Construction of a Secure Sharing Model for Digital Educational Resources Using Blockchain and Cipher Policy Attribute Based Encryption in Smart Education

Wenxiao Lu*
Heilongjiang Institute of Teacher Development, Harbin 150080, China
*E-mail: zl17758888702@163.com

Keywords: smart education, blockchain, attribute-based encryption, ciphertext policy, digital educational resources, secure sharing model

Received: July 10, 2024

As the rapid advancement of information technology, the importance of digital educational resources in the field of education has become increasingly prominent. However, traditional access control techniques can hardly meet the demand for fine-grained sharing of digital educational resources in complex educational environments. Therefore, the study adopts attribute-based encryption based on ciphertext policy and combines it with the decentralised and tamper-proof features of blockchain to design a secure sharing model combining blockchain technology and attribute-based encryption algorithms to achieve secure and precisely controlled sharing of digital educational resources. The outcomes denote that the average encryption and decryption time of the designed model were 1.66 s and 1.65 s, respectively. Compared with attribute based key policy encryption and policy based attribute based encryption, the average encryption time was reduced by 0.65 s and 2.61 s, respectively, and the average decryption time was reduced by 0.69 s and 2.04 s, respectively, proving that it is more efficient in processing tasks. The ciphertext upload time of the design model remains constant at 9.2 ms, proving that it can scale better to more users without increasing the latency. Meanwhile, as the amount of attributes increases, the design model is able to keep the ciphertext length small, proving that it can effectively reduce the storage space requirement and raise the overall efficiency of the system. The model provides a powerful solution to the data sharing problem in smart education, as well as a reference for other domains that require secure data sharing.

Povzetek: Predlagan je varni model za deljenje digitalnih izobraževalnih virov, ki združuje tehnologijo blockchain in šifriranje na osnovi atributov s politiko šifriranja. Model zagotavlja decentralizirano in fino nadzorovano deljenje, povečuje učinkovitost in zmanjšuje zahteve za shranjevanje, kar omogoča varno upravljanje virov v pametnem izobraževanju.

1 Introduction

In the tide of global education informatisation, digital education resources have become an important pillar of the smart education system. With their richness, diversity and convenience, these resources have revolutionised the traditional education model. Students and teachers are able to cross the boundaries of time and space to achieve instant access to knowledge and interactive sharing [1]. Students have properly incorporated mobile devices and applications into their daily lives and use mobile apps for personal, social, and academic activities on varying scales [2]. However, with the explosive growth of data volume, the problem of resource management and secure sharing in education has become increasingly prominent. How to realize efficient use of resources while safeguarding data privacy and intellectual property rights has become a bottleneck restricting the growth of smart education. Educational organisations need to ensure that sensitive information is not subject to unauthorised access, while also preventing illegal copying and distribution of educational content to safeguard the interests of content providers and learners [3]. In addition, the sharing mechanism of educational resources (ER) needs to meet the needs of personalisation and dynamic adjustment to accommodate the trend of diversification and individualisation in education [4]. The traditional centralised management model is difficult to adapt to these needs, and the introduction of blockchain technology offers a new solution to this challenge. The core advantages of blockchain technology are its decentralisation, transparency and security. It is able to provide tamper-proof records for the storage of ER and achieve traceability of information through distributed ledger technology. The application of Attribute-based encryption (ABE) algorithm can provide a more fine-grained and flexible control mechanism for accessing resources. In view of this, the research combines the ABE algorithm with blockchain and introduces ciphertext policy into the ABE algorithm to design a secure sharing model for digital ER that combines blockchain and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The innovation of this model is that it combines the untamperable and decentralised characteristics of blockchain with the fine-grained encryption strategy of CP-ABE algorithm, thus tapping the new potential of

smart education data management while guaranteeing the secure sharing of ER. The model can raise the sustainable development of smart education and provide a reference for similar challenges faced by other fields. The study consists of five parts. The first part is a background introduction to digital ER, blockchain and ABE algorithm. The second part is a review of the current research status in the field of secure and safe sharing of digital ER at home and abroad. The third part is the design of the secure sharing model combining blockchain and CP-ABE algorithm. The fourth part is the performance analysis of the designed secure sharing model and the analysis of the practical application effect. The fifth part is the summary of the research outcomes and points out the shortcomings of the research.

2 Related works

With the development of smart education, digital ER have become a critical part of modern education. However, unauthorised access, data leakage and intellectual property infringement pose significant threats to the educational ecosystem. To address these problems, scholars have proposed many solutions. Liang and other researchers designed a fast detection algorithm with deep reinforcement learning for the copyright protection of intellectual property rights, which uses a deep Q-learning algorithm to generate watermarked locations so that they are safe and close to the original design, and an artificial neural network algorithm to train feature vectors speed [5]. Li et al. designed a blockchain federation based data security storage and sharing scheme for privacy protection and efficient transmission in student education record data storage and sharing, which uses blockchain and storage server to complete the data security storage together, and the outcomes denote that the scheme has good robustness [6]. Gajendran designed a blockchain-based e-learning data environment for the security problem of e-learning data environment, and the outcomes denote that the algorithm can effectively raise the detection speed. A blockchain-based e-learning framework, which uses blockchain technology to ensure the integrity of e-learning data and prevent tampering and protect learners' privacy, and the outcomes denote that the framework can provide a fair and open online education environment [7]. Sharma and other scholars have designed an efficient and secure peer-to-peer distributed IoT network model based on blockchain to achieve secure data sharing in IoT systems. In this model, untrusted devices can use blockchain to interact with other devices in automatic verification mode without the need for trusted intermediaries. The results show that compared with other encryption methods, the hash output of this model changes significantly [8]. Eunaicy and other researchers, in order to provide an easy-to-use, secure and anonymous access environment to the ER, design a semantic web-based e-learning content retrieval system, which is based on the use of semantic words and user query to generate a resource description framework, the outcomes denote the novelty and applicability of the system [9].

Zhang et al. designed a data security sharing method based on CP-ABE and blockchain to enhance the security of data trading platforms. The method protects the privacy information of access policies by designing appropriate ciphertext and key structures and constructing an efficient and flexible multi authorization center access control scheme that supports policy hiding. The results show that the method has good performance [10]. Irshad et al. designed a blockchain-based system, Block-ED, which applies blockchain technology to provide credibility to the creators of resources and prevent unauthorised operations or changes, and the outcomes denote that the system can effectively manage ER. They designed a blockchain-based system, Block-ED, which uses blockchain technology to provide credibility to the creators of resources and prevent unauthorised operations or changes, and the outcomes denote that the system can effectively manage ER [11]. Xue and other researchers designed a blockchain-based smart education platform to ensure the authenticity and trustworthiness of identities, which protects the copyrights of resources through the invariance and high transparency of blockchain, and protects the copyrights of resources through the invariance and high transparency of blockchain, and the system can maintain high performance. Transparency, protects the copyright of resources, and establishes a mechanism for knowledge currency and credit conversion, and the outcomes denote that the platform can effectively protect ER [12]. Bathula et al. propose a signature-based Rivest Shamir framework for improving data sharing between students and teachers in the educational system, and estimate the possible harmful attacks on data transmission through the designed framework. The outcomes denote its high performance in its in protecting data security and improving efficiency [13]. Chen and other researchers to address the current web resource sharing model, designed a semantic web-based online digital educational resource sharing model, which takes XML as the basic syntax, and creates relevant applications based on XML according to the specifics of the application of the teaching resources, and the outcomes denote that the model The usage rate of ER is high [14].

