applied sciences

MDPI

Article

HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications

Ziang Chen [1], Jiantao Gu [1,2] and Hongcan Yan [1,2,*]

[1] College of Science, North China University of Science and Technology, Tangshan 063210, China; chenziang19990512@163.com (Z.C.); gujiantaoncst@163.com (J.G.)
[2] Hebei Key Laboratory of Data Science and Application, Tangshan 063210, China
* Correspondence: yanhongcan@ncst.edu.cn

Abstract: The integration of cryptographic algorithms like Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) is pivotal in bolstering the core attributes of blockchain technology, especially in achieving decentralization, tamper resistance, and anonymization within the realm of medical applications. Despite their widespread utilization, the conventional AES and ECC face significant hurdles in security and efficiency when dealing with expansive medical data, posing a challenge to the effective preservation of patient privacy. In light of these challenges, this study introduces HAE (hybrid AES and ECC), an innovative hybrid cryptographic algorithm that ingeniously amalgamates the robustness of AES with the agility of ECC. HAE is designed to symmetrically encrypt original data with AES while employing ECC for the asymmetric encryption of the initial AES key. This strategy not only alleviates the complexities associated with AES key management but also enhances the algorithm's security without compromising its efficiency. We provide an in-depth exposition of HAE's deployment within a framework tailored for medical scenarios, offering empirical insights into its enhanced performance metrics. Our experimental outcomes underscore HAE's exemplary security, time efficiency, and optimized resource consumption, affirming its potential as a breakthrough advancement for augmenting blockchain applications in the medical sector, heralding a new era of enhanced data security and privacy within this critical domain.

Keywords: AES; ECC; blockchain; hybrid cryptographic algorithm

check for updates

Citation: Chen, Z.; Gu, J.; Yan, H. HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications. *Appl. Sci.* **2023**, *13*, 12163. https://doi.org/10.3390/app132212163

Academic Editor: Gianluca Lax

Received: 29 September 2023
Revised: 2 November 2023
Accepted: 8 November 2023
Published: 9 November 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The widespread collection and storage of digitized medical information have raised significant concerns regarding patient privacy and data security, presenting a major challenge for the medical industry. With its decentralized nature, tamper resistance, and traceability, blockchain technology holds considerable promise for medical applications. However, data security and privacy protection warrant careful consideration. Cryptographic algorithms, which form the backbone of a blockchain, offer a viable solution to address the challenges posed by large data volumes, diverse data structures, and the complexities of data storage and sharing in blockchain scenarios.

Several researchers have proposed cryptographic solutions to these challenges. For instance, Banerjee et al. [1] proposed a blockchain-based, fine-grained user access control scheme to address data security and privacy protection issues in the low power wide area network (LPWAN). In this scheme, data collected by IoT smart devices are encrypted using the cryptographic policy attribute-based encryption algorithm (CP-ABE) and transmitted to nearby gateway nodes. While this approach enhances security, it also increases the time cost of network transmission. Li et al. [2] introduced a blockchain-anchored fine-grained access control scheme, FADB, tailored for vehicular ad hoc network (VANET) data. This scheme synergizes the blockchain with ciphertext-policy attribute-based encryption (CP-ABE) to bolster the security of VANET. Within FADB, an enhanced CP-ABE algorithm is deployed,

offering superior data security and a reduced performance overhead. Notably, the scheme leverages the blockchain for user identity management and data storage, eliminating the need for third-party service providers. It also delineates distinct VANET data access privileges based on user attributes. Jadav et al. [3] proposed a secure data exchange framework called GRADE for machine-type communication (MTC) in a separate study. Based on blockchain and garlic routing (GR), this framework employs AES encryption to secure the GR network. Although GRADE offers good security and scalability, its ability to withstand adversarial attacks and malware threats in real-world scenarios needs further strengthening. Mazumdar et al. [4] proposed an anonymous endorsement system for the Hyperledger Fabric platform. This system uses ring signatures to conceal the link of the endorser's identity. The researchers analyzed the security and performance of the system by varying the size of the RSA modulus. However, the time efficiency of this system still requires improvement. Bhattacharjya et al. [5] conceived a lightweight, efficient, and secure hybrid RSA (SHRSA) messaging scheme, fortified with a four-tier authentication stack. While the scheme addresses the sluggish RSA decryption and its computational intensity, its security aspects warrant further exploration. Gupta et al. [6] tackled the vulnerability of the Diffie–Hellman (DH) algorithm to quantum attacks. They devised a certificate-less data authentication protocol employing lattice cryptography, which offers protection against quantum threats. This protocol also facilitates batch validation within a blockchain framework. Chen et al. [7] integrated the Diffie–Hellman (DH) algorithm's digital signature technology to replace conventional blockchain digital signature methods, enhancing resistance to attacks and bolstering the security of blockchain digital currency. Saini et al. [8] addressed the security concerns surrounding electronic medical records (EMRs). They employed the elliptic curve cryptography (ECC) to encrypt EMRs, subsequently storing them in the cloud. The associated hash values of these records are integrated into the blockchain. Jia et al. [9] introduced a privacy-centric authentication protocol tailored for the blockchain and the internet of medical things (IoMT). This protocol, grounded in elliptic curve cryptography (ECC) and physical unclonable function (PUF), not only satisfies stringent security criteria but also boasts minimal communication and computational overheads. Li et al. [10] developed a privacy-preserving blockchain model with ring signatures. This scheme establishes a data storage protocol based on elliptic curve ring signatures. Leveraging the inherent anonymity of ring signatures ensures robust data security and conceals user identity within blockchain applications. Ghayvat et al. [11] introduced a blockchain-centric confidentiality privacy protection scheme, CP-BDHCA, to mitigate user latency, excessive computation, and single-point-of-failure vulnerabilities inherent in healthcare cloud servers. Initially, the scheme employs elliptic curve cryptography (ECC) for digital signatures, establishing secure communication among various healthcare entities. Subsequently, it integrates both AES and RSA to shield cloud servers from malicious threats. Notably, this scheme outperforms conventional models in response time and offers robust defense against DoS and DDoS attacks.

Traditional cryptographic algorithms, like AES, boast impressive time efficiency. Their rapid encryption and decryption capabilities render them ideal for real-time data processing. This is particularly pertinent in healthcare applications where immediate data access is paramount. However, AES, as a symmetric encryption algorithm, uses the same key for encryption and decryption, which makes the security of the key critical. If the key is compromised or corrupted, all medical data encrypted using that key may be exposed or become inaccessible. This necessitates a secure mechanism for key distribution and management, an increasingly complex task in expansive healthcare systems. On the other hand, the elliptic curve cryptography (ECC) algorithm offers enhanced security with reduced key sizes and computational overhead, making it apt for resource-limited settings such as healthcare environments. Nonetheless, ECC may encounter efficiency challenges when processing large volumes of data. The computational complexity associated with ECC can render the encryption and decryption processes relatively sluggish, posing a concern in situations necessitating real-time access to medical data. Furthermore, if the

encryption and decryption of medical data are not sufficiently secure or efficient, there is a risk of exposing sensitive patient information to unauthorized entities. Such exposure could not only infringe upon patients' privacy rights but also subject healthcare organizations to legal liabilities and reputational harm. Consequently, selecting an encryption algorithm that strikes a balance between security and efficiency is crucial for safeguarding patient privacy and ensuring the integrity of medical data. To address the challenges of ensuring data security, facilitating rapid encryption, and simplifying key management complexities, this paper introduces a hybrid cryptographic algorithm that integrates the strengths of both AES and ECC. In this approach, AES swiftly encrypts the data, while ECC is employed to secure the AES key. We apply the hybrid cryptographic algorithm to data storage and sharing in blockchain healthcare scenarios and experimentally analyze its security, time efficiency, resource consumption, and advantages. The principal contributions of this paper are as follows:

1. We introduce HAE, a hybrid cryptographic algorithm based on AES and ECC. This algorithm employs AES for data encryption and ECC for encrypting the AES key. This approach not only ensures data security and algorithmic efficiency but also addresses the challenges associated with managing AES keys.
2. We have developed a blockchain-based healthcare application framework. Within this structure, we have seamlessly integrated technologies such as a blockchain and IPFS. Furthermore, we utilize the HAE hybrid cryptographic algorithm for the encryption and decryption of medical data.
3. We conducted a series of comparative experiments to underscore the advantages of HAE. Our results indicate that HAE outperforms other commonly used cryptographic algorithms in the blockchain in terms of security, time efficiency, and resource consumption.

The paper is ordered as follows. Section 2 provides an overview of AES, ECC, and blockchain technologies. In Section 3, we detail the encryption and decryption processes of the hybrid cryptographic algorithm, HAE. Section 4 presents a series of experiments related to HAE, accompanied by an in-depth analysis of the results. Lastly, Section 5 concludes the paper and outlines potential avenues for future research.

2. Relevant Knowledge

2.1. Advanced Encryption Standard—AES

The need for data security and privacy protection has become increasingly pressing in the digital age. Consequently, the research and development of encryption algorithms have taken on paramount importance. The advanced encryption standard (AES), also known as the Rijndael encryption algorithm, is a block cipher standard established by the National Institute of Standards and Technology (NIST) in 2001 [12]. AES operates on data blocks of 128 bits, and its variants are categorized based on key length: AES-128, AES-192, and AES-256. Each variant has a different number of encryption rounds, as detailed in Table 1.

Table 1. AES classification.

AES Type	Key Length/Bit	Packet Length/Bit	Encrypted Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

The AES algorithm operates on the principle of a block cipher, wherein plaintext data are divided into fixed-length blocks, and encryption and decryption are achieved through iterative operations and key expansion. The AES encryption process is depicted in Figure 1. This process ensures data protection through iterative rounds of encryption, with each round comprising specific steps such as byte exchange, row shift, column mix, and round key plus. A detailed breakdown of Figure 1 is as follows:

1. Initial Key Plus: The plaintext undergoes an exclusive OR operation with the initial key.
2. Byte Exchange: Each byte is replaced by referencing a predefined table, known as the S-box, to introduce confusion.
3. Row Shift: Each row of the plaintext undergoes a cyclic shift to the left, determined by its row number.
4. Column Mix: Specific mathematical operations are employed to mix the data columns, enhancing the encryption's complexity.
5. Round Key Plus: The outcome of each round undergoes an operation with the corresponding round key.

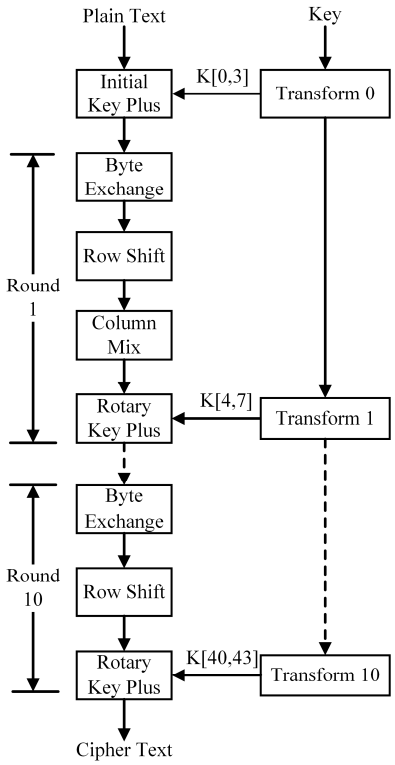

Figure 1. AES algorithm encryption process.

This procedure is iteratively executed across multiple rounds, with each round utilizing a distinct round key, culminating in the generation of the final ciphertext.

The AES algorithm has achieved international standardization and has been extensively adopted across diverse application domains. Given the existing computational capabilities, it offers rapid encryption and decryption through a highly optimized algorithmic design and is currently resistant to cracking. However, the AES algorithm necessitates rigorous key management, and the complexity associated with key management could potentially compromise security. As technology continues to evolve, the long-term security of the AES algorithm warrants ongoing research and validation.

2.2. Elliptic Curve Cryptography—ECC

Public key cryptography algorithms, as a cornerstone of modern cryptography, address the challenges of key management and distribution inherent in symmetric cryptography algorithms. Elliptic curve cryptography (ECC) [13] stands as a prominent public-key encryption technique. First introduced by Koblitz and Miller in 1985, ECC boasts distinct advantages and holds vast potential for a wide range of applications. Compared to traditional asymmetric cryptography algorithms such as RSA and Diffie–Hellman, ECC provides higher security with shorter key lengths, making it well-suited for encrypting

large data volumes, as seen in blockchain medical scenarios. However, the ECC algorithm is more complex, and it is less time-efficient as an asymmetric cryptographic algorithm.

The ECC algorithm is grounded in the mathematical theory of elliptic curves, characterized by the functional equation $y^2 = x^3 + ax + b$, which defines an approximate elliptic curve on the projective plane coordinate system. In ECC, a point at infinity, denoted as O_∞, serves as the zero element. A base point G is defined, and after k scalar multiplications, it generates the final point K, where k acts as the private key of the ECC cipher, and K serves as the public key. ECC leverages the computational difficulty of the elliptic curve discrete logarithm problem for encryption and decryption: given k and G, it is straightforward to compute $K = kG$; however, computing k when K and G are known is challenging, as division is more computationally intensive for computers.

Currently, ECC is emerging as the dominant choice in the new generation of public key cryptography. Much like RSA, ECC is typically employed for data encryption. In our blockchain medical application scenario, we specifically use ECC to enhance AES key management. By encrypting the AES key with ECC, we not only bolster the security of medical data but also elevate the overall trustworthiness of the blockchain-based medical application framework.

2.3. Blockchain Technology

In 2008, Satoshi Nakamoto introduced a groundbreaking electronic transaction system that operates independently of a trusted third party, marking the inception of blockchain technology [14]. A blockchain is a decentralized global ledger database, fortified by cryptographic methods, ensuring its attributes of decentralization, immutability, data integrity, and transparency. This avant-garde technology amalgamates peer-to-peer (P2P) networking [15], asymmetric encryption [16], and consensus mechanisms [17]. Utilizing an encrypted blockchain architecture, it stores data and verifies their authenticity and precision. Its applications span various sectors, including financial transactions, healthcare, digital currencies, and more. Figure 2 delineates the hierarchical structure of a blockchain.

