Hindawi
Security and Communication Networks
Volume 2023, Article ID 9797836, 1 page
https://doi.org/10.1155/2023/9797836

Retraction

Retracted: Analysis of Co-Construction and Sharing Mechanism of Digital Education Resources based on Digital Information Encryption Technology

Security and Communication Networks

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. Zhang and L. Xiang, "Analysis of Co-Construction and Sharing Mechanism of Digital Education Resources based on Digital Information Encryption Technology," *Security and Communication Networks*, vol. 2022, Article ID 4880385, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4880385, 11 pages
https://doi.org/10.1155/2022/4880385

Research Article

Analysis of Co-Construction and Sharing Mechanism of Digital Education Resources based on Digital Information Encryption Technology

Mingbao Zhang and Li Xiang

School of Digital Arts and Design, Dalian Neusoft University of Information, Dalian 116023, Liaoning, China

Correspondence should be addressed to Mingbao Zhang; zhangmingbao@neusoft.edu.cn

Received 28 March 2022; Revised 19 May 2022; Accepted 24 May 2022; Published 29 June 2022

Academic Editor: Mohammad Ayoub Khan

In order to solve the problem of information security, the process of digital resource development and integration has become the key. A method based on focusing on the development and integration of digital instructions is proposed, which discusses digital data encryption in detail, focusing on the DES algorithm in the symmetric encryption algorithm and the RSA algorithm in the asymmetric encryption algorithm and conducts a security evaluation. Through comparative analysis, the comprehensive communication system based on the combination of DES encryption algorithm and RSA encryption algorithm aims to realize the integration and sharing of digital display. Through experimental analysis and comparison with traditional commonly used encryption methods, 64-bit keys are very easy to generate, but the keys must be distributed before communication, and the keys must be changed from time to time. In this way, key management consumes a lot of system overhead. From the final experimental data, it can be concluded that the encryption algorithm has performance advantages over the separate DES and RSA algorithms.

1. Introduction

With the introduction of the concept of "Informatization Education" and the implementation of the "Information Superhighway" plan in the United States, countries around the world have begun to construct educational informatization. Owing to this opportunity, digital educational resources have begun to be widely concerned by all sectors of the society. With an understanding of the teaching and educational process, the best digital teaching methods are playing a greater role in higher education as a new type of education. The development and success of the digital cloud has opened up new avenues for integrating digital learning into colleges and universities. The use of digital cloud to realize the integration of digital learning in colleges and universities has irreversible value. However, in the process of sharing digital information through digital cloud, how to ensure the security and reliability of data resources becomes the key. Figure 1 shows the protection diagram in the process of digital teaching resource sharing.

Now, there are three more common uses. One is the self-identification service, which needs to integrate the resources provided by the university and provide user authentication at the same time. However, this method requires the authentication server of each school to verify all user requests, which has a large load and is not conducive to privacy protection. The second is to establish a shared resource authentication center, that is, the authentication center uniformly manages users' interschool resource access requests, but this method requires high reliability of the authentication center and poor flexibility when colleges and universities join or exit. The third is the alliance cooperation method, that is, each member university in the shared alliance independently manages its own users and resources, and forms an alliance in the form of distribution. The user obtains a token that can identify the identity from the identity authentication system of the University. The token is common in the alliance and can be recognized by the identity authentication system of other universities, but this method is difficult and has low universality.

Based on the aforementioned problems and the characteristics of digital technology development and sharing, this paper adopts digital data encryption technology to encrypt and protect data in the process of collaborative design of digital teaching. Based on the characteristics of the DES encryption algorithm and the RSA algorithm, this paper explains the integrity of these two types of connections and discusses their security procedures in the reporting processing, creating, and sharing of digital content. On the basis of not changing the investment in educational information resources, studying the use of information technology to promote the "tilting" of educational information resources to weak schools and promoting the coordinated and balanced development of educational information resources between urban and rural schools can open up a new way for exploring educational equity in the information age.