In summary, many researchers have made significant contributions to ensuring the security of digital ER and improving the performance and stability of educational resource sharing. However, these methods face problems such as high complexity and high implementation cost. Therefore, the research combines blockchain with ABE algorithm and introduces a ciphertext policy based on ABE algorithm to design a blockchain data access control model with CP-ABE algorithm in order to enhance the overall performance of the system and the user interaction experience as well as to reduce the cost of deployment and maintenance. The specific content of the existing models mentioned above and the proposed model's improvements to the limitations of the existing models are shown in Table 1.

Table 1: Specific content of existing models and proposed improvements to the limitations of existing models

Existing models	Key features	Method	Result	Boundedness	Improvement of the proposed model
[5]	Intellectual Property Protection	Deep reinforcement learning	Improve detection speed	High algorithm complexity and high implementation cost	Introducing CP-ABE algorithm to simplify copyright protection process
[6]	Data security storage and sharing	Blockchain alliance	Enhanced robustness	Limited scalability	Improved the scalability of the system
[7]	Electronic Learning Data Security	Blockchain framework	Integrity and tamper proof	High implementation cost	Reduced deployment and maintenance costs
[8]	IoT data security sharing	Efficient and secure peer-to-peer distributed IoT network model based on blockchain technology	Significant changes in hash output	Its application scope is mainly limited to the Internet of Things	Applicable to a wider range of educational fields
[9]	Educational resource access environment	Semantic network retrieval system	Usability, security, and anonymity	Possible lack of fine-grained access control	Provide fine-grained access control
[10]	Data security sharing	Data security sharing method based on CP-ABE and blockchain	Support policy hiding for multi authorization center access control	High complexity	Simplified the management of multiple authorization centers
[11]	Educational Resources Management	Blockchain System Block ED	Fair management of resources and prevention of unauthorized operations	There may be user experience barriers	Improved user experience
[12]	Identity authenticity and credibility	Blockchain Education Platform	Protect copyright and establish a credit conversion mechanism	Lack of low latency characteristics	Improved the response speed of the system
[13]	Data sharing	Signed Rivest Shamir framework	Data security and efficiency	High technical complexity	Simplified the technical implementation process
[14]	Network resource sharing	Semantic Web Model	High utilization rate of teaching resources	Difficult to implement	Reduced implementation difficulty

3 Secure sharing model for digital educational resources combining blockchain and ABE algorithms

As the wide usage of information technology in education, a large amount of digital ER have been generated. However, the traditional centralised architecture is difficult to meet the demand for secure sharing of these resources. Therefore, the research constructs a secure sharing model of digital ER combining blockchain and ABE algorithm to address the security issue in the sharing process.

3.1 Construction of a safe sharing model for digital educational resources

In the digital information age, with the increasing abundance of ER, data security and privacy protection have become key issues in the design of information systems [15, 16]. Especially in the field of education, the diversity and individuality of the needs of teachers, students, researchers and other users require that the educational resource management system must have highly flexible and precise access control capabilities [17]. Therefore, in order to achieve efficient sharing of ER under the premise of privacy protection, the research combines blockchain and ABE algorithm to construct a digital educational resource sharing model, and the overall system framework of this model is denoted in Figure 1.

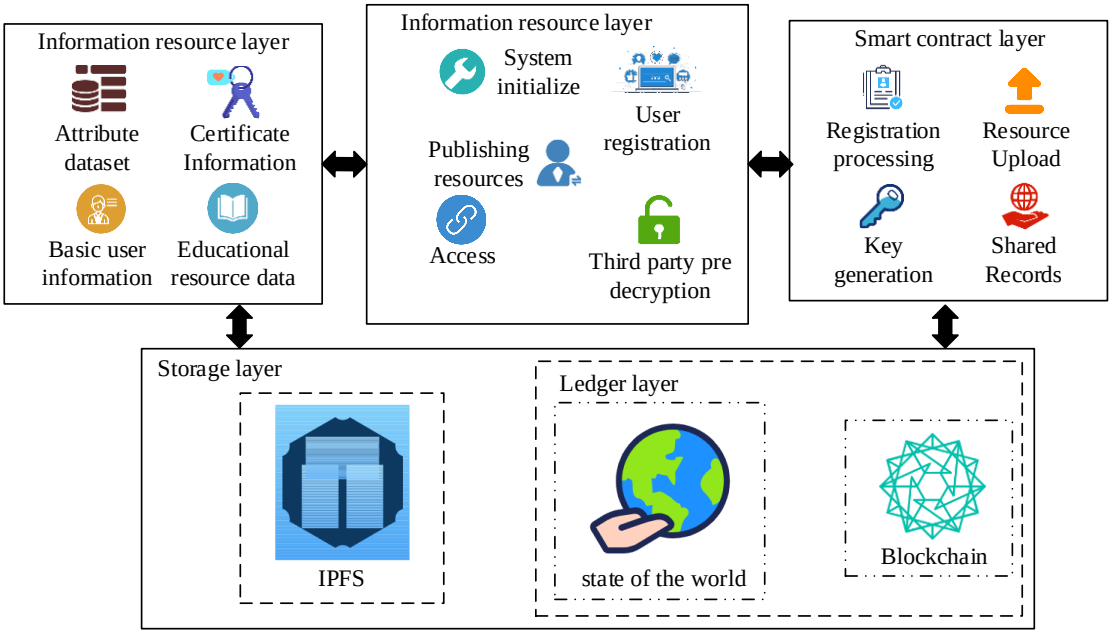


Figure 1: Model system framework

The model integrates blockchain technology and ABE algorithms to form a multi-layered architecture, including an information resource layer, an information processing layer, a smart contract layer, and a storage layer. Among them, the information resource layer is responsible for managing and categorising educational resource data, including text, video, test banks and other educational materials in various formats. The information processing layer handles the distribution logic of resources and is responsible for handling user requests and application logic. It is an intermediary for user-system interaction, converting user requirements to serve the system. The smart contract layer uses blockchain technology to automatically execute complex business rules, such as resource copyright management and allocation of usage rights, through smart contracts to ensure the transparency and non-tampering of business logic. The storage layer is responsible for the long-term storage of data, ensuring data integrity and reliability. It usually includes a database management system that uses encryption to protect stored data from unauthorised access. The specific structure of the model is denoted in Figure 2.

