Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 3624360, 11 pages
https://doi.org/10.1155/2022/3624360

Research Article

Construction of a Multimedia Education Resource Security Model Based on Multistage Integration

Lina Yuan

Changchun Humanities and Sciences College, Changchun 130117, China

Correspondence should be addressed to Lina Yuan; yuanlina@ccrw.edu.cn

Received 14 April 2022; Accepted 13 May 2022; Published 3 June 2022

Academic Editor: Xuefeng Shao

A security model of multimedia education resource fusion based on multistage integration of multimedia educational resources is constructed in this paper in the context of smart education. First, the teaching model of multimedia education resource fusion is analyzed and the IoT communication evolution model and functional architecture model are constructed accordingly, based on which the realization path of IoT intelligent sensing, intelligent management, emotional computing, device sharing, and vision simulation functions for smart education are discussed. The security model uses a decentralized cryptographic data security sharing method based on blockchain for protection and supports blockchain to record user attributes to ensure the confidentiality and integrity of data. The experimental and analytical results indicate that the scheme can effectively reduce the computational overhead of smart devices while ensuring the security of data sharing. Moreover, the proposed model in the paper achieves better performance than other methods in terms of security strength, encryption, and decryption time.

1. Introduction

In the current context of the gradual improvement of China's science and technology level, both the way of life and the content of work have seen certain changes. The application of information technology can not only guide the stable development of China's social economy but also create good conditions for the healthy development of education. In the Internet environment, various multimedia technologies are applied in school teaching activities. The integration of multimedia teaching resources can lead to the reform and innovation of information-based teaching methods. This can cater to the development needs of the times and set a perfect teaching system [1, 2]. Information-based teaching is not only a single teaching technology but also a reflection of modern teaching methods and concepts [3]. This not only promotes the integration of multimedia educational resources and classroom teaching resources but also broadens the transmission channels of professional subject knowledge and expands the horizons of students' professional subject knowledge. Emphasis on the development of the teaching model with the integration of multimedia educational resources can enrich the educational resources of professional disciplines and achieve the effectiveness of the development of the teaching model [4].

Smart education is formed by drawing on the core of the concept of "wisdom", integrating it closely with culture, and extending it to the field of education. Smart education relies on technology integration, which upholds the principle of optimal collaboration, pursues the creation of thinking with precision and personalization, and facilitates teachers to effectively broaden their teaching paths. At the same time, it uses efficient and flexible teaching methods to provide learners with personalized teaching services that enhance their learning experience and stimulate their learning and creative potential, while it implicitly guides learners to form correct values and refine their thinking quality [5]. Smart education is a new form of education that emerges from the integration of new-generation information technologies such as cloud computing, big data, social networks, wireless communication, and the Internet of Things under the guidance of advanced educational ideas [6, 7]. The development of smart education has set off the fourth wave after digital education, mobile education, and ubiquitous education and has become one of the current hot spots with the highest attention in the international education field. The key technologies of smart education are mainly composed of multimedia, radio frequency identification (RFID), sensors, network communication, data processing and fusion, etc. Through the use of RFID, sensors, infrared sensors, laser scanners, global positioning systems, and other information collection devices, any item information is connected to the Internet for communication and interaction to achieve intelligent perception, identification, calculation, display, monitoring, positioning, tracking, and management [8, 9].

The development of smart education environment depends on the development process and strength of smart education Internet of Things (IoT), which has developed rapidly in China in the last decade [10]. Especially after National Leaders inspected R&D Center, smart education IoT has received wide attention and related research has shown explosive growth [11]. Between 2015 and 2021, keywords such as multimedia education resource integration, affective computing, visual simulation, smart classroom [12], and education informatization 2.0 became the buzzwords of smart education [13]. This indicates the development trend of smart education IoT on the one hand and the era of mature application of smart education IoT on the other hand. However, there are fewer studies to study the functional model of IoT with the entry point of smart education centered on the integration of multimedia educational resources. Also, for the security of IoT education data, in-depth research is needed [14].

Facing the security problem of IoT in a cloud computing environment, many solutions have been proposed [15]. The literature [16] addresses the problem of IoT resource management in cloud computing services. Literature [17] distributed a fog resource management framework for IoT services using dynamic resource configuration in the fog framework to handle user requests. There are also cryptographic-based security privacy frameworks for IoT [18]. The literature [19] uses blockchain combined with keyword-based searchable attribute-based encryption (KSABE) to achieve IoT security and privacy protection. Literature [20] proposed a blockchain data access control scheme based on a ciphertext-policy attribute-based encryption (CP-ABE) algorithm. A blockchain-based secure verifiable data sharing scheme for in-vehicle social networks is proposed in literature [21]. This scheme relies on traditional trusted third-party AA servers to manage user attributes and a cloud service provider (CSP) to keep the attribute private keys. Therefore, it has the risk of data leakage due to single point of failure of the third party and malicious impersonation of legitimate cloud service providers by attackers. Literature [22] uses blockchain technology to ensure the integrity and tamper-evidence of data in the CP-ABE searchable encryption scheme. The abovementioned schemes effectively improve the security of IoT, but they are not able to resist the problem of user impersonation attribute attacks and the encryption of data is single algorithm or less identity authentication.

Based on the above research, in order to improve the security performance of the smart education IoT model centered on the integration of multimedia educational resources, this paper proposes a multistage IoT security model based on multimedia education resource fusion. The model constructs the IoT communication evolution model and functional architecture model for smart education, in which a blockchain-based multistage decentralized cryptographic data security sharing scheme is designed for the model, which can effectively ensure the security of education IoT in a cloud computing environment.

Section 2 of the paper is the state of the art, which is an introduction to the multimedia educational resources integration features and the IoT model for smart education. Section 3 is the methodology, which is about the security scheme of the IoT model. Section 4 is the result analysis and discussion. Section 5 is the conclusion.