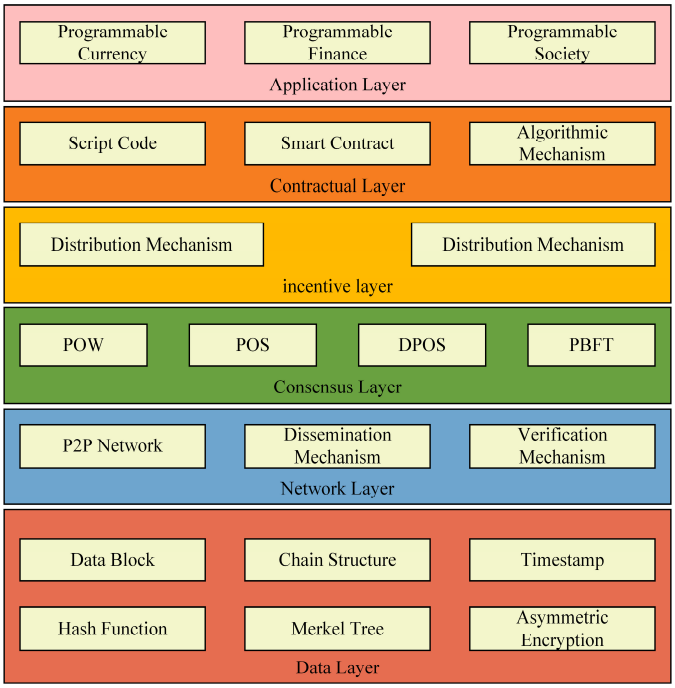

Figure 2. Hierarchy of blockchain.

In the blockchain architecture, the data layer employs hash functions and asymmetric encryption. This layer consists of data blocks and chained structures that house transac-

tional data, while Merkle trees archive state data. Integrating these methodologies ensures that the blockchain remains structured and resistant to tampering. At the network layer, the predominant protocol is P2P. Upon generating a new block, the primary node disseminates it to the subsidiary nodes. These nodes, upon receipt, proceed to validate the block's authenticity. Central to the blockchain's hierarchy is the consensus layer, which addresses the challenge of data consistency within distributed systems. Notable consensus algorithms encompass practical byzantine fault tolerance (PBFT) [18–20], delegated proof of stake (DPoS) [21], proof of stake (PoS) [22], and proof of work (PoW) [23]. The incentive layer primarily rewards nodes involved in computational and verification tasks. The intelligent contract anchors the contract layer. Within the blockchain ecosystem, all participants concur on predefined rules to deploy these smart contracts. When a transaction aligning with these conditions arises, the smart contract's code and algorithms are autonomously activated. The application layer, on the other hand, facilitates blockchain integration into everyday scenarios, predominantly spanning programmable currency, finance, and society. As blockchain gains traction, its potential to revolutionize sectors like healthcare becomes increasingly evident. For instance, Reegu et al. undertook a comprehensive review and analysis of the interoperability requisites for blockchain-supported EHR within the healthcare domain [24]. They introduced an interoperable framework for blockchain-based EHR [25] that aligns with the stipulations set forth by multiple national and international EHR standards, such as HIPAA and HL7. This framework guarantees the confidentiality, privacy, and integrity of medical records.

Furthermore, based on accessibility and deployment strategies, blockchains can be categorized into public, private, and consortium chains. Table 2 elucidates the distinctions among these three types.

Table 2. Three kinds of blockchain comparisons.

	Public Chain	Private Chain	Alliance Chain
Network Structure	fully decentralized	partially decentralized	multiple trusted centers
Joining Mechanism	random joining	internal node joining	specific group vetting joining
Consensus Mechanism	high fault tolerance and low transaction efficiency	low fault tolerance and high transaction efficiency	moderate fault tolerance and transaction efficiency

3. Hybrid Cipher Algorithm Based on AES and ECC

Individual encryption algorithms often have limitations but combining them can achieve more satisfactory results in practical applications. For instance, Ma et al. [26] introduced DRMchain, a novel blockchain-based digital rights management model. This model employs the AES algorithm for content encryption and the EDSA algorithm for digital signatures, offering a robust, secure, efficient, and tamper-proof solution for digital copyright protection. Oladipupo et al. [27] employed the ECC algorithm for encrypting and decrypting data within wireless sensor networks. For key exchange, they utilized a key negotiation algorithm based on both ECC and Diffie–Hellman, known as ECDH. Additionally, for the authentication of communicating nodes, he adopted a digital signature algorithm that integrates both ECC and DSA, termed ECDSA. Lin et al. [28] presented a composite cryptographic approach that leverages AES and RSA. In this method, RSA encrypts the AES key, while AES encrypts the data stored within the blockchain. Zhang et al. [29] developed a terminal data access control strategy to tackle data privacy and security challenges in the agricultural internet of things. This strategy employs CP-ABE and DES algorithms for hybrid data encryption, substantially simplifying key management and facilitating efficient encrypted data sharing. Abrar et al. [30] utilized the secure hash algorithm, SHA-256, for watermarking and storing these in the blockchain. Once encrypted with AES, these watermarks are integrated into images, thereby augmenting the image content's security,

anonymity, and integrity. Benil et al. [31] introduced the elliptic curve certificate-less aggregated cryptographic signature scheme (EC-ACS) to bolster the security of electronic health records (EHRs). This approach employs ECC to encrypt medical data. Concurrently, the certificate-less aggregated signature scheme (CAS) generates digital signatures. The integration of blockchain technology ensures the integrity and traceability of the EHR. Ghimire et al. [32] presented a novel video integrity verification method (IVM) grounded in a blockchain framework to counter video tampering attacks. This method synergizes a hash function-based message authentication code with the elliptic curve cipher to ascertain the video's integrity. Within this system, video clips of a fixed size are hashed, chained in real-time, and sequentially archived, culminating in a trustworthy database. During verification, the method is reapplied to the video clips, and the resultant hash value is juxtaposed with the one stored in the blockchain.

In the ever-evolving medical domain, swift data access and stringent data protection are paramount. Building upon prior research, this paper introduces a hybrid cryptographic algorithm, HAE (hybrid AES and ECC), which synergistically integrates the strengths of AES and ECC to address the inherent challenges posed by conventional cryptographic algorithms in medical data applications. AES, a symmetric cryptographic algorithm, is renowned for its exceptional time efficiency, making it indispensable for real-time data processing—a critical requirement in medical applications. However, the symmetric characteristic of AES, where encryption and decryption employ the same key, presents a significant challenge: the secure distribution and management of this key. In expansive healthcare systems with multiple entities requiring access to encrypted data, the secure dissemination of AES keys becomes intricate. On the other hand, ECC, an asymmetric cryptographic method, boasts superior security with shorter key lengths, making it especially valuable in resource-limited healthcare settings. The asymmetric design of ECC ensures data security; even if the public key is compromised, the data remain protected as long as the private key remains confidential. However, ECC's heightened security comes with a trade-off in time efficiency, rendering it less optimal for situations demanding rapid data access. Our proposed HAE algorithm endeavors to harness the strengths of both AES and ECC while mitigating their drawbacks. The encryption and decryption mechanics of this algorithm are delineated in Figures 3 and 4.