2. Literature Review

Data encryption is the use of digital or physical means to protect electronic data during transmission and store it in a system to prevent it from being leaked. Almeida-Santana et al. [1] found that information data encryption is the information that can be read, understood, and recognized by a large range of people (or machines) through information transformation or coding (these information can be voice, text, image, symbol, etc.). Through a certain method (algorithm), make it become difficult to understand the garbled information, so as to ensure the information security and prevent it from being illegally embezzled or read by non-relevant personnel beyond their authority. Liu, and others [2] called the original information in the encryption process "plaintext," and Byron [3] proposed that the form of plaintext after conversion and encryption is "ciphertext." The process of converting "plaintext" to "ciphertext" is called "encryption," and the process of converting ciphertext to plaintext is called "decryption." Evtikhiev et al. [4] considers the possibility of time-integrated optical encryption in quasi-bichromatic spatially incoherent light using a digital micromirror device. An experimental setup for optical registration of images to be encrypted on a digital camera is presented. Images containing textual and graphic information are encrypted and successfully decrypted using the inverse filtering method.

Generally speaking, data encryption can be divided into two types: symmetric key encryption and asymmetric key encryption.

(1) Symmetric key encryption is also known as private key encryption or key encryption. Symmetric key is a traditional encryption method, which is the simplest way. During symmetric key encryption, both sides of communication need to exchange each other's keys. When they need to send information data to each other, they use their own encryption key for encryption, and when they need the information data of the receiver, they use the key given by the other party for decryption. The specific encryption method is shown in Figure 2.

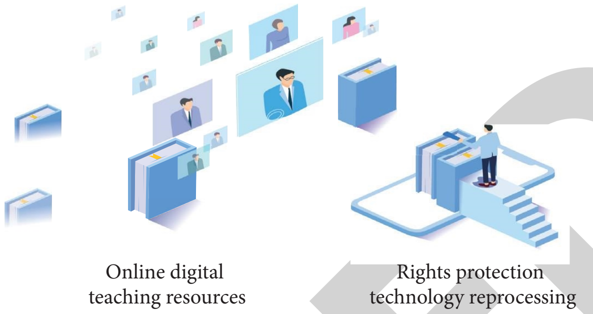

Online digital teaching resources
Rights protection technology reprocessing

FIGURE 1: Resource protection mechanism in the process of sharing digital teaching resources.

Symmetric key encryption algorithms include des, 3des, input, feel, blowfish, and so on. DES algorithm still has higher security than other encryption algorithms, because DES algorithm has quite high complexity, especially in some cases with high confidentiality requirements, it is more reliable to use triple des or 3DES system. DES algorithm has a wider range of functions because it is easy to master, economical, and effective. Tian et al. [5] thought that at present, there is no other effective attack method except that the exhaustive search method can effectively attack the DES algorithm.

Idea algorithm has undergone a lot of detailed review. Mirkovski and others [6] found that the algorithm has strong resistance to cryptanalysis, so it is used in many product industries. The input is split into 64-bit data blocks and encrypted plaintext blocks with a key length of 128 bits. It is based on the design concept of "hybridization of multiple algebraic groups." The algorithm is easy to use in both hardware and software and is much faster than DES. Access input algorithms for 64-bit data sets are generally divided into four 16-bit subsets: a_1, a_2, a_3, and a_4. These four groups create the first stage of the data entry algorithm in eight steps.

Feal algorithm is not suitable for small systems. It is proposed to focus on the implementation of DES only in hardware at that time. Feal algorithm is a set of packet encryption algorithm similar to DES proposed by Chen and Ma [7]. However, Feal has higher security intensity than DES in each round, which is more suitable to be realized by software. Feal does not use permutation functions to confuse the data during encryption or decryption. Feal uses XOR, rotation, addition, and modulus operations. The generation of Feal subkey uses eight rounds of iterative cycles, each cycle generates 2 16 bit subkeys, and a total of 16 subkeys are generated for encryption algorithm.