2. State of the Art

Smart education relies on network technology and multimedia technology to carry out intelligent teaching with digital characteristics. It upholds the concept of "learner-centered", relies on an open teaching platform, realizes intelligent teaching, and instantly achieves a high level of sharing of teaching information. Relying on large-scale digital and networked teaching, smart education realizes in-depth teaching interaction and highlights the differentiated features and personalized advantages of ubiquitous learning. Through innovative information technology, smart education can widely acquire and precisely find teaching resources and complete the comprehensive production of teaching resources according to teaching needs. Moreover, in the process of building the teaching environment, it relies on cloud technology, various types of smart terminals, and flexibly uses diversified teaching methods to promote the teaching effect to achieve significant enhancement.

The important value of IoT for smart education in the process of promoting qualitative changes in smart education is mainly reflected in two aspects. (1) The frontier technology of IoT for smart education has triggered changes in education management mode and teaching mode, profoundly changed the learning and lifestyle of teachers and students, and can promote the cultivation of students' innovation ability. (2) The IoT for smart education has a great application potential, which helps to better promote students' growth, improve teaching quality and efficiency, and create a new future for education development.

2.1. Characteristics of Multimedia Education Resource Integration

2.1.1. Multiple Teaching Modes in Conjunction. The smart education model of multimedia educational resources is a task-driven model with teaching objectives as a guide for exploration, leading students, and teachers to move toward the goals in the process of learning and education implementation, thus achieving the goal of good education according to the material. The smart education mode, relying on multimedia educational resources, promotes the diversification of professional subject education. Through the cooperation of various teaching modes, including group cooperative learning mode and contextual teaching mode, the mode of knowledge transfers and instillation is changed, thus driving students' learning enthusiasm, promoting students' acquisition, absorption and perception of knowledge, and thus promoting students' effective mastery of subject knowledge.

2.1.2. Changes in the Role. In the traditional teaching mode, the teacher is the leader, delivering professional course knowledge to students. In contrast, the wisdom education mode of multimedia education resources' integration is different from the previous education form, which attaches more importance to students' subjective learning status. In this mode of education, teachers are the organizers and leaders of teaching, organizing teaching activities for students, and carrying out effective theoretical and practical teaching modes. This allows students to rely on multimedia educational resources to carry out effective learning mode, so that students can continue to improve their own abilities and qualities in independent learning.

2.1.3. Enriching Educational Resources. Multimedia educational resources are rich, innovative, comprehensive, mobile, diverse, miniaturized, and of high quality. This can provide rich educational resources for the implementation of intelligent education mode, so as to realize the effectiveness of professional subject education and teaching. With the further development of information technology, multimedia education resources are also constantly being broadened and improved. For example, the generation of thinking and the amount of information of network data are unimaginable. After further research of educators, the richness and comprehensiveness of multimedia educational resources will be further optimized.

2.2. IoT Communication Evolution Model and Functional Architecture Model. The evolution of smart education IoT communication includes functional evolution and field evolution. The Internet and mobile Internet provide conditions for intelligent interaction in smart education. The IoT communication evolution model for smart education is shown in Figure 1.

Smart education communication is rapidly developing based on the underlying communication protocols of computer and communication technology. The information is sensed and identified through IoT PADs, RFID of smart devices, sensors, global positioning system (GPS), programmable logic controller (PLC), etc., to obtain audio, video, images, and other information. The acquired information is then proximity-propagated by Zigbee, near field communication (NFC), and Bluetooth to the ubiquitous sensor network (USN). Smart education IoT communication evolution has gone through three stages: first, the Machine-Machine (M2M) phase, i.e., the computer education era. This phase saw its sensing information evolve rapidly toward IP-based (field evolution) and intelligent (functional evolution) directions, respectively. Then, it enters the human-object communication stage, i.e., the network education era. This stage realizes communication for all Human-Human (H2H) through telegraphic telephones, mobile telephones, and leveraging mobile Internet and Internet, and its perceived information continues to evolve toward broadbandization (field evolution) and mobility (functional evolution). Finally, it enters the education communication stage, in which advanced teaching interaction is realized through IPV6, educational cloud computing, and educational big data technology, and its perceived information develops rapidly in the direction of ubiquitination and wisdom. This stage is also the "artificial intelligence + education" era of intelligent education.

The evolution of the communication of smart education IoT shows the recurrence of its structural functions. The smart education IoT is characterized by intelligence, perception, interconnection, automation, and its polymorphic interaction function. According to the smart education IoT evolution, the development trend of itself and the smart education environment has been evoluted. And from the analysis of the conceptual model of IoT, the model of IoT architecture level (sensing layer, transmission layer, and application layer) and the social IoT architecture model. Starting from the analysis of smart education applications (smart campus, smart classroom, smart laboratory, and smart library, etc.) and smart education development architecture, a smart education IoT functional architecture model is constructed as shown in Figure 2.

Perception technology and wireless sensor networks (WSN) for smart education IoT are the foundation of smart education communication. Internet and mobile networks are the key to human-computer interaction. Smart chips, sensors, and GPS sense the information of smart education environment. Zigbee, Bluetooth, WiFi, NFC, etc. transmit information and carry out network identification, positioning, tracking, monitoring, display, and management through "Human-Thing" (H2T), "Human-Machine" (H2M), "Thing-Machine" (T2M), "Human-Human" (H2H), "Thing- Thing" (T2T), and "Machine-Machine" (M2M). M2M interactions provide services for smart learning and meet the requirements of interactive experiences for learners. Humanized multistate interaction often depends on the "Human-Thing" communication equipment "intelligence" and multimodal "human-computer" interaction design. Smart education IoT provides support for natural, convenient, and efficient interactions between people, machines, and things to achieve intelligent perception, intelligent management, emotional computing, device sharing, and vision simulation.

2.3. Function Implementation. From the smart education IoT functional architecture model, it is found that the functional realization paths are mainly as follows.