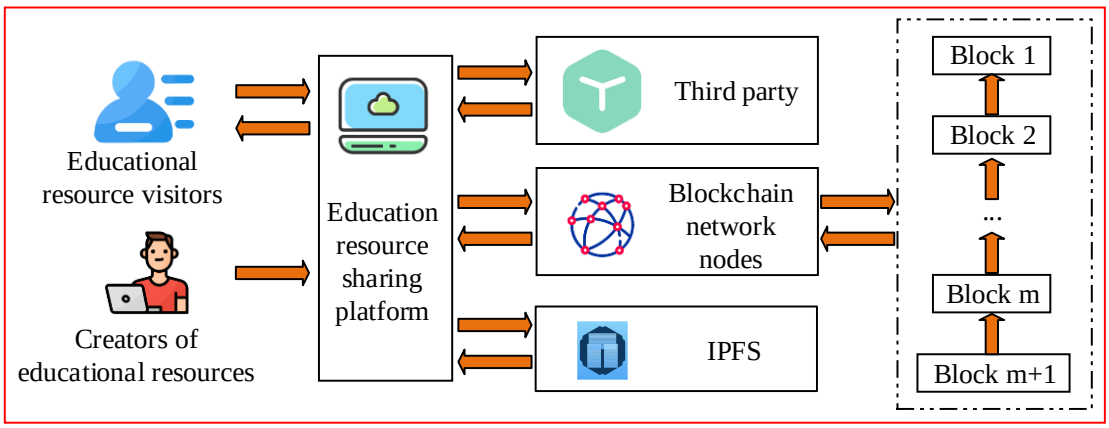


Figure 2: The specific structure of the model

Before a user can start using the platform, he or she must complete the registration process. During this process, the user is required to submit a set of attributes to the authorisation centre, which include the user's identity information, organisational affiliation; role responsibilities; etc. The authorisation centre is responsible for verifying the authenticity and validity of these attributes. After verification, the authorisation centre generates corresponding attribute keys based on the user's set of attributes and distributes these keys securely to the user, and these attribute keys will be utilized to identify the user's access rights when he/she accesses the protected resources. The creator of an educational resource needs to undergo a registration process similar to that of a regular user to obtain his/her unique attribute key before publishing the resource. After that, the creator will define an access policy for the resource. This policy is a set of rules stating which user attributes can access the resource. The creator will use the ABE algorithm to encrypt the resource based on the defined access policy. After completing the encryption, the creator publishes the encrypted resource to the platform along with the access policy that corresponds to it. When users try to access a particular resource, users need to prove that their attributes match the access policy of the resource. Users request to decrypt the resource by providing their attribute key. The smart contract will verify that the requestor's attribute key matches the resource's access policy. If the verification is successful, the smart contract will allow the decryption operation and the user will be able to access the plaintext resource. The resource [18] can be successfully decrypted only if the user's attribute key conforms to the access policy of the resource. The specific flow of the related algorithm is shown in Figure 3.

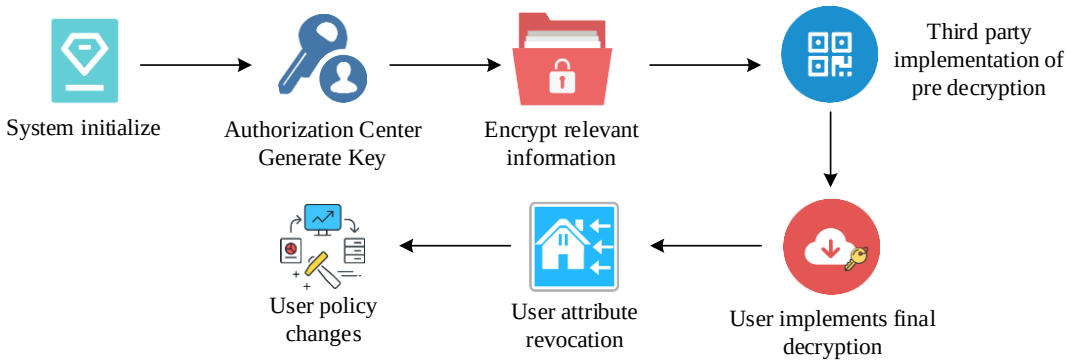


Figure 3: The specific process of ABE algorithm

In Figure 3, the ABE algorithm includes six steps: system initialization, embedding ciphertext data in access policies, third-party pre decryption, final decryption, and data update. Firstly, the system administrator performs the initialisation operation, generates the global parameters and master key, publishes the public parameters and implements the function as shown in Equation (1).

$$Setup(1^{\lambda}) \rightarrow (PK, MK) \tag{1}$$

In Equation (1), 1^{λ} denotes the security parameter, PK means the public key of the system, and MK means the master key. Then the authorisation centre generates the corresponding private key based on the set of user's attributes, the expression is shown in Equation (2).

$$KeyGen(MK, A) \rightarrow SK_A \tag{2}$$

In Equation (2), A represents the set of user's attributes and SK_A represents the attribute key generated based on the set of user's attributes. Then the educational resource creator selects the appropriate access policy and encrypts the resource using the public parameters of the system. The encryption process is shown in Equation (3).

$$Encrypt(PK, M, P) \rightarrow CT \tag{3}$$

In Equation (3), M represents the content of the resource to be encrypted, P represents the access policy, and CT represents the encrypted ciphertext. When a requester requests a resource, the third-party organisation performs a pre-decryption operation based on the attributes of the requester and the requested resource to generate partially decrypted data, as described in Equation (4).

$$DelegateDecrypt(PK, CT, SK_A) \rightarrow CT' \tag{4}$$

In Equation (4), CT' represents the partially decrypted ciphertext. The final decryption of the pre-decrypted data is carried out by the requestor using his private key, the expression of which is given in Equation (5).

$$Decrypt(CT', SK_A) \rightarrow M \mid \perp \tag{5}$$

The user can decrypt the original message M only if the user's attribute key SK_A satisfies the access policy P of the ciphertext CT. If it is not satisfied, the decryption operation will fail and return a special symbol $\perp$ to indicate that the decryption is unsuccessful. When the user's attribute is no longer valid, the system will revoke his/her private key to prevent the user from accessing the

new encrypted resource, which is calculated as shown in Equation (6).

$$Revoke(A) \rightarrow SK_{A_{new}}, CT_{new} \tag{6}$$

In Equation (6), $SK_{A_{new}}$ denotes the new attribute key and CT_{new} denotes the ciphertext updated according to the new key. If the access policy of the resource is changed, the encrypted resource needs to be updated to ensure that only the users who comply with the new policy can access it, and the calculation method is shown in Equation (7).

$$Update(P, P_{new}, CT) \rightarrow CT_{new} \tag{7}$$

In equation (7), P_{new} represents the new access policy.