Asymmetric key encryption is also known as public key encryption, in other words, asymmetric encryption algorithms require two keys, a public key and a private key. There are public encryption keys and multiple encryption keys. We use different keys, such as different encryption and

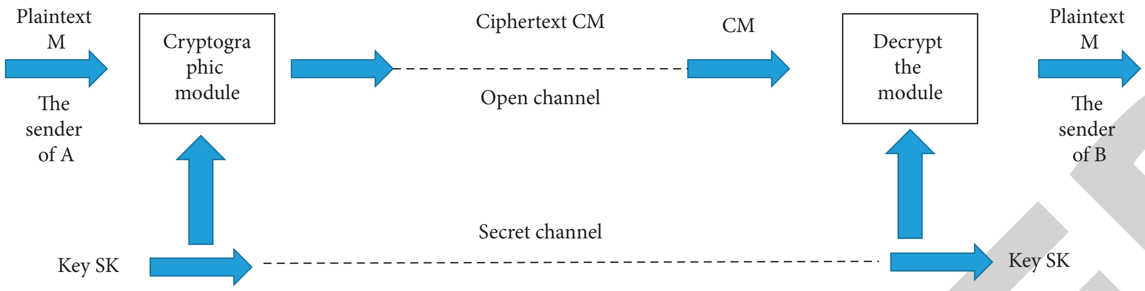


Figure 2: Schematic diagram of symmetric encryption algorithm.

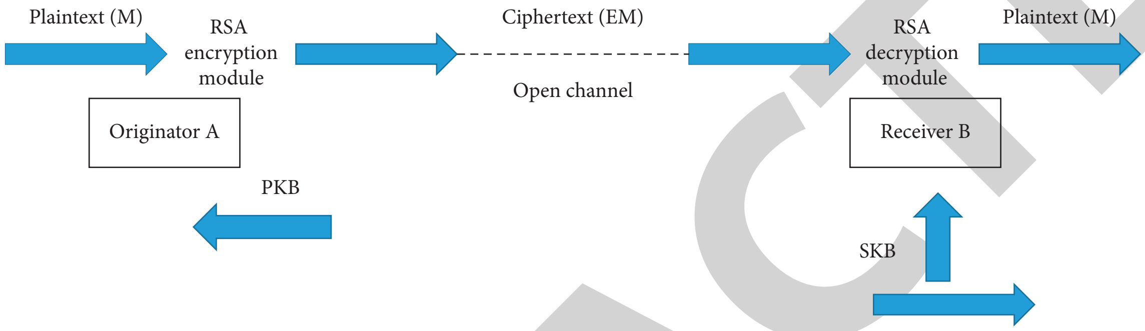


Figure 3: Encryption diagram.

decryption algorithms. There is some connection between the two, but it is impossible to separate the two. If you use the private key to encrypt data, you must use the public key to access it. If data are encrypted with the public key, only the associated private key can be encrypted. A special form of image encryption is shown in Figure 3.

A typical algorithm for asymmetric key encryption is the RSA algorithm. The RSA algorithm is the world's first asymmetric encryption algorithm that can be used for data encryption and digital signatures. RSA algorithm was developed by Dong et al. [8], Yohei, and Seki in 1977 [9] and Lee et al. [10] published at the Massachusetts Institute of technology. RSA is the most influential public key encryption algorithm at present. Amat [11] and others think it can resist all known cryptographic attacks and has been recommended as the public key data encryption standard by the ISO. The security of RSA algorithm depends on large number decomposition, but it has not been proved that large number decomposition is necessary to crack RSA. Therefore, whether it is equivalent to large number decomposition has not been supported by theoretical proof. Lu and Cao proposed a blockchain-based secure storage and sharing scheme for ELR in MOOCs learning systems [12]. Shahidinejad et al. found that such smart devices are generating data and connecting to each other through edge cloud infrastructure [13]. The Zhang et al. study identified 13 key capabilities of digital technologies most relevant to circular economy strategies [14]. Shahidinejad et al. found that cloud computing is an emerging distributed computing paradigm and has become one of the most popular computing paradigms today [15]. Dakhil et al. task digital twins to update building information models in near real-time using IoT sensors, while blockchain authenticates and increases confidence in all data transactions of digital twins [16]. Mazidi et al. found that the scalability nature of cloud computing attracted application service providers (ASPs) to use cloud application hosting [17].

3. Research Methods

Shared resources refer to the sharing of digital resources, especially digital sharing projects based on school networks. Digital tutoring is a great way to reduce educational waste and improve your overall learning resources. On one hand, it can improve the utilization level of educational resources and give full play to the role of educational resources; on the other hand, it can integrate high-quality training resources [12]. In the use of cloud to jointly build and share digital teaching resources, the construction of teaching resource library has changed from closed to open, which promoted the efficient transmission and utilization of teaching resources, and fully integrated existing resources based on cloud-based teaching resource sharing. Provide open and fair learning resources for the majority of students, promote the efficient transfer and use of learning resources, open relatively independent learning resources for colleges and universities, move from closed to open, and provide users with unimpeded learning resources. It can also include various management software, database resources, hardware resources, and so on teaching resources have a large number, different forms, and complex structure, which also puts forward greater adjustments for the security protection of the transmission process of teaching resources [13].