2.3.1. Intelligent Sensing. Intelligent sensing is the most essential feature of smart education. Smart perception includes accurate location, comprehensive sensing, and

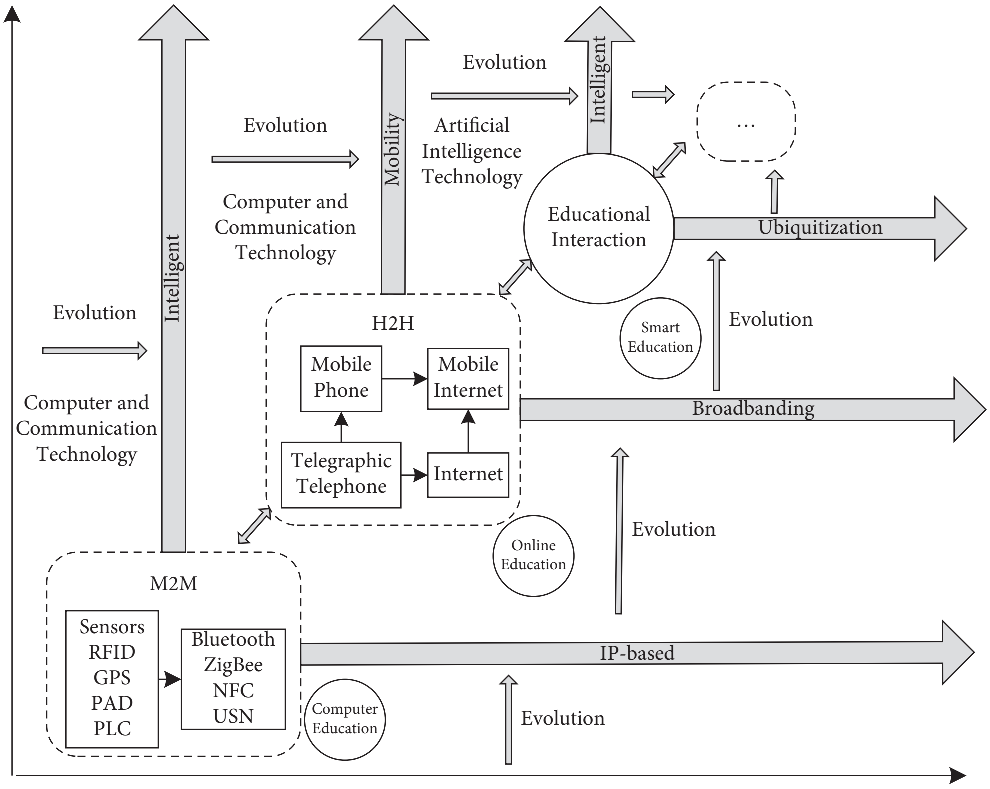

Figure 1: IoT communication evolution model.

reliable transmission. Smart perception senses information about students through sensor nodes and provides students with autonomous, personalized, and adaptive learning services. Smart perception in smart education is mainly manifested in three aspects: First, the smart perception of the learning environment. Second, intelligent perception of learning contents. The third is the intelligent perception of the learning context. The three aspects are processed in batches. The inconsistency, incompleteness, and imprecision in each batch of information can be cleared up before its inference, so that the uncertainty of high-level information can be limited to a specific degree.

2.3.2. Smart Management. The IoT for smart education can be built with functions such as teacher and student identification and positioning, teaching and learning process management, learning and teaching information inquiry, and early warning. The intelligent management process with the theme of teacher-student communication, teaching evaluation, learning test, and information tracking is shown in Figure 3.

The mechanism of smart management is to read and write information through RFID sensor chips, then exchange information with information database through reader, and finally query, release, and present information and management through the IOT “PC management terminal” for smart education. We use sensors, RFID, and Zigbee to integrate teachers, teaching, evaluation, communication, students, learning, testing, tracking, and other information to a card or a smart bracelet for smart management. At present, the common management functions of IoT for smart education include the following: location management, access management, dormitory management, attendance management, and meeting management, etc.

2.3.3. Emotional Computing. Emotional computing collects data and extracts information through high-precision sensor interfaces, performs emotion computing based on the information (including face emotion recognition, gesture action recognition, human posture recognition, voice emotion recognition, smell emotion recognition, and touch emotion recognition of students in universal learning activities), and finally provides emotion computing information to the intelligent education service platform. The platform is established with students’ expression database, posture database, subject knowledge database, subject test database, students’ knowledge level database, and students’ knowledge structure database. Through intelligent emotion computing and emotion-aware computing, it realizes emotional interaction and personalized homework. Emotion computing for intelligent education IoT includes emotion computing of sensory channel and emotion computing of the text channel.

2.3.4. Equipment Sharing. With big data as the core, mobile Internet as the nerve network, education sensing network as the nerve endings, adaptive and personalized user interaction as the means, and smart education application services