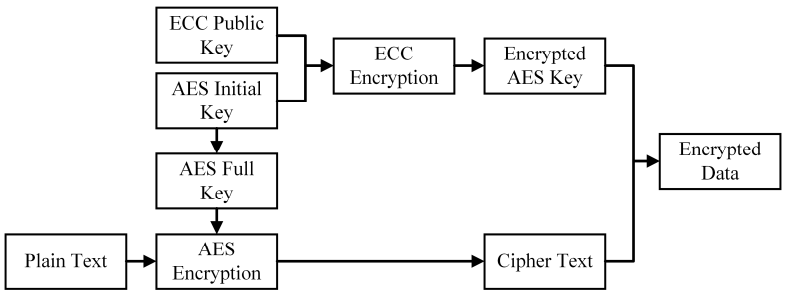

Figure 3. Hybrid cipher algorithm HAE encryption process.

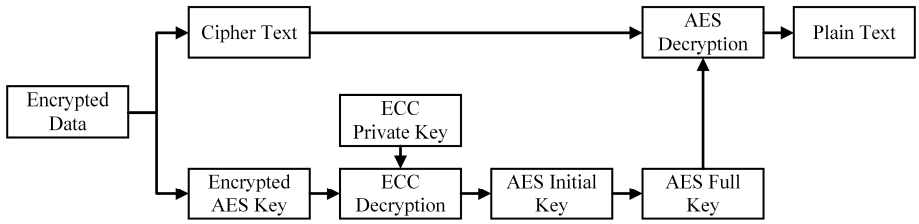

Figure 4. Hybrid cipher algorithm HAE decryption process.

HAE encryption process (as shown in Figure 3):

1. AES Key Generation: A 128-bit random number is generated as the AES initial key. Subsequent key expansion, alignment, and other operations are performed to derive the AES full key.
2. Plaintext Encryption: Using the AES full key, the plaintext undergoes AES encryption to produce the ciphertext. Given AES's efficiency, the plaintext can encompass extensive data, such as medical records.
3. AES Key Encryption: The AES initial key is encrypted using the ECC public key, resulting in the encrypted AES key. Encrypting only the AES initial key is a strategic choice to heighten the challenge for potential attackers attempting to intercept the AES full key during transmission.
4. Encrypted Data Formation: The encrypted AES key and the ciphertext are amalgamated to produce the final encrypted data, which are then dispatched to the recipient.

HAE decryption process(as shown in Figure 4):

1. Retrieving Encrypted Data: Upon receiving the encrypted data from the sender, the recipient extracts both the ciphertext and the encrypted AES key.
2. AES Key Decryption: The ECC private key decrypts the encrypted AES key, yielding the AES initial key.
3. Deriving the AES Full Key: The AES initial key undergoes processes like key expansion and alignment to derive the AES full key.
4. Ciphertext Decryption: The ciphertext is decrypted using the AES full key to retrieve the original plaintext.

The hybrid algorithm, HAE, seamlessly integrates the rapid encryption capabilities of the AES algorithm with the heightened security and streamlined key distribution and management features of the ECC algorithm. While AES is renowned for its robust security, its key management can be intricate. A superior layer of key protection is achieved by leveraging ECC to encrypt the AES key. AES is distinguished for its exceptional time efficiency, making it indispensable for real-time data processing. Although ECC may exhibit slightly reduced time efficiency, the impact is minimal due to the mere 128-bit size of the AES initial key, ensuring overall high efficiency. The HAE algorithm safeguards keys throughout the encryption process, effectively addressing the challenge of AES key management without sacrificing performance. This offers a robust solution to the intertwined challenges of security and efficiency that are intrinsic to cryptographic algorithms. Particularly within the unique realm of blockchain healthcare applications, HAE ensures the confidentiality, integrity, and authenticity of medical data.

4. Experiments and Analysis

4.1. Experimental Environment

The hardware environment utilized in this study comprised an Intel(R) Core(TM) i7-10750H CPU @ 2.60 GHz with 16 GB of RAM. The operating system was a 64-bit version of Windows 10. The compiler used was IntelliJ IDEA 3 February 2022, and the programming languages employed were Java and Golang. Algorithm simulation and testing were conducted using the Vmware16 virtual machine within the Ubuntu environment. The blockchain was constructed on the Hyperledger Fabric platform to facilitate the simulation and testing of the algorithms.

4.2. Experimental Procedures

Figure 5 presents the framework for the application of the hybrid cryptographic algorithm, HAE, within a blockchain healthcare context. This framework encompasses the blockchain, hospital entities, the InterPlanetary File System (IPFS), medical data, and the processes of encryption, decryption, data uploading, and retrieval. The detailed experimental procedure is as follows. When a patient visits Hospital 1, the institution generates the patient's medical data. These data are encrypted using the hybrid cryptographic algorithm HAE (as detailed in Figure 3) and subsequently uploaded to the InterPlanetary File System (IPFS) [33]. IPFS, a novel peer-to-peer file system, has gained significant traction in

blockchain and other distributed systems in recent years. Unlike traditional file systems that rely on directory-based addressing, IPFS uses content-based addressing. This unique approach facilitates segmenting large files into smaller chunks, enhancing throughput and storage efficiency. Once a file is archived in IPFS, the system provides a hash value as an address tag, enabling users to locate the file using this tag swiftly. Upon receiving the address hash from IPFS, Hospital 1 integrates with the blockchain as a node and uploads this hash. If a patient subsequently visits Hospital n and requires access to the medical data from Hospital 1, they simply grant authorization of their personal details to Hospital n. With this authorization, Hospital n retrieves the address hash via blockchain sharing, extracts the encrypted medical data from IPFS, and decrypts it using the HAE algorithm (as depicted in Figure 4) to access the original medical data. All medical data are encrypted using HAE and stored within IPFS. To access these data, hospitals must obtain patient authorization before decryption, including relevant personal information and the ECC private key. Importantly, hospital nodes on the blockchain store only have access to the address hash corresponding to the medical data, not the data themselves. This approach underscores the blockchain's decentralization principle and is pivotal for safeguarding medical data and patient privacy.

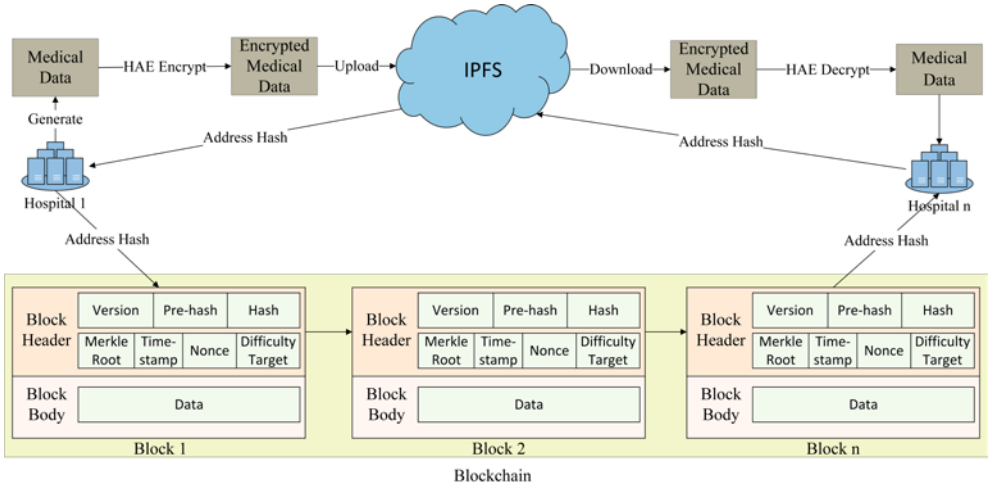

Figure 5. HAE application framework for blockchain healthcare scenarios.