At this stage, there are three measures that can be adopted: password-based authentication, smart-card-based authentication, and biometric-based authentication. Given

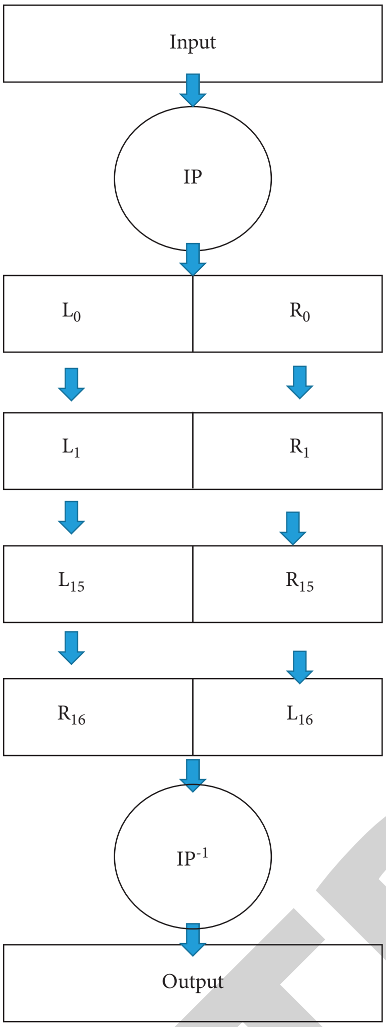


Figure 4: Overall process of DES algorithm.

Table 1: IP replacement table.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Table 2: IP^{-1} replacement table.

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

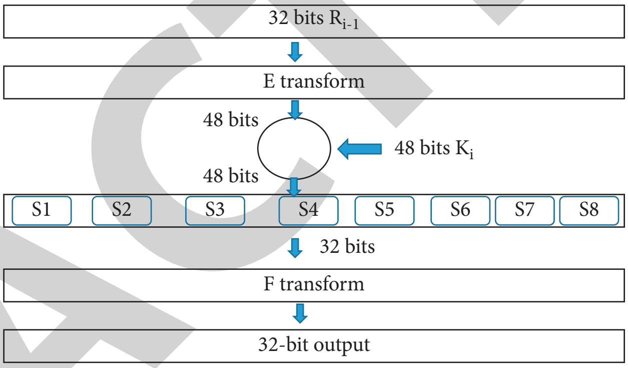


Figure 5: Specific process of F function.

the cost and current state of digital learning resources in colleges and universities, the best approach is password-based authentication. I have edited it. If you use the private key to encrypt data, you must use the public key to access it.

DES algorithm is the most typical symmetric encryption algorithm so far. It is widely used in many fields and is one of the representatives of block cipher. DES algorithm is a kind of symmetric cipher. It was developed by IBM in the United States and played a key role in supporting the development of cryptography [14]. However, since the algorithm was proposed, it has faced security threats from all aspects, such as exhaustive attack and selective plaintext attack [15]. The overall process of DES algorithm is shown in Figure 4.

DES algorithm mainly has three steps:

Step 1: Plaintext transformation [16]. First, the input bit plaintext is initially replaced to obtain the replaced plaintext X_0. X_0 is still 64-bit, but the order of plain-text information has changed. After replacing 64 bits, the plaintext is divided into L_0 and R_0 on the left and right, representing the left 32 bits and the right 32 bits of X_0 respectively.

Step 2: After the 64 bit plaintext input iteratively is divided into two groups, carry out round encryption. The encryption algorithm of each round is the same. Take the L_{i-1} and R_{i-1} of the previous round as the input of the next round, and the iteration rule of L_i and R_i of the output bits is $L_{i\,=}R_i$. $R_i = L_i \oplus f(R_{i-1}, K)$ $(i = 1, 2, 3, \ldots, 16)$. Here, f is a permutation function [17], which includes E change, S and P transformation, The ⊕ symbol indicates XOR.