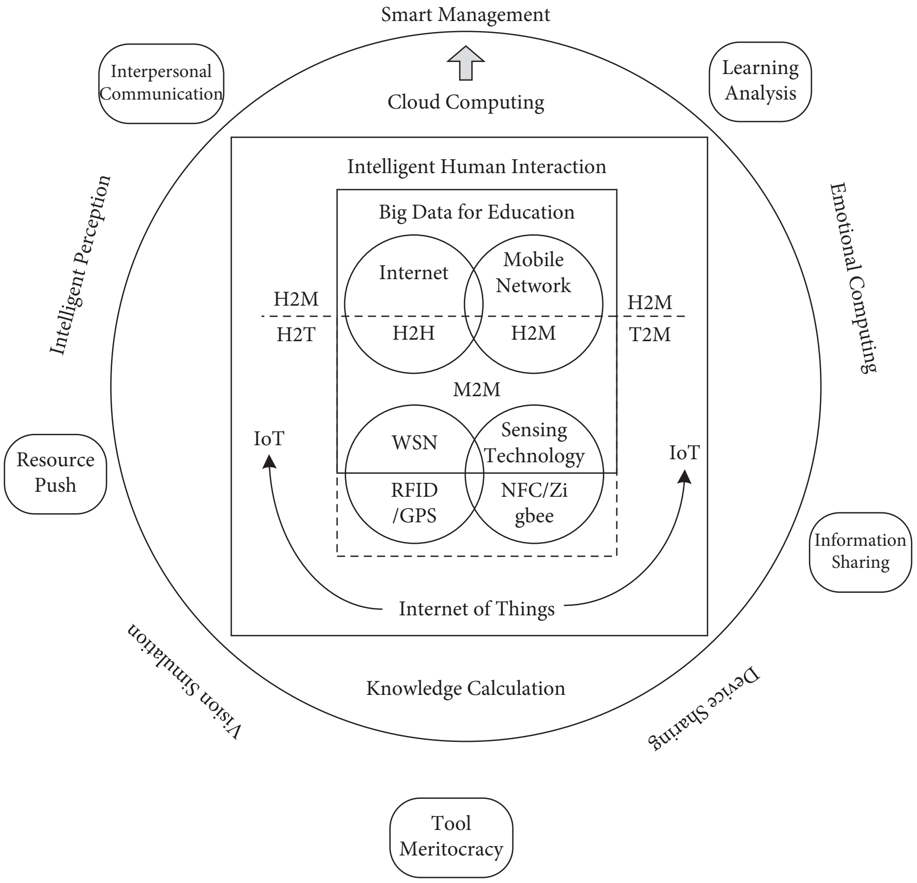

Figure 2: Smart education IoT functional architecture model.

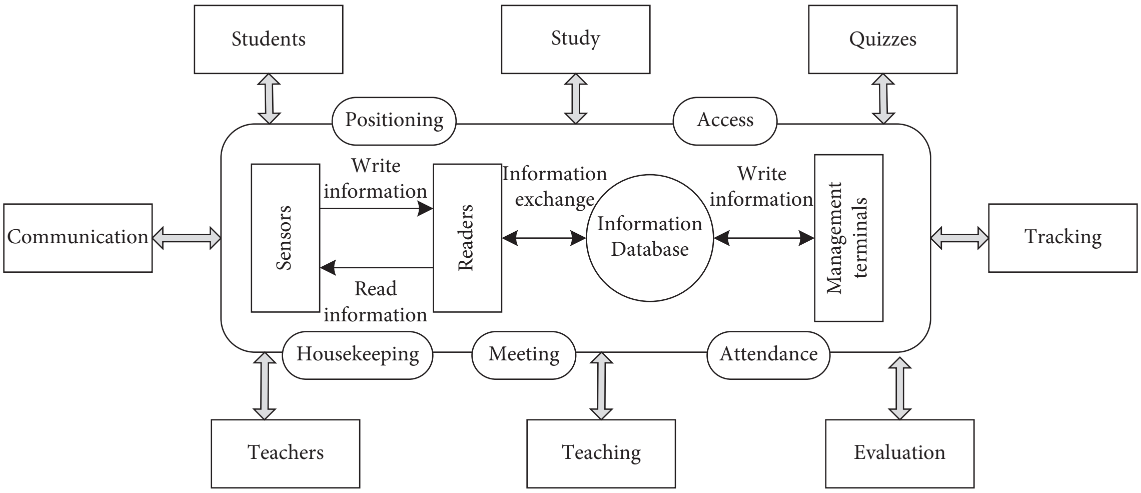

Figure 3: Intelligent management process.

as the goal, device data computing completes the transmission, analysis, storage, and display of its information.

3. Methodology

With the massive amount of data and information carried by the Internet of Things for smart education, coupled with its open architecture, there are undoubtedly potential new security and privacy issues in addition to the security issues of traditional networks. Issues such as data confidentiality for perceptual interactions with students and the inability to identify and track without authorization are particularly salient in education. Illegal users may forge RFID tags to send information to readers, resulting in confusion in the processing of school information systems and posing a serious threat to the information security of teachers and students. Therefore, the smart education data center server in the background must maintain a strict ban on unauthorized access routes and must prevent illegal access and tampering of information to avoid illegal profitability of educational information or loss of data information.

3.1. Decentralized Ciphertext Data Secure Sharing Framework. For the security and privacy issues of smart education IoT, this paper proposes a decentralized data security framework.

To address the needs of decentralized data sharing, resistance to user attribute forgery and tampering attacks, frequent state changes in smart education environments, and to achieve secure sharing effects without trusted third parties and with low node computation, this paper constructs a decentralized cryptographic data sharing framework for smart education models based on federal blockchain, CP-ABE, and outsourced decryption. The details are shown in Figure 4. The framework shown in Figure 4 contains three entities, namely, data owners (DO), data user (DU), attribute authorities (AAs), and the identity-attribute chain (IAC) with the file block (FIC).

3.1.1. Property Authority. AAs are groups of nodes that make up the blockchain network and are also participants and maintainers of the federated chain, consisting of a set of high-performance servers.

$$AAs = \{\text{Server}_x | 4 \le x \le t\}, \quad (1)$$

where t is the number of servers. AAs are responsible for managing user attributes and forwarding data between users and the smart contracts deployed locally on them.

AAs assign the corresponding attributes according to the user's identity and calculate and distribute the attribute private keys through smart contracts to record the identity and attributes in the form of transactions on the IAC. In addition, AAs integrate the user's uploaded file information and file key cipher text through smart contracts to form transactions for uploading to FIC.

3.1.2. Data Owners (DO). DO is the data provider and has the control of the data. DO makes the access policy N for the files. DOs can access the data when the attribute set S satisfies $N_i(S) = 1$. DO is a set of smart devices that share data in the smart home. DO has limited computing and storage capacity. DO can encrypt the shared files and upload them to the cloud storage system. Considering the mobility of smart devices, DO can dynamically join or exit the access control system.

3.1.3. Data Users (DU). DU is a data consumer and obtains the corresponding file by initiating a data access request. DU owns the attribute set S. In practice, both DO and DU are possible in an IoT model.

3.1.4. Identity Attribute Chain (IAC). Each transaction on the IAC corresponds to a set of user's identity attribute pairs.