3.2 Blockchain data access control model based on optimised ABE algorithm

Although the designed secure sharing model for digital ER achieves the security and efficiency of data sharing to a certain extent, the traditional ABE algorithm still suffers from inefficiency in dynamic user attribute changes and policy updates [19]. Meanwhile, when the amount of users increases dramatically, the workload of distributing and managing attribute keys increases dramatically, resulting in limited system scalability. Moreover, for complex access control policies, the original model is not expressive enough, and it is difficult to accurately realise fine-grained access control [20, 21]. Therefore, to solve these problems, the research designs a blockchain data access control model based on CP-ABE algorithm to raise the flexibility, scalability and accuracy of the system. The optimised model flow is shown in Figure 4.

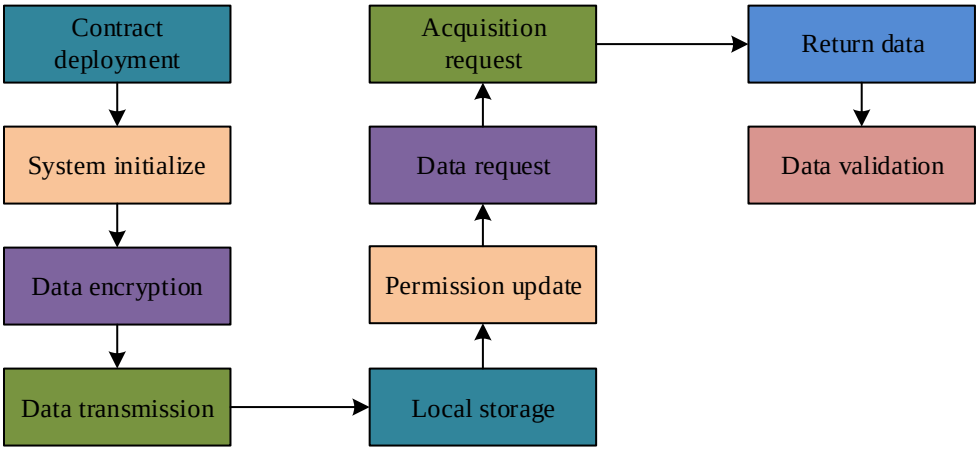


Figure 4: Optimized model process

First, the model introduces a new attribute and policy update mechanism to address the problem of dynamic user attribute and policy changes. The update mechanism allows the user's attributes to change dynamically without revealing the user's private key, and the access policies of resources can be updated flexibly in response to environmental changes. The update operation is calculated as shown in Equation (8).

$$\begin{cases} SK_{new} = U_{update}(Attr_{new}, SK) \\ CT_{new} = P_{update}(AC_{new}, CT) \end{cases} \tag{8}$$

In Equation (8), SK_{new} represents the updated private key, $Attr_{new}$ the user's new set of attributes, and AC_{new} the new access control policy. To raise the scalability of the model, the study adopts a distributed attribute authorisation management mechanism in the model, which balances the load of key distribution and management by multiple authorisation centres in the blockchain network working together. The key distribution mechanism expression is shown in Equation (9).

$$Distribute(SK) = \{AuthCente_1r, AuthCenter_2, \ldots, AuthCenter_n\} \tag{9}$$

In Equation (9), $Distribute(SK)$ represents the set of authorisation centres involved in key distribution. For complex access control policies, the study introduces a policy construction method based on logical expressions, which enables the policy to describe the access conditions more flexibly and precisely. The policy construction method is shown in Equation (10).

$$AC = AC_{construct}(Attributes, Logic) \tag{10}$$

In Equation (10), $Attributes$ represents the set of available user attributes, $Logic$ represents the logical expression, and AC represents the constructed access control policy. To further raise the security and privacy protection of the model, an anonymous attribute proof mechanism is introduced so that users do not have to disclose their attribute information when requesting access. The anonymous proof mechanism is shown in Equation (11).

$$Proof = Prove_{anon}(SK, AC) \quad (11)$$

In Equation (11), $Proof$ represents the anonymous attribute proof provided by the user. When the user requests access to the resource, the smart contract will judge whether the access policy is satisfied based on the user's anonymous attribute proof, and this verification process is shown in Equation (12).

$$Accept, Reject = Verify(Proof, AC) \quad (12)$$

In Equation (12), $Verify$ represents the validation function. If the $Verify$ function determines that the submitted information is valid and meets the predefined criteria or conditions, it returns $Accept$. If the $Verify$ function determines that the submitted information is invalid, does not satisfy the predefined criteria or conditions, or is an obvious forgery, it will return to the $Reject$ state. To ensure the security of the data transmission process, the study also uses a new ciphertext transmission mechanism, defined as Equation (13).

$$Transmit(CT) = \{User_1, User_2, \ldots, User_m\} \quad (13)$$

In Equation (13), $Transmit(CT)$ represents the set of users who receive the ciphertext. Finally, in order to deal with possible key leakage or misuse problems, the study uses a key revocation mechanism with the expression shown in Equation (14).

$$SK_{revoked} = Revoke(SK_{compromised}, BL, PP, MK) \quad (14)$$

In Equation (14), $SK_{revoked}$ represents the new private key after being revoked, $SK_{compromised}$ represents the private key that has been previously leaked or has been identified as needing to be revoked, BL represents the blacklist, which contains all the identifiers or relevant attributes of the revoked keys, and PP represents the public parameter, which is a parameter that is defined by the system for all users. The framework of the designed CP-ABE algorithm is shown in Figure 5.

