights the ABE algorithm's capability to efficiently facilitate the transfer of healthcare data, thereby enhancing overall data transfer efficiency. In comparison with several hybrid encryption algorithms referenced in Refs. [39–41], it is evident that while these hybrid algorithms provide stronger encryption in certain scenarios, their data transmission speeds are significantly lower than those of the ABE algorithm. This reduced transmission speed can create bottlenecks in medical applications requiring high-frequency data transmission, potentially affecting the overall system efficiency. In summary, the ABE algorithm offers a distinct advantage in data transmission speed, effectively improving data transfer efficiency within smart healthcare networks.

Fig. 10 demonstrates the superior performance of the ABE algorithm regarding system stability. Across various experimental runs, the ABE algorithm achieved an average system stability of 98.74 %, slightly surpassing the averages of other algorithms, including IBE, DES, AES, and RSA. This indicates that the ABE algorithm provides more robust performance within smart healthcare networks, thereby enhancing the secure transmission and reliable storage of healthcare data. In summary, the ABE algorithm outperforms other algorithms in terms of access latency, data transfer speed, and system stability, making it the optimal choice for smart healthcare networks. It offers an exceptional solution for secure data transmission and efficient data management in healthcare contexts.

When compared with several hybrid encryption algorithms referenced in Refs. [39–41], hybrid encryption methods demonstrate strong security in specific application scenarios; however, their system stability tends to be slightly lower than that of the ABE algorithm. This difference may affect the long-term reliability of the system, especially in situations where high availability of medical data is crucial. Consequently, the ABE algorithm provides a significant advantage in terms of system stability, ensuring greater reliability and security within smart healthcare networks.

### 5.3. *Security analysis*

To assess the security performance of ABE technology in smart healthcare networks, detailed experiments and analyses focus on data confidentiality, integrity, access control, and resilience against attacks. The findings are summarized in Table 2, which presents a

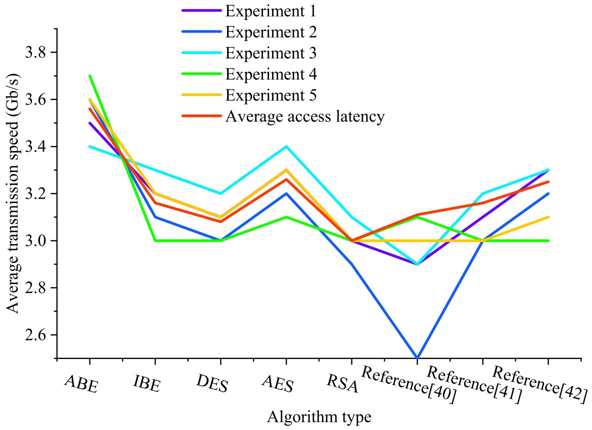

**Fig. 9.** Comparison of data transfer speed among different algorithms (measured in megabytes per second).

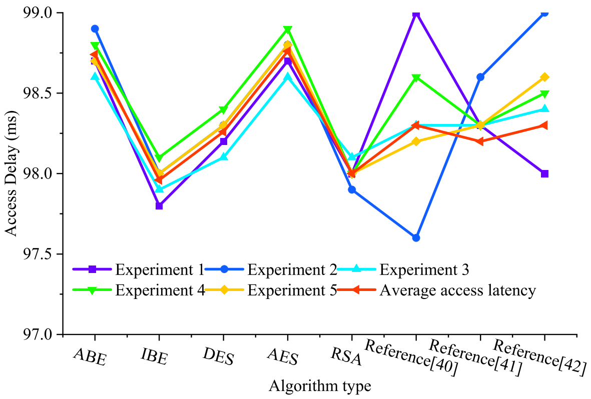

**Fig. 10.** Comparative evaluation of system stability across different algorithms (measured in percentage).

comprehensive analysis of the experimental results:

ABE technology effectively ensures the encryption and integrity of medical data. The decryption success rate stands at 98 %, strictly adhering to defined access policies, with no instances of data tampering detected. The encryption and decryption processes demonstrate robust performance in practical applications, despite slight increases in encrypted data size and network transmission latency, both of which remain within acceptable thresholds. Subsequently, the performance of ABE technology in fine-grained access control is evaluated to ensure that only users meeting specific attribute conditions can access sensitive data. The experimental findings are summarized in Table 3, which provides a detailed analysis of the results:

ABE technology exhibits precise control over data access permissions, achieving a 95 % success rate in authorizing access requests according to specified permissions, while effectively preventing all unauthorized accesses. The execution time for enforcing access control policies is minimal, making it suitable for real-world medical scenarios. Although policy complexity leads to linear growth in execution time, the system adeptly manages complex policies. Additionally, the resilience of ABE technology against various types of attacks is analyzed to evaluate its effectiveness in safeguarding data security. The experimental findings are detailed in Table 4, which presents a comprehensive analysis of the results:

The analysis in Table 4 highlights the robust security provided by ABE technology, which utilizes advanced mathematical constructs such as bilinear mappings and elliptic curve discrete logarithm problems. This technology effectively thwarts 99 % of attack simulations, demonstrating resilience against various forms of attacks. With only one successful breach recorded, resulting in a decryption time of 72 h, the system maintains a high level of security. While the current key lengths are effective against conventional attacks, enhancing them would improve resistance against potential quantum threats. The comprehensive security analysis and experimental findings presented in Table 4 affirm the superior performance of Attribute-Based Encryption technology in smart medical networks. These insights underscore ABE technology's significant contributions to enhancing data confidentiality, integrity, and access control, while also emphasizing its robust defense against adversarial attacks.

### *5.4. Discussion*

Research findings indicate that the ABE algorithm consistently achieves lower access latency compared to other encryption algorithms across diverse experimental scenarios. This capability ensures swift responses to user requests within smart healthcare networks, facilitating timely access to critical information for both patients and healthcare professionals. These results align with the made by Charanya [42]recommendations, who emphasized the importance of low latency for ensuring document integrity using cloud time-shading with link records and temporary signatures. Similarly, Kara [43] introduced an efficient fully homomorphic encryption scheme employing dual-key encryption and magic number fragments, accompanied by a comprehensive cryptographic analysis to evaluate its efficacy. These studies further highlight the significance of low latency, a point reinforced by the current findings.

**Table 2**
Data confidentiality and integrity.

| Metric | Data Result |
|---|---|
| Encrypted data volume | 1000 EHRs |
| Decryption success rate | 98 % |
| Data tampering rate | 0 % |
| Encryption time (per record, average) | 0.45 s |
| Decryption time (per record, average) | 0.55 s |
| Data size (per record) | 500 KB |
| Percentage change in data size | 5 % increase |
| Network transmission latency (before encryption) | 50 ms |
| Network transmission latency (after encryption) | 52 ms |

**Table 3**
Access control results.

| Metric | Data Result |
|---|---|
| Number of access requests | 500 |
| Access authorization rate | 95 % |
| Unauthorized access prevention rate | 100 % |
| Average policy enforcement time | 0.4 s |
| Impact of policy complexity on execution time | Linear growth |
| Maximum policy complexity (number of conditions) | 10 |
| Success rate of policy execution (complex policies) | 90 % |

**Table 4**
Resilience against attacks.

| Metric | Data Result |
|---|---|
| Attack types | Ciphertext attack, Public key attack |
| Security verification rate | 99 % |
| Number of attack simulations | 100 |
| Successful breaks | 1 time |
| Time to break (successful case) | 72 h |
| Key length (bits) | 2048 bits |
| System's resistance to quantum attacks | Moderate, requires longer key lengths for stronger resistance |

Additionally, the ABE algorithm significantly enhances the efficiency of medical data transmission, improving both the speed and accuracy of data transfer. This efficiency reduces the time required for data transmission while ensuring the integrity of data throughout the transfer process, especially when handling large volumes or high bandwidth demands. Furthermore, the ABE algorithm demonstrates exceptional system stability within intelligent healthcare networks, ensuring the secure transmission and reliable storage of medical data. Stability is crucial for preventing data loss, maintaining consistency, and withstanding potential network disruptions and attacks. For instance, Jiang [44] proposed an access control model that integrates risk quantification and usage control to enhance the privacy protection of healthcare data. The stability of the ABE algorithm further validates its applicability in intelligent healthcare networks, establishing it as a key tool for improving data management efficiency and security.