The hybrid cryptographic algorithm HAE involves the following algorithmic steps:

1. AES Key Generation: The 'genKeyAES()' method is employed to generate the initial AES secret key. The 'loadKeyAES()' method is then used to convert the initial AES secret key into a 'SecretKey' object.
2. ECC Key Generation: The 'getKeyPair()' method is utilized to generate an ECC secret key pair. The public and private keys are subsequently converted into 'PublicKey' and 'PrivateKey' objects, respectively.
3. Encryption: The sender reads the medical file content using the 'Files.readAllBytes()' method. The actual content is encrypted with the 'encryptAES()' method using the full AES secret key. The AES initial secret key is then encrypted with the 'publicEncrypt()' method using the ECC public key.
4. Decryption: The receiver decrypts the file using the 'privateDecrypt()' method with the ECC private key to obtain the initial AES secret key. The file is then decrypted using the 'decryptAES()' method with the full AES secret key to retrieve the actual content of the file.

4.3. Experimental Results

The algorithm's outcomes are illustrated in Figure 6. This figure sequentially presents the ECC public key, ECC private key, the AES key used for encryption, the AES key post-

encryption with the public key, the actual content encrypted using the AES key, the AES key after decryption, and the actual content post-decryption. For the results in Figure 6, we employed Base64 encoding. Base64 is a widely used encoding method that transforms binary data into a text format composed of 64 printable ASCII characters. This encoding is essential for transmitting binary data in systems or communication protocols that do not support binary transmission. Since ASCII characters can be securely transmitted in text-based protocols, Base64 encoding ensures the data's integrity and reliability by converting binary data into a text format for transmission.

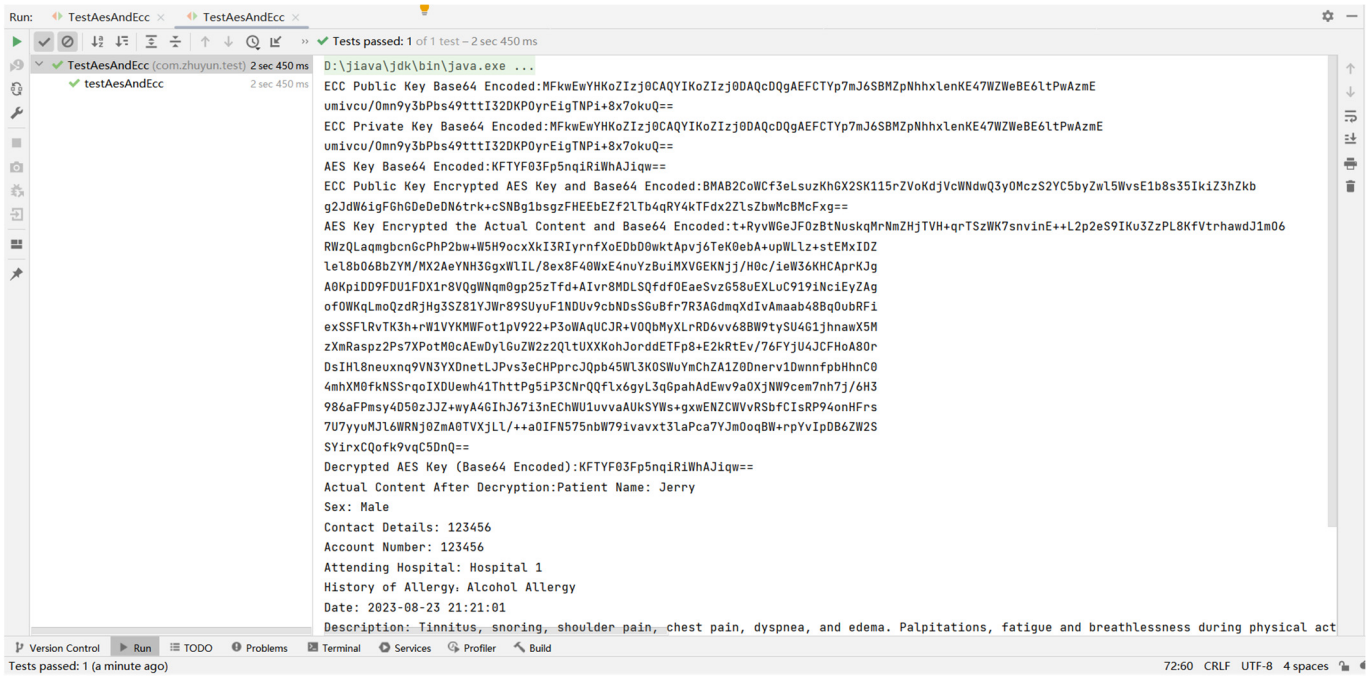

Figure 6. Result of running the hybrid cipher algorithm.

Figure 7 illustrates the procedure for sharing the address hash within the blockchain-based healthcare system. The figure delineates various elements, including the transaction ID, transaction time, data deletion status, and the IPFS address hash. Hospital 1 uploads the address hash to the blockchain. To access data related to a specific visit, Hospital n must retrieve the IPFS address hash, initially uploaded by Hospital 1, via blockchain sharing. Subsequently, Hospital n extracts the encrypted data from IPFS and decrypts them using the hybrid cryptographic algorithm HAE to obtain the original medical data, as depicted in Figure 8.

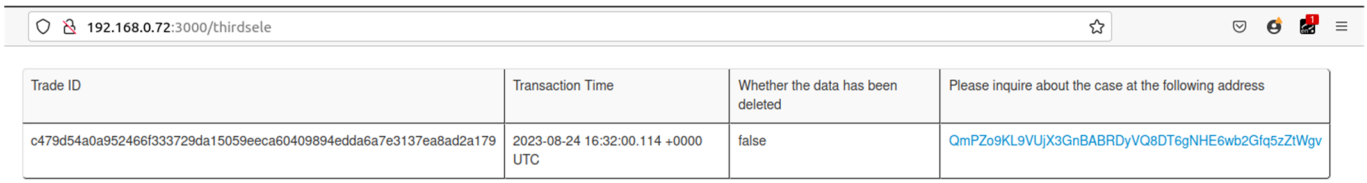

Figure 7. Shared address hash.