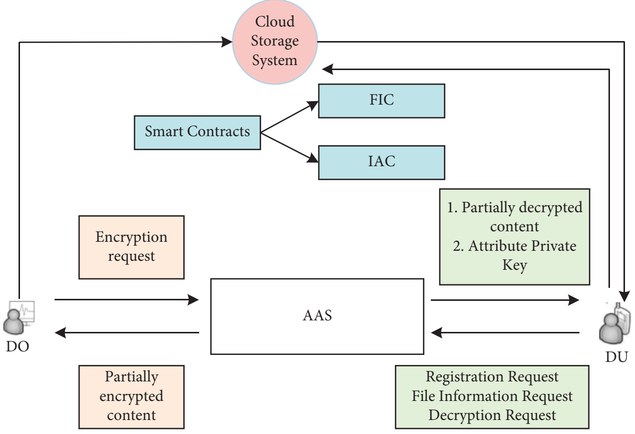

Figure 4: Decentralized ciphertext data secure sharing framework.

The federation chain uses a node access management mechanism and the feature that only smart contracts can access the identity attribute pair information to effectively protect user privacy. In this framework, each new member needs to register with AAs to get its own attribute private key. The registration process is done autonomously by AAs invoking a smart contract, which constructs a transaction to record the user's identity, attribute set, and other information and stores it on the IAC after encryption.

In addition to some information such as the generic transaction ID, signature key, etc., the transaction information on the IAC block contains the following.

(1) Device identifier (DID, device identity): $I\ D = \{0, 1\}^{16}$, a unique identifier for each user.

(2) Attribute set (ATTRS, attribute set): the set of attributes corresponding to the user's identity, ATTRS ⊆ S. When ATTRS changes, the user's access rights also change.

3.1.5. File Information Chain (FIC). FIC maintains the meta-information about the user's uploaded files $\text{File Info} = \{\text{FileAddr}, \text{Keywords}, \text{hash}, CN_Z\}$.

In addition to some information such as the generic transaction ID and signature key, the transaction information on the FIC contains the following.

FileAddr: The address of the file on the cloud storage system. The user requests the corresponding encrypted file based on this address.

A collection of document keywords, which is used to quickly retrieve and match user request documents. Keywords = {Keyword1, Keyword2, ...}.

hash: hash of the encrypted file, which is used to ensure the integrity of the file and avoid missing data due to the network. hash = SHA256 (digest(file)).

CN_Z: the ciphertext of the symmetric encryption key Z used by the user to encrypt the file.

3.2. Multistage Decentralized Ciphertext Data Security Protection. The blockchain-based decentralized ciphertext data secure sharing method supports blockchain to record user attributes, ensures data confidentiality and integrity, and improves the efficiency of data sharing. In order to better describe the proposed method, the conventional encryption and decryption operations involved are defined.

Definition 1. Encopt (•), where opt ∈ {AES, PPK}. AES denotes the symmetric encryption AES (advanced encryption standard) algorithm and PPK denotes the execution of the RSA encryption algorithm using the public key PPK.

Definition 2. Decopt (•), where opt ∈ {AES, PSK}. PSK denotes the execution of the RSA decryption algorithm using the private key PSK.

The proposed method consists of four phases: setup phase, register phase, upload phase, and secure sharing phase.

3.2.1. Setup Phase. The initialization process is mainly completed to deploy smart contracts and generate system master key pairs. The initialization and registration process is shown in Figure 5.

In the initialization phase, first the smart contracts SC_{XG}, SC_{FX} on AAs, subsequently SC_{XG} constructs the bilinear cyclic group A_0 of order prime p and its generating element g and the bilinear pair mapping e: $A_0 * A_0 \longrightarrow A_1$ with randomly chosen $g, h \in K_u$ and computes

$$b = a^{h}, \tag{2}$$

$$e(a,a)^{g}. \tag{3}$$

The master key pair $(MSK = \{h, a^{g}\}, PK = \{A_0, a, b, e(a,a)^{g}\})$is generated. MSK is the system master key and PK is the system public key.

3.2.2. Register Phase. When a new user joins the system, it first sends a registration request to the AAs with its device identifier DID, and the AAs verify the user's identity based on the DID. The AAs assign the corresponding attribute set S and public-private key pair < PPK, PSK > to the user and forward < DID, S > to the smart contract SC_{XG}, which selects a random number $r \in K_u$ and calculates

$$SZ_r = a^{g+r/h}. \tag{4}$$

For each attribute y within S, choose a random number $r_y \in K_u$ and compute

$$SZ_s = \left\{\forall y \in S, D_y = a^{r} \cdot B(y)^{r_y}, D'_y = a^{r_y}\right\}. \tag{5}$$

The attribute private key $SK = \{SZ_r, SZ_s\}$ is obtained. Finally, SC_{XG} returns < SK, PPK, PSK > to the user via AAs and uploads < DID, S > to IAC in the form of transactions.

3.2.3. Upload Phase. Data sharing is the process of user uploading data. In this phase, DO first selects the key Z, calculates $C_f = Enc_{AES}(Z, \text{file})$, and uploads C_f to IPFS. Subsequently, DO encrypts Z to get CN_Z.

DO choose a random number $s \in K_u$ and compute

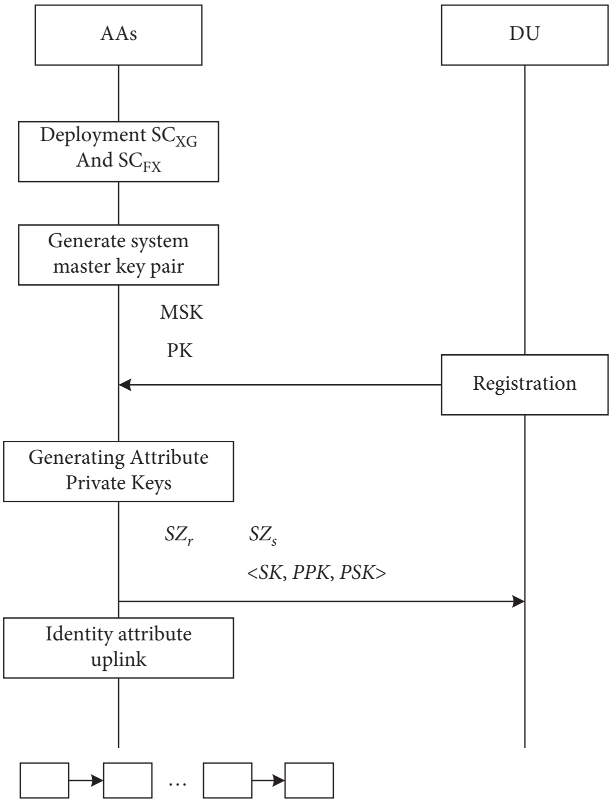
AAs
DU
Deployment SC_{XG} And SC_{FX}
Generate system master key pair
MSK
PK
Registration
Generating Attribute Private Keys
SZ_r
SZ_s
<SK, PPK, PSK>
Identity attribute uplink
...