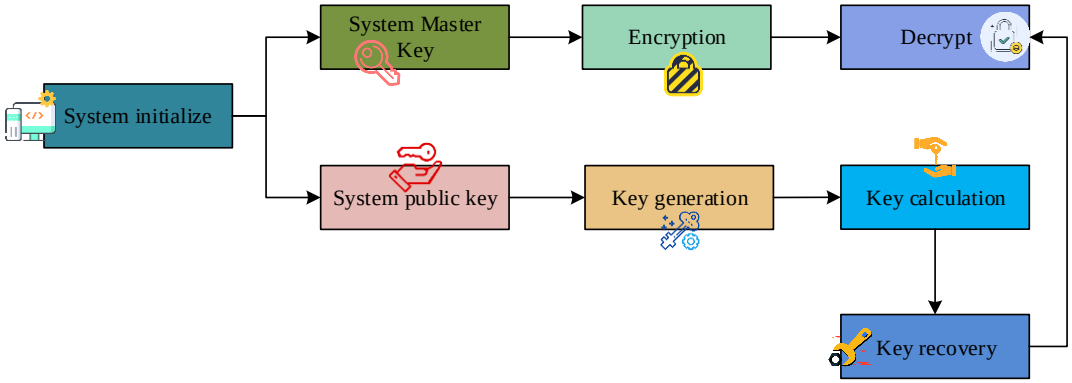


Figure 5: Designed CP-ABE algorithm framework

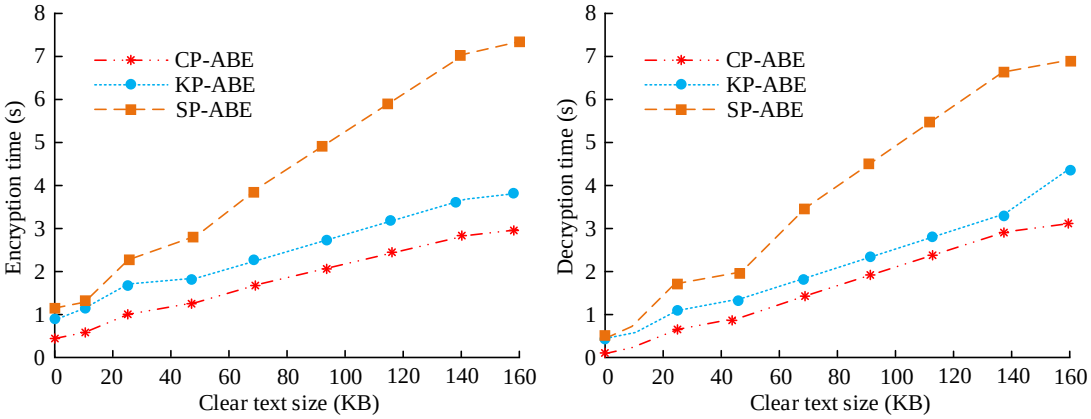
The designed blockchain data access control model based on CP-ABE algorithm effectively solves the problems in the original model while ensuring the secure sharing of digital ER. Through the new mechanism of policy update, distributed attribute authorisation management, flexible construction of complex policies and anonymous attribute proof, the model achieves higher security, better scalability and more accurate access control.

4 Analysis of the results of the security sharing model based on the CP-ABE algorithm

In order to verify the effect of digital ER security sharing model based on CP-ABE algorithm, the study analyses its performance and practical effect application through simulation experiments.

4.1 Performance analysis of blockchain data access control model based on CP-ABE algorithm

In order to verify the performance of the designed secure sharing model, the study conducts simulation experiments with the JPBC open-source Java library under the operating system with a processor of Intel Core i7-10750H, running on 16 GB of RAM, and 64-bit Windows 10. Firstly, encryption and decryption operations are performed on a set of 160 KB plaintexts, and the encryption and decryption times are calculated separately and compared with those of Key-Policy Attribute-Based Encryption (KP-ABE) and Specific-Policy Attribute-based Encryption (SP-ABE). Based Encryption, SP-ABE) encryption and decryption times are compared and the results are shown in Figure 6.



(a) Comparison of encryption time (b) Decryption time comparison

Figure 6: Comparison of encryption and decryption times for different algorithms

From Figure 6(a), the encryption time of different algorithms tends to increase as the plaintext size increases. The average encryption time of SP-ABE algorithm is 4.27 s, the average encryption time of KP-ABE algorithm is 2.31 s, and the average encryption time of CP-ABE algorithm is 1.66 s. From Figure 6(b) that the decryption time of the different algorithms increases with the increase of the size of the plaintexts, and the average decryption time of the three algorithms is 3.69 s, 2.34 s, and 1.65 s, respectively. In comparison with the KP-ABE and SP-ABE algorithms, CP-ABE exhibits shorter time consumption in both encryption and decryption processes, which proves its superiority in computational efficiency. Then, to verify the security of the designed secure sharing model, the study compares it with several other algorithms from multiple perspectives, and the output is 1 if the feature is supported and 0 if it is not supported, and the findings are denoted in Table 2.

Table 2: Comparison of security performance of different algorithms

Programme	Fine-grained access control	Privacy	Ease of key management for encryption/decryption	Key secure distribution
ABE	0	1	0	1
SP-ABE	0	1	1	1
KP-ABE	1	1	0	1
CP-ABE	1	1	1	1

From Table 2, the designed secure sharing model satisfies these characteristics in four aspects: fine-grained access control, privacy protection, ease of encryption and decryption key management, and secure key distribution. This means that it is able to provide comprehensive security and at the same time ensure ease of use. It proves that it can provide a comprehensive, secure and user-friendly data sharing environment.

Finally the variation of storage space required for the access control model with the amount of users under different algorithms is calculated and the results are denoted in Figure 7.

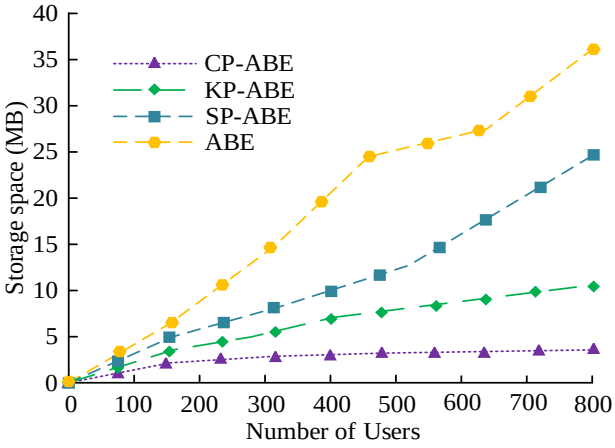


Figure 7: Changes in storage space required for access control models under different algorithms

In Figure 7, with the increase of the amount of users, the storage space required for the access control model under different algorithms shows a gradual upward trend. It can be found that when the amount of users reaches 800, the storage space required for the access control model under the CP-ABE algorithm is 3.9 MB, which is significantly lower than that required for the access control model under other algorithms. It shows that CP-ABE algorithm reduces the storage burden due to the increase in the amount of users while ensuring security, so that the scalability of the system is improved. To further verify the security of the proposed blockchain data access control model based on CP-ABE algorithm, the success rate of the proposed model against Sybil attack, Dos attack, and U2R attack was calculated in a distributed environment, and compared with KP-ABE and the model in reference [20]. The results are shown in Table 3.