The ABE algorithm demonstrates exceptional performance in smart healthcare networks across key metrics such as access latency, data transfer speed, and system stability, providing a reliable solution for secure data transmission and efficient data management. It promptly responds to user requests, ensuring timely access to medical information, while efficiently transferring substantial volumes of healthcare data. This combination enhances data transfer efficiency and maintains system stability, ultimately ensuring the security and reliability of healthcare data. In summary, the ABE algorithm shows significant promise for applications in smart healthcare networks, offering a practical and dependable solution for secure data transmission and efficient data management. In the future development of smart healthcare, the ABE algorithm may play a pivotal role in advancing and enhancing system capabilities.

In practical applications, ABE technology holds significant potential to enhance data security and trustworthiness in smart healthcare networks across various scenarios.

1. Remote Healthcare and Mobile Health Applications: In these applications, sensitive patient data transmitted over the internet can be protected using ABE. Access to this data is restricted to healthcare personnel based on specific attribute criteria, safeguarding patient privacy during transmission.
2. EHR Management: ABE effectively manages access to EHRs through fine-grained access control. Different healthcare professionals, such as doctors, nurses, and administrative staff, can access relevant medical records based on their roles and permissions, preventing unauthorized access and ensuring data confidentiality.
3. Medical Data Sharing Platforms: In platforms designed for sharing medical data among researchers and institutions, ABE ensures secure data sharing. By establishing access policies, only authorized researchers can access specific datasets, maintaining data confidentiality and integrity throughout the sharing process.
4. Security of Medical IoT Devices: ABE technology is crucial for securing IoT devices connected to smart healthcare networks. Data generated by these devices is encrypted during transmission, ensuring that only designated recipients with appropriate credentials can decrypt and access the data, thereby safeguarding against unauthorized access and potential data breaches.

The adoption of ABE technology not only mitigates data security vulnerabilities but also prevents data corruption and misuse, enhancing the integrity and security of medical data transmission and management. Its wide-ranging impacts include.

1. Enhancing Data Trustworthiness: ABE ensures data integrity and immutability during transmission and storage, thereby improving the overall trustworthiness of medical data. This contributes to more accurate medical decision-making and enhances patient outcomes.

2. Building Patient Trust: Effective data privacy protections facilitated by ABE bolster patient trust in smart healthcare systems. This trust encourages greater patient participation and utilization of these systems, promoting efficiency and effectiveness in healthcare service delivery.
3. Driving Policy Formulation: The application of ABE technology informs the development of healthcare data security policies and standards. This supports the formulation of stricter data protection regulations, advances healthcare information security practices, and ensures compliance with regulatory requirements.
4. Promoting Technological Innovation: ABE technology fosters innovation in data security and privacy protection within smart healthcare networks. Its implementation inspires further advancements, driving continuous innovation in safeguarding sensitive medical data and improving overall network efficiency.

In conclusion, ABE technology represents a robust solution for securing medical data in smart healthcare networks, offering comprehensive protection against unauthorized access while ensuring the confidentiality, integrity, and trustworthiness of healthcare information.

## 6. Conclusion

This study introduces the ABE algorithm to smart healthcare networks and highlights its advantages through comparative experiments. The ABE algorithm outperforms other encryption methods in access latency, data transfer speed, and system stability. It particularly excels in data transfer speed and surpasses competitors in access latency and system stability, providing a robust solution for ensuring data security in smart healthcare environments. ABE technology offers a distinct advantage by enabling fine-grained access control based on user attributes, which is essential in smart healthcare networks with diverse roles, including doctors, nurses, and patients. The algorithm dynamically manages and regulates data access permissions according to predefined user attributes, enhancing both system flexibility and security. Through encryption and decryption processes aligned with specified access policies, ABE ensures that only authorized users who meet specific criteria can access sensitive data. This proactive approach effectively mitigates unauthorized access attempts, safeguarding the privacy and integrity of medical information.