Figure 5: System initialization and user registration process.

$$\tilde{C} = Ze(a,a)^{gs}, \tag{6}$$

$$\begin{aligned} C &= b^{s}, \\ CN_g &= \left\{\tilde{C}, C\right\}. \end{aligned} \tag{7}$$

At the set J of leaf nodes of N, compute for $\forall j \in J$

$$\begin{aligned} C_j &= a^{v_j(0)}, \\ C'_j &= B(\text{attr}(j))^{v_j(0)}, \end{aligned} \tag{8}$$

where attr (j) means to obtain the attribute corresponding to j. Let $CN_s = \left\{C_j, C'_j\right\}$, DO generates the ciphertext $CN_Z = \left\{CN_g, CN_s\right\}$, and the file information FileInfo, where FilEInfo = {FileAddr, Keywords, hash, CN_Z}.

In the calculation of CN_s, $v_i(\cdot)$ is constructed as follows.

(1) Starting from the root node R, choose a polynomial $v_i(\cdot)$ from top down for each node i of N. The number of times d_i of $v_i(\cdot)$ is 1 smaller than its threshold value z_i, i.e., $d_i = z_i - 1$.

(2) Starting from the root node R, choose a random number, $v_R(0) = S$, and randomly choose d_R points of $v_R(\cdot)$ to perfect $\delta v_R(\cdot)$.

(3) For other nodes i, let $v_i(0) = v_{\text{parent}(i)}(\text{index}(i))$ and randomly choose d_i points to perfect $v_i(\cdot)$.

Finally, DO signs the FileInfo and forwards < FileInfo, δ DO (FileInfo) > to SC_{XG} via AAs. SC_{FX} verifies the signature and uploads the FileInfo to FIC.

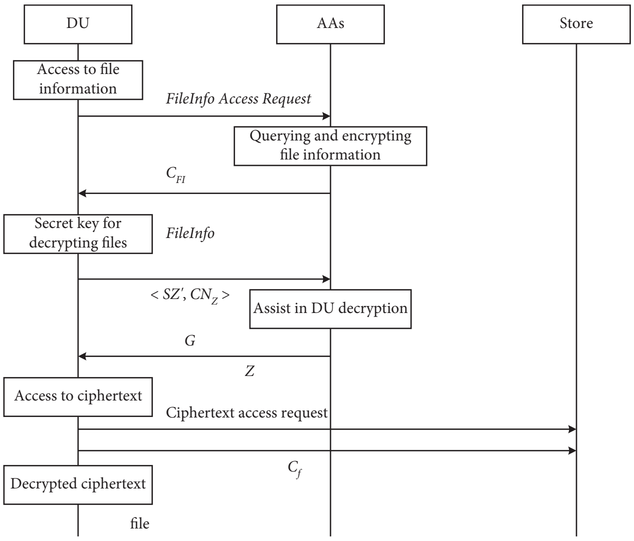

FIGURE 6: Secure sharing process.

3.2.4. Secure Sharing Phase. Secure sharing is the process of user access to data, the flow is as shown in Figure 6. In this phase, DU initiates access request < DID, Keywords > to the contract through the attribute server cluster AAs. The SC_{XG} determines whether the user is registered according to the DID. the SC_{FX} gets the corresponding FileInfo according to the Keywords, calculates $C_{FI} = Enc\,(\text{File Info})$, and returns it to DU.

DU downloads C_f via FileAddr and obtains FileInfo. To recover Z, DU chooses a random number $n \in K_u$ and converts the attribute private key

$$SZ' = \left\{SZ_g^n, SZ_s\right\}. \tag{9}$$

Send < SZ', CN_Z > to AAs.

AAs act as a decryption outsourcing server provider (DSP) to perform decryption calculations for each leaf node i in N

$$\text{Decrypt Leaf}\left(CN_Z, SZ', i\right) = e\,(a, a)^{rv_i(0)}. \tag{10}$$

Then, the result is returned to DU.

$$\begin{aligned} Z &= \frac{\widetilde{C}}{e\left(C, {D'}^{1/n}\right)/G} \\ &= \frac{\widetilde{C}}{e\left(b^s, a^{g+r/h}\right)/e\,(a, a)^{rs}}, \end{aligned} \tag{11}$$

where $G = e\,(a, a)^{rv}\,(0) = e\,(a, a)^{rs}$and $D' = SZ_r^n$.

Finally, DU obtains the plain text of the file.

$\text{Decrypt Leaf}\,(CN_{Z'}SZ', i)$ is computed as follows: for each node i in N, if i is a leaf node, let $x = \text{attr}\,(i)$, then when $x \in S$

$$\begin{aligned} \text{Decrypt Leaf} &= \frac{e\,(D_x, C_i)}{e\,(D_x', C_i')} = \frac{e\left(a^r \cdot B\,(x)^{r_x}, b^{v_i(0)}\right)}{e\left(a^{r_x, B\,(x)^{v_i}\,(0)}\right)}, \\ &= e\,(a, a)^{rv_i(0)}. \end{aligned} \tag{12}$$

If i is a nonleaf node, compute $F_k = \text{Decrypt Leaf}\,(N_Z, SZ', k)$ for all subnodes k of i.