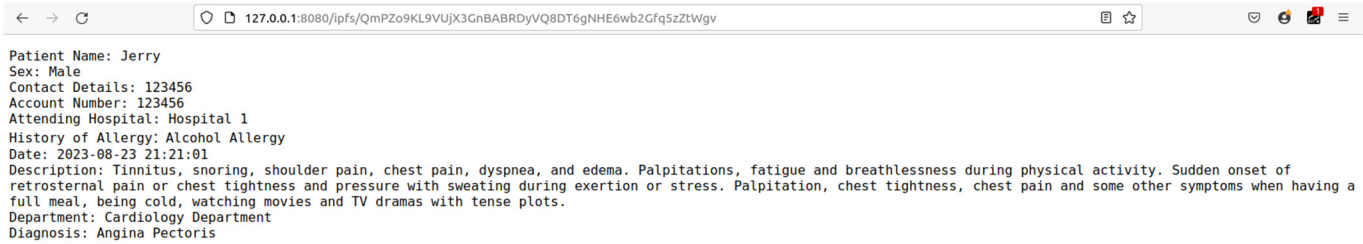

Figure 8. Initial medical data.

4.4. Experimental Analysis

In this section, we provide a comprehensive description of the experimental methodology employed for the hybrid cryptographic algorithm, HAE, and elucidate the advantages it holds over other algorithms. For our experiments, we utilized medical data extracted from patient records. These data were encrypted and decrypted using HAE within a Java environment, with a specific focus on protecting the AES key. From a security perspective, both AES and ECC underwent rigorous mathematical analysis. Their resilience against cryptographic attacks was scrutinized to affirm the superior security attributes of HAE. For assessing time efficiency, we selected the ECC, AES+RSA hybrid cryptographic algorithms, and the HAE algorithm, as previously explored by other researchers. We conducted encryption and decryption tests on medical data sets of sizes 1 MB, 5 MB, 10 MB, 15 MB, and 20 MB. By comparing the time taken by each algorithm for these operations, we aimed to highlight the time efficiency advantages of HAE. Regarding resource consumption, we again used the ECC, AES+RSA, and HAE algorithms to encrypt and decrypt medical data sets of sizes 1 MB, 5 MB, 10 MB, 15 MB, and 20 MB. By observing the differences in CPU utilization during the execution of these algorithms, we sought to demonstrate the resource consumption benefits of HAE.

4.4.1. Security Analysis

The hybrid cryptographic algorithm HAE employs AES for data encryption and ECC for AES key encryption, offering enhanced security compared to the traditional AES algorithm. In the conventional AES algorithm, the same key is used for encryption and decryption operations, making key security crucial. In contrast, HAE uses ECC to encrypt the AES key, leveraging the benefits of asymmetric encryption to provide a higher level of key protection. HAE employs ECC asymmetric encryption in the key exchange and data transmission processes, offering stronger resistance to attacks, particularly against specific attacks targeting the symmetric encryption algorithm AES, such as cryptanalysis and exhaustive search attacks. Even if attackers manage to crack the AES algorithm, they will still need to decrypt the AES key to access the data. Moreover, both the AES and ECC algorithms are inherently secure. AES employs a multi-round iterative network structure that combines complex mathematical operations with nonlinear transformations to achieve robust obfuscation and diffusion properties. AES supports various key lengths, including 128-bit, 192-bit, and 256-bit, with longer key lengths offering higher security. AES has undergone extensive cryptographic analysis and evaluation, and there is no publicly available effective attack method capable of breaking full-round AES encryption. The current best-known attack methods target AES variants with fewer rounds using approaches such as brute force exhaustion, as shown in Table 3. For full-round AES encryption, as long as the key is strong enough, it is theoretically considered secure. The security of ECC is based on the elliptic curve discrete logarithm problem, and there is no effective attack method within the current scope of mathematical knowledge and related algorithms. Therefore, using ECC encryption to protect the AES key is considered safe. In the context of blockchain-based medical applications discussed in this paper, the combined encryption techniques of AES and ECC ensure the protection of medical data during both transmission and storage. Specifically, the use of ECC encryption safeguards the

AES key. Consequently, crypto-attackers cannot access the AES key's details, rendering them incapable of decrypting the ciphertexts. This strategy effectively ensures the security of the medical data. The encrypted data are stored within the IPFS. Any unauthorized alterations to this encrypted data are promptly identified during decryption, as such modifications result in an output that diverges from the original data. Nodes within the blockchain retain the file address hash provided by IPFS. Leveraging public key encryption, timestamps, node consensus, and other advanced technologies, the blockchain guarantees the immutability of data on the chain. This comprehensive approach ensures the medical data's confidentiality, integrity, and authenticity. In summary, AES provides efficient data encryption and decryption, while ECC offers robust key protection. Combining the two into a new hybrid cryptographic algorithm ensures both data and key protection, delivering more comprehensive security.

Table 3. AES attack methods and cracking time.

Style of Attack	Breaking Time (Times)
exhaustive attack	2^{128}
recover key attack	2^{126}
related key attack	2^{99}

4.4.2. Time Efficiency Analysis

Given the limitations of algorithms such as AES, DES, and RSA, including challenges in key management and lower security strength, this paper selects ECC, the AES+RSA hybrid cryptographic algorithm [28], and the AES+ECC hybrid cryptographic algorithm HAE proposed herein for comparative analysis, as depicted in Figure 9.

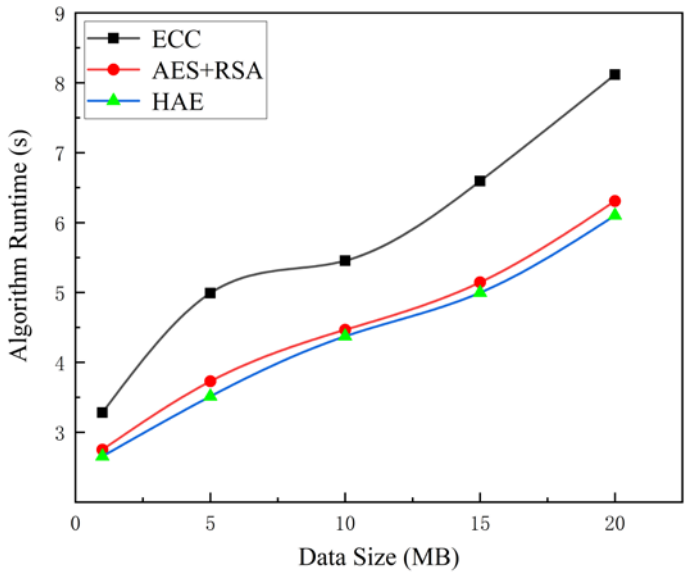

Figure 9. Comparison of encryption and decryption time of three cryptographic algorithms.

For the same data size, the time required for encryption and decryption by the two hybrid cryptographic algorithms is significantly less than that of the ECC algorithm. The hybrid algorithm HAE, based on AES and ECC proposed in this paper, exhibits slightly better time efficiency than the AES+RSA hybrid algorithm proposed by previous authors. Under equivalent security levels, the key length of ECC is substantially shorter than that of RSA, as shown in Table 4. This implies that ECC holds a significant advantage over RSA regarding attack resistance, resource consumption, network consumption, encryption and decryption speed, and suitability for blockchain scenarios. Consequently, the HAE

algorithm offers high time efficiency while ensuring security, providing algorithmic support for encrypted data storage and sharing in blockchain medical scenarios.