Despite the significant experimental findings in this study, several limitations warrant consideration. First, the experimental data are confined to limited scenarios and data scales, which may restrict their applicability to the complexities of real healthcare networks. Second, fluctuations in the network environment that could influence experimental outcomes under varying conditions are not accounted for. Lastly, the focus is solely on the ABE algorithm, without exploring other advanced encryption algorithms, indicating potential avenues for future research to conduct more comprehensive comparative analyses. Building upon these findings, future research will expand in several directions. Efforts will aim to further optimize the ABE algorithm's performance to enhance its efficiency and security in transmitting large-scale healthcare data. Research will also explore solutions to meet the real-time demands of smart healthcare networks, developing low-latency solutions while ensuring robust data security. Additionally, integrating artificial intelligence technologies to construct intelligent healthcare data management systems will be considered, enhancing the efficiency of healthcare data analysis and utilization.

In summary, despite the acknowledged limitations, the results of this study provide a robust foundational support for enhancing data security in smart healthcare networks. Future research will continue to focus on optimizing encryption algorithms, addressing real-time operational needs, and exploring intelligent applications to provide more reliable and innovative solutions for advancing the field of smart healthcare.

## CRediT authorship contribution statement

**Yanzhao Zeng:** Writing – original draft, Software, Data curation. **Xin Guan:** Writing – original draft, Formal analysis. **Jingjing Sun:** Writing – review & editing, Validation, Formal analysis. **Yanrui Chen:** Writing – original draft, Visualization, Data curation. **Zeyu Wang:** Writing – review & editing, Supervision, Investigation, Conceptualization. **Peng Nie:** Writing – review & editing, Resources, Project administration, Methodology.

## Informed consent statement

Informed consent was not required as the study did not involve human participants.

## Data availability statement

The data that support the findings of this study are available on request from the corresponding author, upon reasonable request.

## Ethics approval

Ethical approval was not required as the study did not involve human participants.

## Funding statement

This work was supported by a grant from the Key Program of Guangdong Basic and Applied Basic Research Foundation (Grant No. 2022B1515120060); this work was also supported by Research on Issues in the Development of the Digital Economy Industry (Grant No. PT252022035).

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

[1] M.H.P. Rizi, S.A.H. Seno, A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city, Internet of Things (2022) 20, https://doi.org/10.1016/j.iot.2022.100584.

[2] B. Murdoch, Privacy and artificial intelligence: challenges for protecting health information in a new era, BMC Med. Ethics (1) (2021) 22, https://doi.org/10.1186/s12910-021-00687-3.

[3] B. Jiang, J.Q. Li, G.H. Yue, et al., Differential privacy for industrial internet of things: opportunities, applications, and challenges. Ieee Internet of Things Journal 8 (13) (2021) 10430–10451, https://doi.org/10.1109/jiot.2021.3057419.

[4] E.W. Clayton, P.J. Embí, B.A. Malin, Dobbs and the future of health data privacy for patients and healthcare organizations. Journal of the American Medical Informatics Association 30 (1) (2022) 155–160, https://doi.org/10.1093/jamia/ocac155.

[5] R. Jiang, S.S. Han, Y.M. Yu, et al., An access control model for medical big data based on clustering and risk, Information Sciences 621 (2023) 691–707, https://doi.org/10.1016/j.ins.2022.11.102.

[6] F. Amiri, A. Neshati, S. Hannani, et al., Effect of mobile-based education of patient's privacy protection principles on the knowledge, attitude and performance of operating room staff, Annals of the Romanian Society for Cell Biology 25 (6) (2021) 6876–6882 [cited, http://www.annalsofrscb.ro/index.php/journal/article/view/6784.

[7] D. McGraw, K.D. Mandl, Privacy protections to encourage use of health-relevant digital data in a learning health system, Npj Digital Medicine (1) (2021) 4, https://doi.org/10.1038/s41746-020-00362-8.

[8] C. Thapa, S. Camtepe, Precision health data: Requirements, challenges and existing techniques for data security and privacy, Computers in Biology and Medicine (2021) 129, https://doi.org/10.1016/j.compbiomed.2020.104130.

[9] Z. Wang, S. Zhang, Y. Zhao, et al., Risk prediction and credibility detection of network public opinion using blockchain technology, Technological Forecasting and Social Change 187 (2023) 122177, https://doi.org/10.1016/j.techfore.2022.122177.

[10] M. Jofre-Bonet, J. Kamara, A. Mesnard, Corruption and informal sector households' participation in health insurance in Sierra Leone, PLoS One (4) (2023) 18, https://doi.org/10.1371/journal.pone.0281724.