Let S_i be the set of subnodes of x and S_i of size z_i with $F_k \neq \perp$. If S_i does not exist, the function returns $\perp$.

4. Result Analysis and Discussion

In this paper, experiments are conducted on the basis of PBC library and CP-ABE base development kit using an elliptic curve as $y^2 = x^3 + x$. The experimental environment is a dual-core CPU with 4.0 GHz, 64 GB RAM, and Ubuntu 18.04 64 bit operating system. In addition, AAs are used as blockchain nodes to build a blockchain network based on the Hyperledger-Fabric system with the use of the Byzantine fault-tolerant consensus mechanism. The simulation parameters for IoT are set as shown in Table 1.

4.1. Security Analysis. This section mainly analyzes the security of the proposed scheme in terms of data confidentiality, data integrity, complicity attacks, and attribute tampering and impersonation attacks, and finally compares it with other schemes as shown in Table 2.

It can be seen that the performance of this paper's scheme outperforms other schemes in several aspects such as data confidentiality, data integrity, complicity attacks, and attribute tampering and impersonation attacks, indicating the effectiveness of this paper's scheme. This is because literature [20, 22] have no AA to manage user attributes and lack protection against user attribute tampering and impersonation attacks. Literature [21] is based on a traditional trusted third-party AA server. Its security threshold against attribute impersonation attacks is 100%, but it is powerless against user attribute tampering attacks. Literature [23] is weak against attribute impersonation attacks. Literature [24] has a security threshold of 75% against attribute tampering attacks but is unable to resist attribute impersonation attacks due to the absence of attribute management features. It shows that the model security scheme in this paper can improve the security of data access and provide a reliable guarantee for secure data sharing under smart education.

4.2. Performance Analysis. The experimental performance is evaluated in terms of user encryption and decryption and the total overhead time of the scheme for comparison, and the experiments are conducted using a gradual increase in the number of policy attributes.

As can be seen from Figure 7 to 9, with the increase in the number of access policies or attributes, the time overhead on all aspects of the proposed scheme in this paper is significantly reduced compared to the blockchain trusted data sharing based scheme [23] and the CP-ABE based blockchain data access control scheme [20]. It can be seen that, in comparison with the distributed computing-based data sharing scheme, the scheme proposed in this paper effectively reduces the computation and time cost of the sharing process while ensuring the security of all aspects of data sharing. Compared with blockchain-based onboard data sharing schemes using CSP proxy computing [21, 22], the

Table 1: Simulation parameter settings.

Parameters	Settings
Simulation area	1,000 m × 1,000 m
Number of users	50
Number of educational IoT devices	50
Number of trusted institutions	1
Number of cloud servers	2
Number of gateways	2

Table 2: Safety comparison.

Programs	Data confidentiality protection	Anti-conspiracy attack	Anti-attribute tampering attack	Data integrity protection	Anti-attribute counterfeit attack
[20]	✓	✓	×	✓	✓
[21]	✓	✓	×	✓	✓
[22]	✓	✓	×	✓	✓
[23]	✓	✓	✓	✓	×
[24]	✓	✓	×	✓	×
Proposed	✓	✓	✓	✓	✓

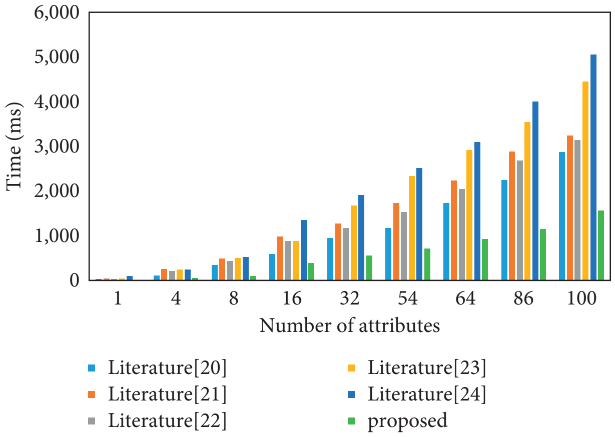

Figure 7: User encryption time.

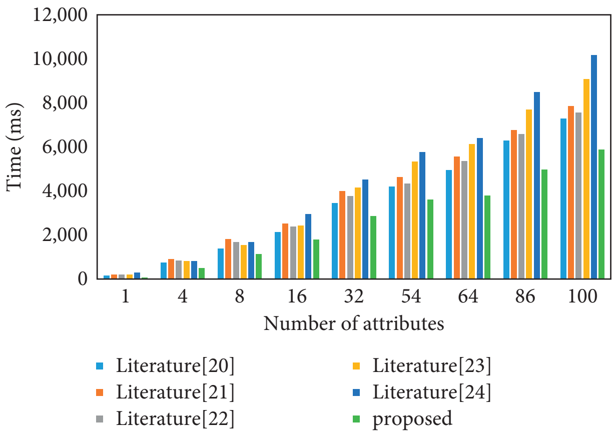

Figure 9: Shared program time.

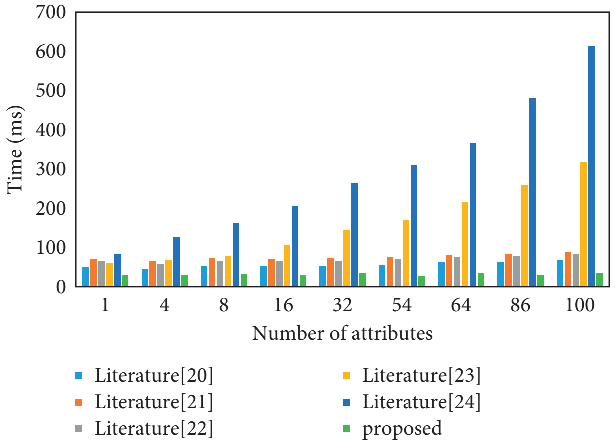

Figure 8: User decryption time.

scheme proposed in this paper reduces user decryption time delay based on outsourced decryption technology, which can effectively resist the threat of data leakage due to attribute tampering by users and malicious users stealing CSP attribute private keys while ensuring data sharing efficiency. Compared with the blockchain-based trusted data sharing scheme [23] and the CP-ABE-based blockchain data access control scheme [24], the scheme proposed in this paper achieves better security against user attribute counterfeiting and tampering, etc., and improves the reliability of data sharing while reducing the time overhead of data sharing.