Step 3: Finally, the ciphertext y is obtained by reversing the IP^{-1} table.

The algorithm process is described in detail as follows.

3.1. *IP Replacement and IP^{-1} Reverse Replacement [18].*

For the input 64 bit plaintext, the first operation is the initial IP replacement [19], which only changes the arrangement of information in the plaintext. The specific replacement table used is shown in IP replacement Table 1. As it is operated in the computer, either 0 or 1, the data after replacement do not have encryption effect. People speculate that these replacement are to prevent simulation attacks during hardware implementation. The replacement IP rule table is shown in Table 1.

From the replacement table, we found that the plain text sequence was broken. In plain text, bit 58 is the first bit, bit 50 is the second bit, bit 42 is the third bit, and so on. L_0 and R_0 are the remaining 32 bits and the remaining 32 bits after the transfer output, respectively. For example, if the input 64

Table 3: E transformation rules.

32	1	2	3	4	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17	18	19	20	21	20	21
22	23	24	25	26	27	28	29	28	29	30	31	32	1

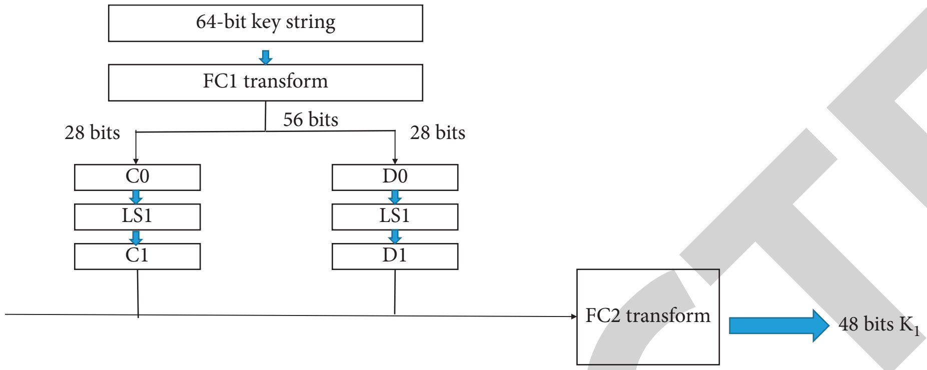


Figure 6: Generation process of subkey.

bit plaintext is $M_1, M_2, \ldots, M_{64}$, the result after initial replacement is $L_0 = M_{58}, M_{50}, \ldots, M_8$, $R_0 = M_{57}, M_{49}, \ldots, M_7$. After 16 iterations, L_{16} and R_{16} are obtained. L_{16} and R_{16} are taken as inputs and sent to the inverse replacement table for inverse replacement, that is, the encrypted ciphertext is obtained. Reversing is the reverse operation of the first gear change. The rule table of inverse permutation IP^{-1} is shown in Table 2.

3.2. F Function. The F function first converts the 32-bit R. The result is XOR with the 48 bit subkey and then sent to the S-box for compression output. The compressed data are changed by P to obtain the 32-bit output result. The specific process of F function is shown in Figure 5 [20].

As can be seen from Figure 5, this round of encryption mainly performs two operations: mixing and substitution, through which the purpose of plaintext disturbance is achieved [21]. Both operations are reversible. The algorithm of E-transform is to expand the 32-bit R_{i-1} into 48 bit data, which is convenient for XOR with the following subkeys. The rule table of E-transform is shown in Table 3.

The e-transformed data and the subkey are XOR operated, and the 48 bits are divided into eight groups, with 6 bits in each group, and then sent to the S-box, which compresses and outputs the data.

3.3. Generation of Subkey [1]. DES algorithm requires a total of 16 subkeys, each of which has 48 bits. Assuming that the original key is k, the actual length of K is 56 bits, including 8 parity bits. The 56 bit key is formed through a series of transformations.

The generation process of the required 48 bit key and subkey is shown in Figure 6.

Table 4: Wheel shift operation.

Wheel	Displacement
1,2,9,16	1 bit
3,4,5,6,7,8,10,11,10,13,14,15	2 bits

Table 5: Process of taking S1 as an example.