[11] U. Ahmed, H.S.M.J.A.o.S.S. Abbas, and Perspective, Institutional corruption in the health sector and role of administration: a case study of Pakistan, Annals of Social Sciences and Perspective 3 (1) (2022) 219–234, https://doi.org/10.52700/assap.

[12] T. Vian, B. Agnew, K. McInnes, Whistleblowing as an anti-corruption strategy in health and pharmaceutical organizations in low- and middle-income countries: a scoping review, Glob. Health Action (1) (2022) 15, https://doi.org/10.1080/16549716.2022.2140494.

[13] Y. Deng, W. Jiang, Z. Wang, Economic resilience assessment and policy interaction of coal resource oriented cities for the low carbon economy based on ai, Resour. Pol. 82 (2023) 103522, https://doi.org/10.1016/j.resourpol.2023.103522.

[14] M. Indushree, M. Raj, A novel blockchain-based authentication scheme for telecare medical information system, The Journal of Supercomputing 80 (1) (2024) 1080–1108, https://doi.org/10.1007/s11227-023-05526-3.

[15] C. Rupa, Greeshmanth, M.A. Shah, Novel secure data protection scheme using martino homomorphic encryption, J. Cloud Comput. 12 (1) (2023) 47, https://doi.org/10.1186/s13677-023-00425-7.

[16] Z. Man, J. Li, X. Di, et al., Research on cloud data encryption algorithm based on bidirectional activation neural network, Inf. Sci. 622 (2023) 629–651, https://doi.org/10.1016/j.ins.2022.11.089.

[17] M.J. Li, Z.H. Tian, X.J. Du, et al., Power normalized cepstral robust features of deep neural networks in a cloud computing data privacy protection scheme, Neurocomputing 518 (2023) 165–173, https://doi.org/10.1016/j.neucom.2022.11.001.

[18] J. Zhou, L. Zhou, D. Wang, et al., Personalized and privacy-preserving federated heterogeneous medical image analysis with pppml-hmi. Computers in Biology and Medicine 169 (2024) 107861, https://doi.org/10.1016/j.compbiomed.2023.107861.

[19] E. Argyridou, S. Nifakos, C. Laoudias, et al., Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study, Journal of Medical Internet Research (2023) 25, https://doi.org/10.2196/41294.

[20] A. Majeed, Attribute-centric and synthetic data based privacy preserving methods: a systematic review, Journal of Cybersecurity and Privacy 3 (3) (2023) 638–661, https://doi.org/10.3390/jcp3030030.

[21] X. Zhang, F. Yang, Y. Guo, et al., Adaptive differential privacy mechanism based on entropy theory for preserving deep neural networks, Mathematics 11 (2) (2023) 330, https://doi.org/10.3390/math11020330.

[22] E.V.D. Subramaniam, K. Srinivasan, S.M. Qaisar, et al., Interoperable iomt approach for remote diagnosis with privacy-preservation perspective in edge systems, Sensors 23 (17) (2023) 7474, https://doi.org/10.3390/s23177474.

[23] H. Wang, J. Liang, Y. Ding, et al., Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health, Computer Standards & Interfaces 84 (2023) 103696, https://doi.org/10.1016/j.csi.2022.103696.

[24] N. Alharbe, A. Aljohani, M.A. Rakrouki, A novel data partitioning method for active privacy protection applied to medical records, Electronics 12 (6) (2023) 1489, https://doi.org/10.3390/electronics12061489.

[25] Y. Zhang, M.J.J.o.C. Zhang, E.I. Management, Review on privacy protection of electronic medical data in cross-domain sharing, Annals of Social Sciences and Perspective 10 (3) (2023) 51–54, 10.54097/ jceim. v10i3.8681.

[26] J. Wang, S. Makowski, A. Cieślik, et al., Fake news in virtual community, virtual society, and metaverse: a survey, IEEE Transactions on Computational Social Systems 2023 (2022) 1–15, https://doi.org/10.1109/TCSS.

[27] J. Su, Y. Cao, Y. Chen, et al., Privacy protection of medical data in social network, Journal of Computing and Electronic Information Management 21 (2021) 1–14, https://doi.org/10.52700/assap.

[28] M. Soni, D.K. Singh, Privacy-preserving secure and low-cost medical data communication scheme for smart healthcare, Comput. Commun. 194 (2022) 292–300, https://doi.org/10.1016/j.comcom.2022.07.046.