In addition, literature [24] has the computational overhead of user access to the network since the user is used as a blockchain network node, which first needs to access the blockchain network for the user with the deployment of smart contracts before the access control occurs.

The proposed scheme uses AAs as blockchain network nodes and users only need to interact with AAs without becoming blockchain system nodes, thus reducing the overall latency of the scheme and improving the efficiency of data sharing in the smart education environment. Therefore, the author's proposed scheme effectively improves the efficiency in the smart education environment while ensuring security.

5. Conclusion

With the arrival of 5G era and the rapid advancement of education informatization 2.0, the development and application of smart education IoT for the integration of multimedia education resources has attracted great attention from the education community at home and abroad, and smart education will become the main development direction of future education. In this paper, the evolution model and functional architecture model of smart education IoT are constructed and the path of functional realization of smart education IoT is given. In the IoT model, a decentralized ciphertext data security sharing scheme based on multistage technology is designed. The security model and scheme ensure the confidentiality and integrity of data and improve the efficiency of data sharing. The experimental and analytical results illustrate that the security model in this paper can meet the requirements of secure data sharing in the smart education environment. The future work is to improve the encryption methods in the security model to further enhance the efficiency of security protection.

Data Availability

The labeled datasets used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by Jilin Province Higher Education Association Higher Education Research Project "Research on the Practice Path of Internet Culture to Enhance College Students' Values" (No. JGJX2021B28).

References

[1] D. Xia, "English multimedia teaching resources integration system based on big data technology," in *Proceedings of the 2020 International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, pp. 22–25, Ottawa, ON, Canada, October 2020.

[2] W. Fu, "The Integration Mechanism of Multimedia Computer Technology and College English Education," *ACM*, in *Proceedings of the 2021 2nd International Conference on Computers, Information Processing and Advanced Education*, pp. 1165–1169, Ottawa, ON, Canada, May 2021.

[3] J. Leem and E. Sung, "Teachers' beliefs and technology acceptance concerning smart mobile devices for SMART education in South Korea," *British Journal of Educational Technology*, vol. 50, no. 2, pp. 601–613, 2019.

[4] H. Singh and S. J. Miah, "Smart education literature: a theoretical analysis," *Education and Information Technologies*, vol. 25, no. 4, pp. 3299–3328, 2020.

[5] N.-S. Chen, C. Yin, P. Isaias, and J. Psotka, "Educational big data: extracting meaning from data for smart education," *Interactive Learning Environments*, vol. 28, no. 2, pp. 142–147, 2020.

[6] A. Z. Faroukhi, I. El Alaoui, Y. Gahi, and A. Amine, "Big data monetization throughout big data value chain: a comprehensive review," *Journal of Big Data*, vol. 7, no. 1, pp. 1–22, 2020.

[7] M. Mohammed Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. Mikaeel Ahmed, A. Saifullah Sami, and R. R. Zebari, "IoT and cloud computing issues, challenges and opportunities: a review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, 2021.

[8] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[9] A. Khanna and S. Kaur, "Internet of things (IoT), applications and challenges: a comprehensive review," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1687–1762, 2020.

[10] M. Kassab, J. DeFranco, and P. Laplante, "A systematic literature review on Internet of things in education: benefits and challenges," *Journal of Computer Assisted Learning*, vol. 36, no. 2, pp. 115–127, 2020.

[11] D. K. A. R. Al-Malah, H. H. K. Jinah, and H. T. S. ALRikabi, "Enhancement of educational services by using the internet of things applications for talent and intelligent schools," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 4, pp. 2358–2366, 2020.

[12] M. K. Saini and N. Goel, "How smart are smart classrooms? A review of smart classroom technologies," *ACM Computing Surveys*, vol. 52, no. 6, pp. 1–28, 2019.

[13] D. Sulistiyarini and F. Sabirin, "21st century literacy skill of information technology and computer education students," *JPI (Jurnal Pendidikan Indonesia)*, vol. 9, no. 4, pp. 576–585, 2020.

[14] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: a survey," *Information Security Journal: A Global Perspective*, vol. 30, no. 2, pp. 63–87, 2021.

[15] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: a hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE)," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8–16, 2020.

[16] A. Javadpour, G. Wang, and S. Rezaei, "Resource management in a peer to peer cloud network for IoT," *Wireless Personal Communications*, vol. 115, no. 3, pp. 2471–2488, 2020.

[17] A. W. Malik, T. Qayyum, A. U. Rahman, M. A. Khan, O. Khalid, and S. U. Khan, "XFogSim: a distributed fog resource management framework for sustainable IoT services," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 4, pp. 691–702, 2020.

[18] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in

Internet of Things," *Neural Computing & Applications*, vol. 32, no. 15, pp. 10979–10993, 2020.

[19] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: blockchain-aided searchable attribute-based encryption for cloud-IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7851–7867, 2020.

[20] Y. Qiu, H. Zhang, Q. Cao, Z. Jiancong, C. Xingshu, and J. Hongjian, "Blockchain data access control scheme based on CP-ABE algorithm," *Chinese Journal of Network and Information Security*, vol. 6, no. 3, pp. 88–98, 2020.

[21] K. Fan, Q. Pan, K. Zhang et al., "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5826–5835, 2020.

[22] S. Niu, P. Yang, Y. Xie, and D. U. Xiaoni, "Cloud-assisted ciphertext policy attribute based eencryption data sharing encryption scheme based on BlockChain," *Journal of Electronics and Information Technology*, vol. 43, no. 7, pp. 1864–1871, 2021.

[23] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in Multiple clouds," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1229–1241, 2020.

[24] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, "TrustAccess: a trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.