Table 3: Resistance success rates of different models against three types of attacks

Attack Type	Resistance success rate (%)		
	CP-ABE	KP-ABE	Reference [20]
Sybil	99.26	91.39	97.72
Dos	97.63	90.98	95.51
U2R	98.59	92.24	96.14

From Table 3, it can be seen that the blockchain data access control model based on the CP-ABE algorithm proposed by the research institute has a success rate of 99.26% in resisting Sybil attacks, 97.63% in resisting Dos attacks, and 98.59% in resisting U2R attacks. Observation shows that the proposed model has a significantly higher success rate in resisting three types of attacks than the other two models, demonstrating its ability to effectively resist different network attacks in distributed environments. To test the stability and robustness of the model, sensitivity analysis was conducted under different network user loads, and the information leakage rates were calculated for user requests of 1000, 2000, and 3000, respectively. The results are shown in Figure 8.

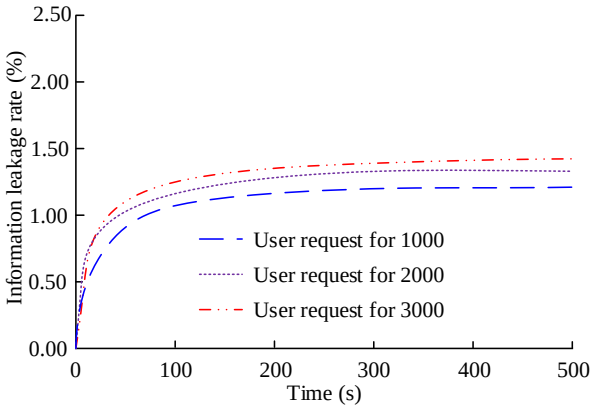
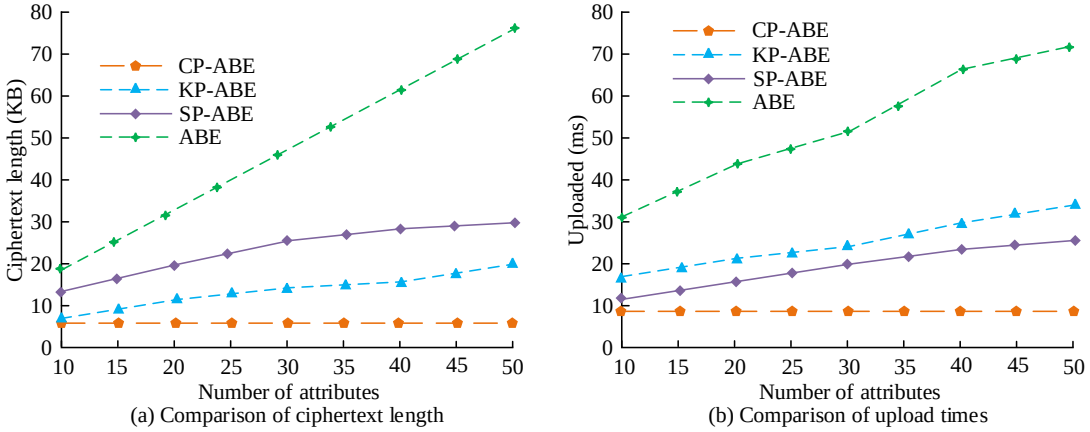


Figure 8 Information leakage rate under different user requests

From Figure 8, it can be seen that with the increase of time, the information leakage rate shows an upward trend and gradually stabilizes. When the user request is 1000, the maximum information leakage rate is 1.20%. When the user request is 2000, the maximum information leakage rate is 1.40%. When the user request is 3000, the maximum information leakage rate is 1.45%. It can be observed that as user requests increase, the information leakage rate gradually increases, but the rate of increase slows down, demonstrating the adaptability and stability of the proposed model in handling high user loads.

4.2 Analysis of practical application effect of blockchain data access control model based on CP-ABE algorithm

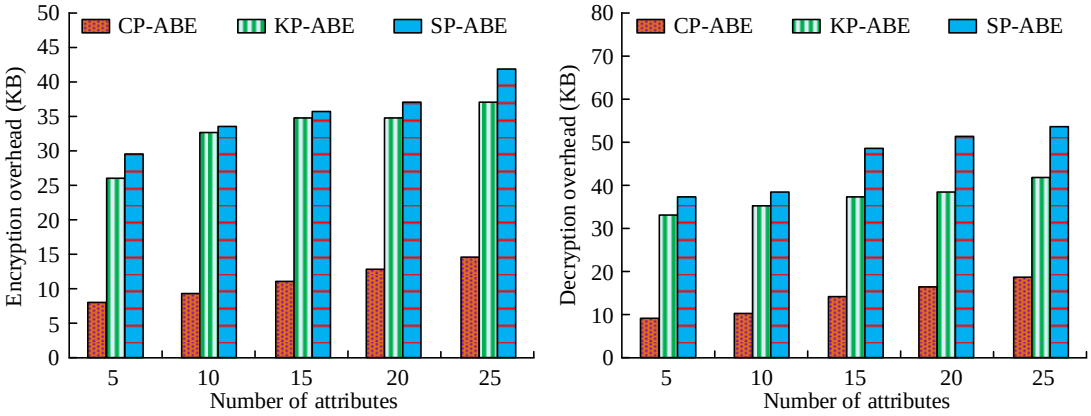
To verify the effectiveness of blockchain data access control model based on CP-ABE algorithm in practical applications, the study tested the ciphertext length and upload time generated by the access control model under different algorithms respectively, and the comparison findings are denoted in Figure 9.



(a) Comparison of ciphertext length (b) Comparison of upload times

Figure 9: Comparison of ciphertext length and upload time generated by access control models under different algorithms

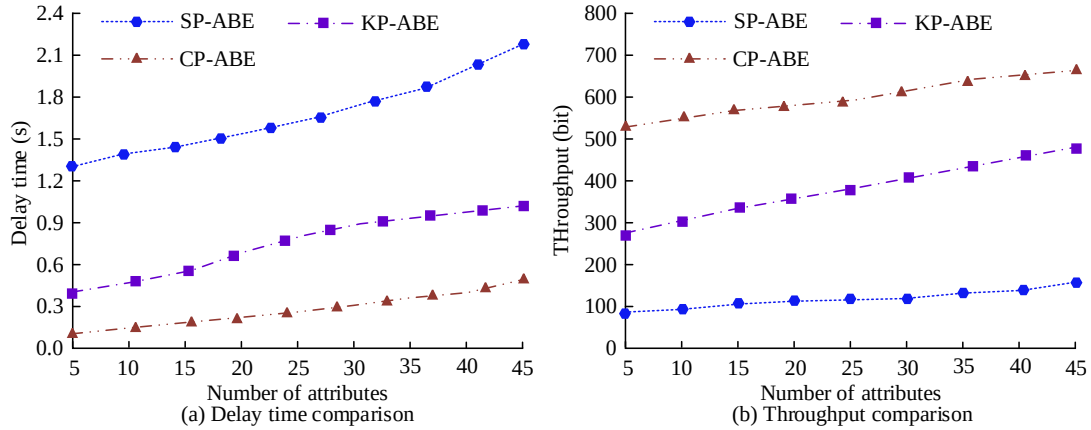
From Figure 9(a), with the increase of the amount of attributes, the three algorithms, SBE algorithm, SP-ABE algorithm, and KP-ABE algorithm, generate the ciphertext length with increasing trend, while CP-ABE algorithm generates a fixed ciphertext length with the value of 5.8 KB. From Figure 9(b), with the increase of the amount of attributes, the ciphertext uploading time of CP-ABE algorithm is constant with a value of 9.2 ms, while the ciphertext uploading time of the other three algorithms increases gradually. It shows that CP-ABE algorithm is able to generate ciphertexts with fixed and short ciphertext lengths, as well as maintain a stable and low latency ciphertext upload time in the application of blockchain data access control. The next step is to calculate the overhead of different algorithms for encryption and decryption respectively and the results are denoted in Figure 10.