[29] M. Zhang, Y. Chen, J. Lin, *A privacy-preserving optimization of neighborhood-based recommendation for medical-aided diagnosis and treatment.* IEEE Internet of Things Journal 8 (13) (2021) 10830–10842, https://doi.org/10.1109/jiot.2021.3051060.

[30] R. Praveen, P. Pabitha, Improved gentry-halevi's fully homomorphic encryption-based lightweight privacy preserving scheme for securing medical internet of things, Transactions on Emerging Telecommunications Technologies (4) (2023) 34, https://doi.org/10.1002/ett.4732.

[31] W. Liu, Y.-H. Zhang, Y.-F. Li, et al., A fine-grained medical data sharing scheme based on federated learning. Concurrency and Computation, Practice and Experience (20) (2023) 35, https://doi.org/10.1002/cpe.6847.

[32] A. Almalawi, A.I. Khan, F. Alsolami, et al., Managing security of healthcare data for a modern healthcare system, Sensors 23 (7) (2023) 3612, https://doi.org/10.3390/s23073612.

[33] P. Kumar, R. Kumar, G.P. Gupta, et al., *A blockchain-orchestrated deep learning approach for secure data transmission in iot-enabled healthcare system.* Journal of Parallel and Distributed Computing 172 (2023) 69–83, https://doi.org/10.1016/j.jpdc.2022.10.002.

[34] F.J. Jaime, A. Muñoz, F. Rodríguez-Gómez, et al., Strengthening privacy and data security in biomedical microelectromechanical systems by iot communication security and protection in smart healthcare, Sensors 23 (21) (2023) 8944, https://doi.org/10.3390/s23218944.

[35] S. Namasudra, P. Roy, Ppbac: Popularity based access control model for cloud computing, Journal of Organizational and End User Computing 30 (4) (2018) 14–31, https://doi.org/10.4018/joeuc.2018100102.

[36] O. Elharrouss, K. Hassine, A.A. Zayyan, et al., 3d point cloud for objects and scenes classification, recognition, segmentation, and reconstruction: a review, Cloud Computing and Data Science 4 (2) (2023) 134–160, https://doi.org/10.37256/ccds.4220232722.

[37] A. Gupta, S. Namasudra, A novel technique for accelerating live migration in cloud computing, Automated Software Engineering 29 (1) (2022) 34, https://doi.org/10.1007/s10515-022-00332-2.

[38] Z. Wang, X. Guan, Y. Zeng, et al., Utilizing data platform management to implement "5w" analysis framework for preventing and controlling corruption in grassroots government, Heliyon (7) (2024) e28601, https://doi.org/10.1016/j.heliyon.2024.e28601.

[39] P. Chinnasamy, P. Deepalakshmi, Hcac-ehr: Hybrid cryptographic access control for secure ehr retrieval in healthcare cloud, Journal of Ambient Intelligence and Humanized Computing 13 (2) (2022) 1001–1019, https://doi.org/10.1007/s12652-021-02942-2.

[40] P. Chinnasamy, P. Deepalakshmi, Design of secure storage for health-care cloud using hybrid cryptography, in: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 1717–1720, 10.1109/ICICCT.2018.8473107.

[41] Deepalakshmi. Karthik Chinnasamy, Hybrid cryptographic technique using otp:Rsa, in: 2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing(INCOS), 2017, pp. 1–4, 10.1109/ITCOSP.2017.8303131.

[42] R. Charanya, R. Saravanaguru, M.J.I.J.o.I.E. Aramudhan, Information security protection for ehealth records using temporal hash signature, International Journal of Intelligent Enterprise 10 (1) (2023) 14–30, https://doi.org/10.1504/ijie.2023.127233.

[43] M. Kara, A. Laouid, M.A. Yagoub, et al., A fully homomorphic encryption based on magic number fragmentation and el-gamal encryption, Smart healthcare use case. Expert Systems (5) (2022) 39, https://doi.org/10.1111/exsy.12767.

[44] R. Jiang, X. Chen, Y. Yu, et al., Risk and ucon-based access control model for healthcare big data, Journal of Big Data 10 (1) (2023) 104, https://doi.org/10.1186/s40537-023-00783-8.