Table 4. Key lengths of ECC and RSA with equal security.

Breaking Time/Mips-YEARS	ECC/Bit	RSA/Bit
10^4	132	768
10^{12}	160	1024
10^{20}	210	2048
10^{31}	283	3072
10^{52}	410	7680
10^{67}	571	15,360

4.4.3. Analysis of Resource Consumption

From an algorithmic perspective, as depicted in Figure 10, the CPU utilization for the hybrid cryptographic algorithm HAE exhibits a slight increase with the growth in data size. Nevertheless, this uptick remains modest, hovering between 20% and 30%. Furthermore, the HAE algorithm demonstrates a reduced CPU utilization rate for equivalent data sizes, compared to both the ECC and the combined AES+RSA algorithms. This suggests that HAE is more efficient in terms of resource consumption.

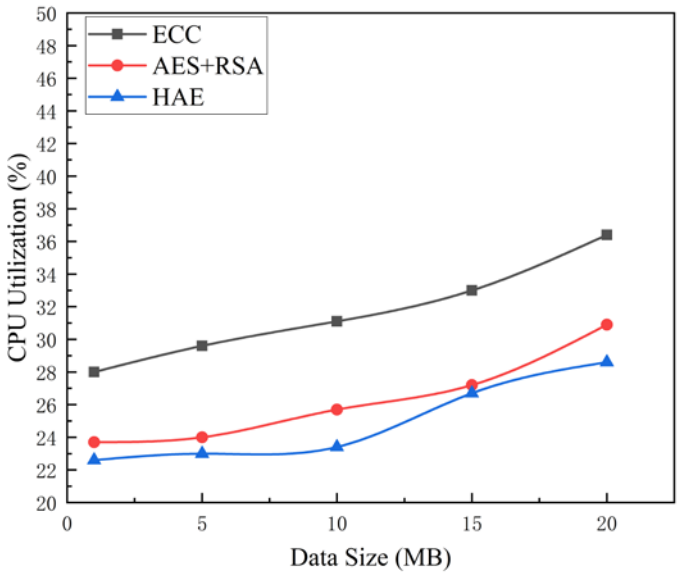

Figure 10. Comparison of CPU utilization of three cryptographic algorithms.

Considering its practical application within blockchain medical contexts, as illustrated in Figure 5, medical data are encrypted and housed within the InterPlanetary File System (IPFS). The address hash returned by IPFS is then disseminated and stored across blockchain nodes. Given the minimal data volume within this hash, there is no significant resource consumption. As a result, the hybrid cryptographic algorithm HAE holds promising potential for deployment in blockchain medical scenarios.

Table 5 presents a performance comparison among the HAE, ECC, and AES+RSA algorithms. As evident from the table, both HAE and ECC exhibit robust security levels. However, the inherent limitations of RSA render the AES+RSA combination slightly less secure than its counterparts. In terms of operational speed, HAE emerges as the fastest, followed by AES+RSA, with ECC trailing behind. Regarding resource consumption, HAE is the most efficient, while ECC consumes the most resources, and AES+RSA falls in between. In the broader context of blockchain healthcare applications, HAE's advantages become even more pronounced. Consider the use case illustrated in Figure 5: medical

data generated by Hospital 1 must be encrypted securely for storage, yet remain accessible for decryption by other entities, such as Hospital n, in a swift and efficient manner. Here, HAE's prowess is unparalleled. Firstly, from a security perspective, HAE employs AES for data encryption and uses ECC for the AES key encryption, effectively offering dual-layer protection for both data and key. Given the widespread validation of ECC and AES as secure algorithms, the integrity of medical data remains uncompromised. Secondly, in terms of time efficiency, HAE consistently outperforms both ECC and AES+RSA in encryption and decryption tasks, especially when handling equivalent data sizes. This implies that when entities like Hospital n retrieve and decrypt medical data from IPFS, HAE facilitates faster access to the original data. Lastly, concerning resource consumption, HAE is more resource-efficient than both ECC and AES+RSA. This efficiency is crucial in resource-sensitive healthcare environments, ensuring that encryption and decryption processes remain streamlined without straining the system. Furthermore, HAE's compatibility with IPFS is noteworthy. IPFS's content-based addressing mechanism allows for the segmentation and storage of large files. When paired with HAE's efficient encryption and decryption capabilities, a secure and efficient storage and retrieval solution for healthcare data is realized. In summation, the HAE hybrid cryptographic algorithm stands out in terms of security, time efficiency, and resource consumption, positioning it as a prime choice for the encryption, storage, and sharing of medical data in blockchain healthcare scenarios.

Table 5. Performance comparison of three cryptographic algorithms.

Cryptographic Algorithm	Security Level	Encryption Speed	Resource Consumption
ECC	high	slow	high
AES+RSA	relatively high	relatively fast	relatively low
HAE	high	fast	low

5. Conclusions

To address the challenge of encrypted storage and secure blockchain data sharing, this paper introduces a hybrid cryptographic algorithm, HAE, based on AES and ECC, and applies it to blockchain medical scenarios. During encryption, HAE uses the ECC public key to encrypt the AES initial key and employs the complete AES key to encrypt the original data. For decryption, the ECC private key is used to decrypt the AES initial key, which is then used with the complete AES key to retrieve the original data. HAE ensures data security while addressing the challenge of managing the AES key. We conducted comparative experiments between the HAE algorithm and both the ECC and AES+RSA hybrid cryptographic algorithms. The results indicate that HAE outperforms ECC and AES+RSA in terms of time efficiency and resource consumption, while maintaining superior security. Within the medical application framework proposed, HAE synergizes with the blockchain, IPFS, and other technologies to securely store and share medical data. Our experimental findings underscore HAE's commendable performance in security, time efficiency, and resource consumption, suggesting its viability for real-world applications in blockchain medical scenarios. In summary, this study presents a novel direction for ensuring data security and privacy protection within the medical sector. The HAE algorithm guarantees the confidentiality, integrity, and authenticity of medical data during transmission and storage, thereby mitigating the risks of data breaches and unauthorized access. By paving the way for an era of enhanced protection in the medical domain, HAE ensures that patient data remain confidential and secure in an increasingly digitalized healthcare environment.

In future endeavors, we aim to refine the efficiency of the HAE algorithm and broaden its applicability to sectors like finance and public services. However, deploying the HAE algorithm in these sectors presents distinct challenges. The financial sector, given the critical nature of its transactions, demands heightened security. Conversely, the public service sector necessitates scalability to cater to an expansive user base. Addressing these unique requirements will entail further research and potential refinements to the HAE

algorithm. Concurrently, we are looking to incorporate user authentication features into our blockchain healthcare application framework. Comprehensive evaluations will be undertaken to assess the framework's security and performance, ensuring HAE's resilience and adaptability across diverse sectors.