S_1															
13	4	13	1	2	15	11	8	3	10	7	12	5	9	0	7
0	15	8	4	14	2	13	1	11	6	12	11	9	6	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	10
15	12	8	2	4	10	1	7	5	11	3	14	10	0	6	13

As can be seen from the figure, the 56 bit key [22] with parity bits removed is divided into two parts, 28 bits in each part, and the left and right parts are shifted to the left in each round. See Table 4 for the specific shift.

3.4. Working Principle of S-Box [23]. S-box takes 6 bits as input and 4 bits as output. Now take S1 as an example to illustrate its process. S1 is shown in Table 5.

The S-box can be regarded as a 4×6 matrix, which changes the originally input 6-bit data into 4-bit data. There are 8 S-boxes in total. The binary number composed of the first and last bits of the data is the row of the S-box, and the binary number composed of the middle 4 bits is the column of the S-box.

Assuming that the input is $A = 100110$, the number represented by 0011 is a number between 0 and 15, that is, 3 in hexadecimal, representing the third column of s box. The number represented by 10 is a number between 0 and 3, that is, 2 in decimal system. In the second row and the third column of S, find a number 7, which can be represented by a 4-bit binary number, 0111, and you can get the output of the first S box.

RSA is an encryption algorithm based on public key mechanism. Each user has two passwords, one public K_e and

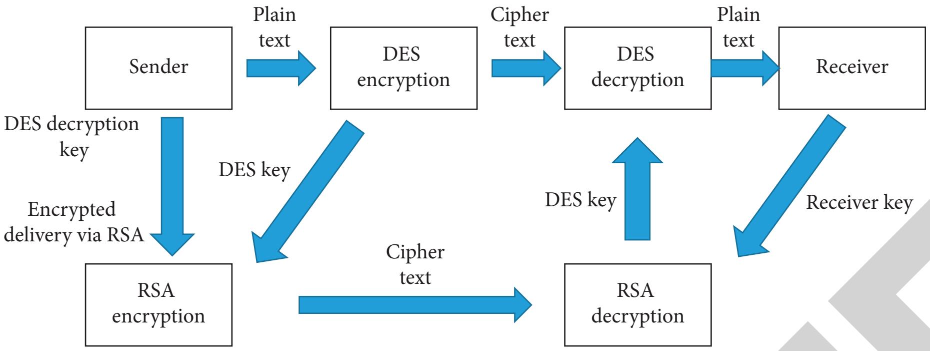


Figure 7: Schematic diagram of hybrid encryption algorithm.

one confidential K_d. For plaintext encryption, either password can be used, but another password must be used for decryption. The encryption/decryption algorithm is public, but the algorithm is irreversible. Key generation: select two large prime numbers p and q, calculate: $n = p * q$ (public), Euler function $\varphi\ (n) = (p-1)\ (q-1)$, e and $(p-1)$ are required to be coprime with $(q-1)$, and then the Euclid algorithm is used to calculate the decryption key D, which satisfies $\mathrm{de} = 1\ (\mathrm{mod}\Phi(n))$。 where n and d are also coprime. The numbers e and n are the public key and d is the private key. The numbers p and q are no longer needed and must be discarded. Do not let anyone know. Encryption method: (1) when encrypting data, m (binary representation) is divided into equal-length data blocks $m_1, m_2, \ldots, m_i$, block length s, where $2S \leq N$, S is as large as possible. (2) The corresponding password is: $c_i = m_i e(\mathrm{mod} n)$.

First, the user can show everyone the access key. Anyone can use this public encryption key [24] to communicate privately with the user. No one can decrypt the encrypted text except the recipient who has the decryption key. In this way, the distribution strategy becomes "public key distribution." Public key cryptography allows users to print or share their keys first so that anyone can see them. Thus, aliens can provide users with confidential communications. Unlike the gamma ray storage system, both parties must agree on a unified key in advance. Finally, public key encryption not only improves the traditional encryption process but also provides an application that the traditional encryption process does not have: this is the digital signature. Public encryption is not perfect, and there are still some issues that need to be addressed. Moreover, the known public encryption methods have a large amount of computation and slow speed of encryption and decryption. The following are the weaknesses of public encryption methods:

(1) When detecting values, the huge computer overhead is the fatal weakness of RSA algorithm. Even if we use VLSI to realize RSA system, its application scope is limited and restricted.