(a) Comparison of encryption costs (b) Decryption Cost Comparison

Figure 10: Comparison of overhead for encryption and decryption using different algorithms

From Figure 10(a), with the increase in the amount of attributes, the overhead of different algorithms for encryption shows an increasing trend. When the amount of attributes is 25, the overhead of SP-ABE algorithm is 42.3 KB, the overhead of KP-ABE algorithm is 36.6 KB, and the overhead of CP-ABE algorithm is 14.9 KB. From Figure 10(b), it can be seen that the overhead of the three algorithms in decrypting is gradually increasing, and the different algorithms have an overhead of 53.5 KB, 41.8 KB, and 19.2 KB, respectively, when the amount of attributes is 25, 19.2 KB. The above outcomes denote that the CP-ABE algorithm has lower resource consumption, which can maintain the device running for a long time and reduce the operation cost. Then the delay time and system throughput of the access control model under different algorithms are calculated to verify the efficiency of the model, and the results are denoted in Figure 11.



(a) Delay time comparison (b) Throughput comparison

Figure 11: Comparison of latency and throughput of different algorithms

From Figure 11(a), the delay time tends to increase with the increase in the amount of attributes. The average delay time of SP-ABE algorithm is 1.76 s, KP-ABE algorithm is 0.71 s, and CP-ABE algorithm is 0.33 s. From Figure 11(b), the system throughput of the different algorithms increases gradually with the increase in the amount of attributes. The average system throughput of the three algorithms are 128.6 bit, 388.2 bit, 594.7 bit. The above outcomes denote that the CP-ABE algorithm can significantly reduce the latency time and increase the system throughput, which proves that it is more efficient in processing data. Finally, the memory resource consumption and CPU resource consumption of different algorithms are calculated respectively, and the comparison results are denoted in Figure 12.

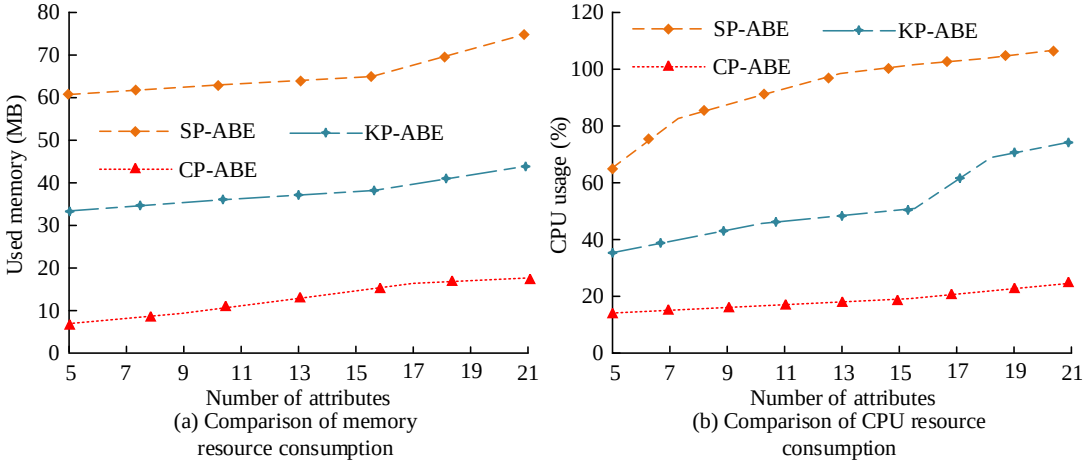


Figure 12: Comparison of memory and CPU resource consumption of different algorithms

From Figure 12(a), with the increase of the amount of attributes, the memory resource consumption of different algorithms are gradually increasing.The average memory occupation of SP-ABE, KP-ABE, and CP-ABE algorithms are 68.3 MB, 38.4 MB, and 12.7 MB, respectively. From Figure 12(b), the CPU occupancy of each algorithm is on the increasing trend, and the average CPU occupancy of three kinds of algorithms have average CPU occupancy of 86.4%, 54.5%, and 19.2%, respectively. The above results indicate that the CP-ABE algorithm is superior to the SP-ABE algorithm and KP-ABE algorithm in terms of memory and CPU resource consumption, indicating that the CP-ABE algorithm has lower computational resource requirements during execution and can process data more quickly, thereby effectively reducing the complexity of the algorithm.

5 Discussion

In order to solve the problems of high complexity and high implementation cost in traditional digital resource education security sharing, a digital education resource security sharing model combining blockchain and ABE algorithm is proposed. The average encryption time of this model is 1.66 s, and the average decryption time is 1.65 s, which is significantly lower than other methods, proving its significant advantage in computational efficiency. Compared with the fast detection method based on deep reinforcement learning proposed by Liang et al. [4], although it can effectively improve the computational speed, the proposed method has significantly faster computation speed. This is because deep reinforcement learning algorithms usually require a large amount of data to train the model, and require a lot of time to converge during the training phase, so their computational efficiency is relatively low. The model proposed by the research institute supports fine-grained access control, privacy protection, easy encryption and decryption key management, and secure key distribution, proving that it can provide comprehensive security protection and ensure ease of use. This is consistent with the findings of Kumar et al. [9], but the security of the proposed model is higher than that of the cloud based online education system proposed by Kumar A et al., as the system relies heavily on cloud computing and also needs to consider the credit issues of cloud service providers when using it. In summary, by combining the CP-ABE algorithm with blockchain technology, a digital education resource security sharing model is proposed, which effectively improves the sharing efficiency and provides new ideas for the secure management of educational data and resource sharing.