Author Contributions: Conceptualization, Z.C. and J.G.; methodology, Z.C.; software, Z.C.; validation, Z.C.; formal analysis, Z.C.; investigation, H.Y.; resources, J.G.; data curation, Z.C.; writing—original draft preparation, Z.C.; writing—review and editing, Z.C. and J.G.; visualization, Z.C.; supervision, H.Y.; project administration, Z.C. and J.G.; funding acquisition, H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Hebei Province Higher Education Teaching Reform Research and Practice Program grant number (2020GJJG158), and by the Ministry of Education Industry–University–Research Cooperative Education Program grant number (202101107009).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Acknowledgments: Support by colleagues and the university is acknowledged.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Banerjee, S.; Bera, B.; Das, A.K.; Chattopadhyay, S.; Khan, M.K.; Rodrigues, J. Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. *Comput. Commun.* **2021**, *169*, 99–113. [CrossRef]
2. Li, H.; Pei, L.S.; Liao, D.; Chen, S.; Zhang, M.; Xu, D. FADB: A Fine-Grained Access Control Scheme for VANET Data Based on Blockchain. *IEEE Access* **2020**, *8*, 85190–85203. [CrossRef]
3. Jadav, N.K.; Kakkar, R.; Mankodiya, H.; Gupta, R.; Tanwar, S.; Agrawal, S.; Sharma, R. GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G. *Digit. Commun. Netw.* **2023**, *9*, 422–435. [CrossRef]
4. Mazumdar, S.; Ruj, S. Design of Anonymous Endorsement System in Hyperledger Fabric. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1780–1791. [CrossRef]
5. Bhattacharjya, A.; Zhong, X.F.; Li, X. A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme with Four-Layered Authentication Stack. *IEEE Access* **2019**, *7*, 30487–30506. [CrossRef]
6. Gupta, D.S.; Karati, A.; Saad, W.; da Costa, D.B. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3255–3266. [CrossRef]
7. Chen, H.; Su, K.C.; Gao, W.D. The Analysis of Blockchain Digital Currency Product Innovation Based on Artificial Immune Algorithm. *IEEE Access* **2022**, *10*, 132448–132454. [CrossRef]
8. Saini, A.; Zhu, Q.Y.; Singh, N.; Xiang, Y.; Gao, L.X.; Zhang, Y.S. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2021**, *8*, 5914–5925. [CrossRef]
9. Jia, X.Y.; Luo, M.; Wang, H.Q.; Shen, J.; He, D.B. A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things. *IEEE Internet Things J.* **2022**, *9*, 21838–21850. [CrossRef]
10. Li, X.F.; Mei, Y.R.; Gong, J.; Xiang, F.; Sun, Z.X. A Blockchain Privacy Protection Scheme Based on Ring Signature. *IEEE Access* **2020**, *8*, 76765–76772. [CrossRef]
11. Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1937–1948. [CrossRef] [PubMed]
12. Dogan, A.; Ors, S.B.; Saldamli, G. Analyzing and comparing the AES architectures for their power consumption. *J. Intell. Manuf.* **2014**, *25*, 263–271. [CrossRef]
13. Benssalah, M.; Rhaskali, Y.; Drouiche, K. An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimed. Tools Appl.* **2021**, *80*, 2081–2107. [CrossRef]
14. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: http://bitcoin.org//Bitcoin.pdf (accessed on 23 August 2023).
15. Li, H.; Lu, R.; Mahmoud, M.M.E.A. Security and privacy of machine learning assisted P2P networks. *Peer-Peer Netw. Appl.* **2020**, *13*, 2234–2236. [CrossRef]
16. Yuan, Y.; Wang, F.Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1421–1428. [CrossRef]

17. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Kim, D.I. A survey on consensus mechanisms and mining management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
18. Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1146–1160. [CrossRef]
19. Chen, Z.; Qiang, L. Improved PBFT consensus mechanism based on K-medoids. *Comput. Sci.* **2019**, *46*, 101–107.
20. Li, B.; Xu, W.; Abid, M.Z.; Distlerand, T.; Kapitza, R. SAREK: Optimistic Parallel Ordering in Byzantine Fault Tolerance. In Proceedings of the 2016 12th European Dependable Computing Conference (EDCC), Gothenburg, Sweden, 5–9 September 2016; pp. 77–88.
21. Song, M.Y.; Li, C.L.; Ye, J.S.; Gong, X.Q.; Luo, Y.L. Efficient consensus algorithm based on improved DPoS in UAV-assisted mobile edge computing. *Comput. Commun.* **2023**, *207*, 86–99. [CrossRef]
22. Yaqin, W.; Pengxin, S.; Fuxin, W. Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and Its Application in Blockchain. *Math. Probl. Eng.* **2020**, *2020*, 7270624.
23. Wei, Y.K.; An, Z.X.; Leng, S.P.; Yang, K. Evolved PoW: Integrating the Matrix Computation in Machine Learning into Blockchain Mining. *IEEE Internet Things J.* **2023**, *10*, 6689–6702. [CrossRef]
24. Reegu, F.A.; Abas, H.; Jabbari, A.; Akmam, R.; Uddin, M.; Wu, C.M.; Chen, C.L.; Khalaf, O.I. Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges. *Secur. Commun. Netw.* **2022**, *2022*, 9227343. [CrossRef]
25. Reegu, F.A.; Abas, H.; Gulzar, Y.; Xin, Q.; Alwan, A.A.; Jabbari, A.; Sonkamble, R.G.; Dziyauddin, R.A. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability* **2023**, *15*, 6337. [CrossRef]
26. Ma, Z.F.; Jiang, M.; Gao, H.M.; Wang, Z. Blockchain for digital rights management. *Future Gener. Comput. Syst.-Int. J. eSci.* **2018**, *89*, 746–764. [CrossRef]
27. Oladipupo, E.T.; Abikoye, O.C.; Imoize, A.L.; Awotunde, J.B.; Chang, T.Y.; Lee, C.C.; Do, D.T. An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks. *IEEE Access* **2023**, *11*, 1306–1323. [CrossRef]
28. Lin, H.; Li, X.L.; Gao, H.Y.; Li, J.; Wang, Y.S. ISC-MTI: An IPFS and smart contract-based framework for machine learning model training and invocation. *Multimed. Tools Appl.* **2022**, *81*, 40343–40359. [CrossRef] [PubMed]
29. Zhang, G.F.; Chen, X.; Zhang, L.; Feng, B.; Guo, X.C.; Liang, J.Y.; Zhang, Y.A. STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted Agricultural IoT Blockchain Terminal. *Int. J. Interact. Multimed. Artif. Intell.* **2022**, *7*, 66–75. [CrossRef]
30. Abrar, A.; Abdul, W.; Ghouzali, S. Secure Image Authentication Using Watermarking and Blockchain. *Intell. Autom. Soft Comput.* **2021**, *28*, 577–591. [CrossRef]
31. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **2020**, *178*, 107344. [CrossRef]
32. Ghimire, S.; Choi, J.Y.; Lee, B. Using Blockchain for Improved Video Integrity Verification. *IEEE Trans. Multimed.* **2020**, *22*, 108–121. [CrossRef]
33. Politou, E.; Alepis, E.; Patsakis, C.; Casino, F.; Alazab, M. Delegated content erasure in IPFS. *Future Gener. Comput. Syst.-Int. J. eSci.* **2020**, *112*, 956–964. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.