(2) Although increasing the number of bits of $r = p * q$ will undoubtedly greatly improve the security of RSA cryptosystem, its computing overhead will increase exponentially, resulting in infeasibility in fact.

(3) Simmons and Norris have proved that if p is not carefully selected, g can decipher RSA cryptosystem without decomposition. They found that for some keys, re-encrypting the ciphertext for a few seconds can restore the original message.

(4) The actual analysis shows that increasing the difference between the two selection primes p and q may reduce the numerical result of $p * g$ de-product term, which will have an adverse impact on the security of RSA cryptosystem.

3.5. Implementation of Hybrid Encryption Algorithm based on the Combination of DES and RSA Algorithm. Although DES algorithm encrypts a large amount of data slowly, it can ensure security and carry out digital signature. Although encryption is fast, it has the security problem of key management. We use encrypted plaintext data and encrypted key. In this way, the plaintext can still be encrypted very quickly, its key is encrypted, and the security is also well guaranteed. Therefore, the hybrid algorithm can solve the security problem well.

The principle of using the hybrid algorithm is shown in Figure 7. The elliptical text file is first encrypted by an algorithm, then the encryption key, and the encrypted text and encryption key are sent to the recipient [25]. After the receiver receives the information, it first uses the decryption key. The keys for encryption and decryption are the same, so you get the key and then decrypt the ciphertext to get the plaintext.

It should be noted that in the specific implementation process, RSA needs to generate large prime numbers, so the operation of large numbers needs to be used in RSA algorithm, but the ordinary compiler can only support 64 bit integer operation. Therefore, in the algorithm, this paper establishes a large number library to solve this problem. Suppose that for a 32-bit compiler, the maximum number that can be supported is 232, expressed in hexadecimal, which is 0xffffff. For a 1024 bit number, if converted to 0xffffff it becomes 32 bits. The increase of hexadecimal is used to reduce the number of bits of data for convenient storage. For example, there is a binary number of 10010001, which becomes 91 after being converted to hexadecimal, and the previous 8 bits are also reduced to 2 bits. In 0xffffff [26], the value of each bit is 0-0xfffffff.

Specific implementation process of hybrid algorithm:

(1) Firstly, the algorithm is used to generate large prime numbers p and q and determine n, e and d, where p, q and d are hexadecimal numbers;

(2) For key encryption, you need to enter an 8-bit key and encrypt it with DES

(3) The encryption time of the whole file is represented by 1.txt, and the encryption algorithm is used to encrypt the whole file [27, 28];

(4) File decryption: before decrypting the file, decrypt the RSA encrypted key, get the des key, and then decrypt the ciphertext. The decrypted ciphertext is saved in 3.txt.

The hybrid encryption system is an encryption module designed to realize the file encryption function of the digital rights management system [29, 30]. The system uses des as the symmetric key algorithm and RSA as the public key algorithm. The data are first encrypted using the DES algorithm, and then the des key is encrypted using the RSA algorithm. The main features of the system are as follows:

(1) Two encryption methods for files are provided, namely hybrid encryption and des encryption.

(2) The system can also check the authenticity of the key, since the encrypted ciphertext key is still stored in the file during the encryption process. When decrypting, first decrypt the ciphertext key with the current key. If the received key has the same meaning as the current key, the current key must be valid.

(3) The hybrid encryption module of the hybrid encryption system also has the function of detecting RSA key errors, which depends on the length of the decrypted DES key, because that is the RSA key path, the length of the decrypted DES key must exceed 16 bytes.

(4) The DES encryption method of the system can realize one-level DES encryption (standard DES encryption) and three-level DES encryption. Depending on the length of the key, the encryption process is automatically selected. Standard DES encryption is used when the long key is in 64 objects. When the key length exceeds 64 bits, the system sets a second key and enables DES encryption three times, and the key length can reach 112 objects.