6 Conclusion

At present, the secure sharing of digital ER still faces many challenges, such as irrational use of resources and piracy problems, which seriously affect the effective use and sharing of ER. Therefore, the study constructs a secure sharing model by means of the ABE algorithm optimised by ciphertext policy and integrating it with blockchain technology, aiming to improve the refinement of data management while ensuring information security and user privacy. The outcomes denote that the CP-ABE algorithm has shorter time consumption during encryption and decryption compared to the SP-ABE algorithm and the KP-ABE algorithm, down to 1.66 seconds and 1.65 seconds, respectively, indicating that it significantly improves the processing efficiency. As the amount of users increases to 800, the required storage space is only 3.9 MB, proving that the designed secure sharing model alleviates the storage burden caused by scalability. In terms of practical application effects, the CP-ABE algorithm is able to maintain a constant ciphertext length of 5.8 KB and a stable upload time of 9.2 ms when the amount of attributes increases, demonstrating its superiority in data access control. From the perspective of resource consumption, the design model can effectively reduce the latency time to 0.33 seconds and increase the system throughput to 594.7 bits, proving its ability to process data efficiently. However, the performance of the model in handling very large scale users has not been fully validated and the storage optimisation potential is yet to be explored. Future research will explore further optimization of algorithms to cope with the rapid growth of user base, and expand the application scope of models for specific needs in different educational scenarios. At the same time, specific access control policies can be added

and blockchain technology can be optimized to enable the model to query data access records. Through stricter access control and data protection measures, the model can be extended to other fields that require secure and fine-grained data sharing to enhance its actual influence.

References

[1] Wei X, Yan Y, Guo S, Qiu X, Qi F. Secure data sharing: blockchain-enabled data access control framework for IoT. IEEE Internet of Things Journal, 2021, 9 (11): 8143-8153. http//:doi.org/10.1109/JIOT.2021.3111012.

[2] John K V. An empirical investigation into the extent university students Utilise mobile educational applications for learning. Acta Informatica Malaysia. 2022, 6(1): 25-33. http//:doi.org/10.26480/aim.01.2022.25.33

[3] Feng C, Yu K, Bashir A K, Al-Otaibi Y D, Lu Y, Chen S, Zhang D. Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. IEEE Network, 2021, 35(1): 130-137. http//:doi.org/10.1109/MNET.011.2000223.

[4] Alattas A H A, Al-Shareeda M A, Manickam S, Saare M A. Enhancement of NTSA secure communication with one-time pad (OTP) in IoT. Informatica, 2023, 47(1). http//:doi.org/10.31449/inf.v47i1.4463.

[5] Liang W, Huang W, Long J, Zhang K, Li K C, Zhang D. Deep reinforcement learning for resource protection and real-time detection in IoT environment. IEEE Internet of Things Journal, 2020, 7(7): 6392-6401. http//:doi.org/10.1109/JIOT.2020.2974281.

[6] Li Z, Ma Z. A blockchain-based credible and secure education experience data management scheme supporting for searchable encryption. China Communications, 2021, 18(6): 172-183. http//:doi.org/10.23919/JCC.2021.06.014.

[7] Gajendran N. Blockchain-Based secure framework for e-learning during COVID-19. Indian Journal of Science and Technology, 2020, 13(12): 1328-1341. http//:doi.org/10.17485/ijst/v13i12.152.

[8] Sharma R K, Pippal R S. Blockchain based efficient and secure peer-to-peer distributed IoT network for non-trusting device-to-device communication. Informatica, 2023, 47(4). http//:doi.org/10.31449/inf.v47i4.3494.

[9] Eunaicy J I C, Vadivelu V S. A SEMWORD based semantic secure content retrieval system in e-learning. Indian Journal of Science and Technology, 2023, 16 (31): 2447-2457. http//:doi.org/10.17485/15T/1631.833.

[10] Zhang Z, Ren X. Data security sharing method based on CP-ABE and blockchain. Journal of Intelligent & Fuzzy Systems, 2021, 40(2): 2193-2203. http//:doi.org/10.3233/JIFS-189318.

[11] Irshad S, Brohi M N, Soomro T R. Block-ed: the proposed blockchain solution for effectively utilising educational resources. Applied Computer Systems, 2020, 25(1): 1-10. http//:doi.org/10.2478/acss-2020-0001.

[12] Xue H, Guo K. The key technologies of blockchain and the design of smart education platform. International Journal of Education and Humanities, 2023 International Journal of Education and Humanities, 2023, 8(2): 90-95. http//:doi.org/10.54097/ijeh.v8i2.7753.

[13] Bathula A, Muhuri S, Gupta S K, Merugu S. Secure certificate sharing based on Blockchain framework for online education. Multimedia Tools and Applications, 2023, 82(11): 16479-16500. http//:doi.org/10.1007/s11042-022-14126-x.

[14] Chen L, Feng T, Fan D. Construction of a sharing model for network digital teaching resources oriented to big data. International Journal of Continuing Engineering Education and Life Long Learning, 2020, 30(2): 190-203. http//:doi.org/10.1504/IJCEELL.2020.106343.

[15] Deng H. Resource sharing system of college English education based on wireless sensor network. International Journal of Continuing Engineering International Journal of Continuing Engineering Education and Life Long Learning, 2023, 33(1): 37-53. http//:doi.org/10.2478/acss-2020-0001.

[16] Han C. English information teaching resource sharing based on deep reinforcement learning. International Journal of Continuing Engineering Education and Life Long Learning, 2024, 34(1): 53-65. http//:doi.org/10.1504/IJCEELL.2024.135269.

[17] Yang X, Li W, Fan K. A revocable attribute-based encryption EHR sharing scheme with multiple authorities in blockchain. Peer-to-Peer Networking and Applications, 2023, 16(1): 107-125. http//:doi.org/10.1007/s12083-022-01387-4.

[18] Groumpos P P. A critical historic overview of artificial intelligence: issues, challenges, opportunities, and threats. Artificial Intelligence and Applications. 2023, 1(4): 197-213. http//:doi.org/10.47852/bonviewAIA3202689.

[19] Mishra A K, Mohapatra Y. Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems. International Journal of Information Technology, 2024, 16(1): 121-130. http//:doi.org/10.1007/s41870-023-01625-9.

[20] Weber-Lewerenz B C, Traverso M. Navigating applied artificial intelligence (AI) in the digital era: how smart buildings and smart cities become the key to sustainability. Artificial Intelligence and Applications. 2023, 1(4): 230-243. http//:doi.org/10.47852/bonviewAIA32021063.

[21] He Y, Wang H, Li Y, Huang K, Leung V C, Yu F R, Ming Z. An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain. IEEE Internet of Things Journal, 2021, 9(4): 2722-2733. http//:doi.org/10.1109/JIOT.2021.3099171.