If a broad group $(Q,^{\oplus})$ satisfies that for any $a, b \in Qa, b$, the equations $a^{\oplus}r = b$ and $y^{\oplus}a = b$ have unique solutions on Q, then $(Q,^{\oplus})$ is called a pepper group, and the cardinality |Q| of set Q is called the order of quasi group $(Q,^{\oplus})$. For a quasi group $(Q,^{\oplus})$, $(Q,^{\oplus})$, we define six binary operations $^{\oplus}(1,2,3),^{\oplus}(1,3,2)^{\oplus}(2,3,1)^{\oplus}(2,3,1)^{\oplus}(3,1,2)$ on Q. As follows: $a^{\oplus}b = c$, see formulas (1) and (2).

$$a^{\otimes}(1,2,3)^{b} = c,$$

$$a^{\otimes}(1,3,2)^{c} = b, \tag{1}$$

$$b^{\otimes}(2,1,3)^{a} = c,$$

$$\begin{aligned} b \otimes (2,3,1)^{c} &= a, \\ c \otimes (3,1,2)^{a} &= b, \\ c \otimes (3,2,1)^{b} &= a. \end{aligned} \tag{2}$$

Obviously, the set Q with respect to these six binary operations constitutes the conjugate of six quasi groups $(Q\oplus_{(i,j,k)}), \{i, j, k\} = \{1,2,3\}$, which is called quasi group $(Q,^{\oplus})$. If a quasi group $(Q,^{\oplus})$ satisfies $a \otimes b = c \Rightarrow b \otimes a = c$, then quasi Group $(Q,^{\oplus})$ is commutative, and if a quasi group $(Q,^{8})$ satisfies $a \otimes b = c \Rightarrow a \otimes c = b$, then quasi group $(Q,^{\oplus})$ is commutative. If a quasi group $(Q,^{\oplus})$ is commutative, its (2.1.3)-conjugate quasi group $^{\oplus}(2,1,3)$ can be known by the same principle. If a quasi-group $(Q,^{\oplus})$ is postcommutative, its (1,3,2)-conjugate quasi-group $(Q, Oqu, a) = (Q,^{\oplus})$ can be known. Given a commutative quasi-group $(Q,^{8})$, it is obvious that its (3,1,2) conjugate quasi-group $^{\oplus}(1,3,2) = (Q,^{\oplus})$ is postcommutative. Vice versa, if we give a postcommutative quasi group $(Q,^{\oplus})$, we can also get that its (2,3,1) conjugate quasi group $\oplus(2,3,1)$ is commutative. If $(Q,^{8})$ is a postcommutative quasi group, it satisfies the following properties, as shown in formulas (3) and (4):

$$a \otimes (a \otimes b) = b, \tag{3}$$

$$\forall a, b \in Q. \tag{4}$$

Suppose $A = \{x_1, x_2, \ldots x_n\}$ is a set composed of one character, $(A, \bullet)$ is a postexchangeable quasi group defined on A, and A^{+} is a set composed of all nonempty character declarations in set A [31, 32]. The character declaration transformations E and D. Based on the operation, $\odot$ are defined as follows as equations (5) and (6):

$$E(x_1 x_2 \cdots x_l) = y_1 y_2 \cdots y_t, D(y_1 y_2 \cdots y_t) = z_1 z_2 \cdots z_l, \tag{5}$$

$$\begin{cases} y_1 = a \cdot x_1 \\ y_{i+1} = y_i \cdot x_{i+1}, i = 1, 2, \ldots \ell - 1 \end{cases}, \tag{6}$$

where $\alpha \in Q$ ∘

The theorem makes E and D as defined earlier, then E and D are bijective and have formula (7) for any $X = x_1 x_2 \cdots x\ell \in A+$:

$$D(E(X)) = X. \tag{7}$$

That is, $D = E^{-1}$ is the inverse of E.

It is easy to deduce from the formula that if E and D are bijection, there is and $\begin{cases} yi + 1 = yi\theta xi + 1, i = 1, 2, \ldots, i - 1 \\ zi + 1 = yi\theta yi + 1, i = 1, 2, \ldots, i - 1 \end{cases}$.

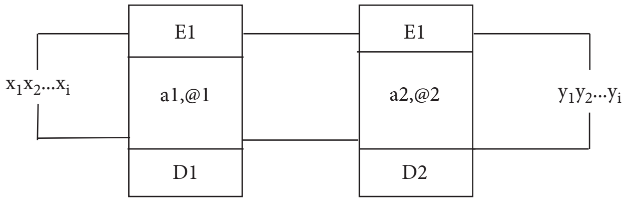


Figure 8: Synthesis of common mappings.

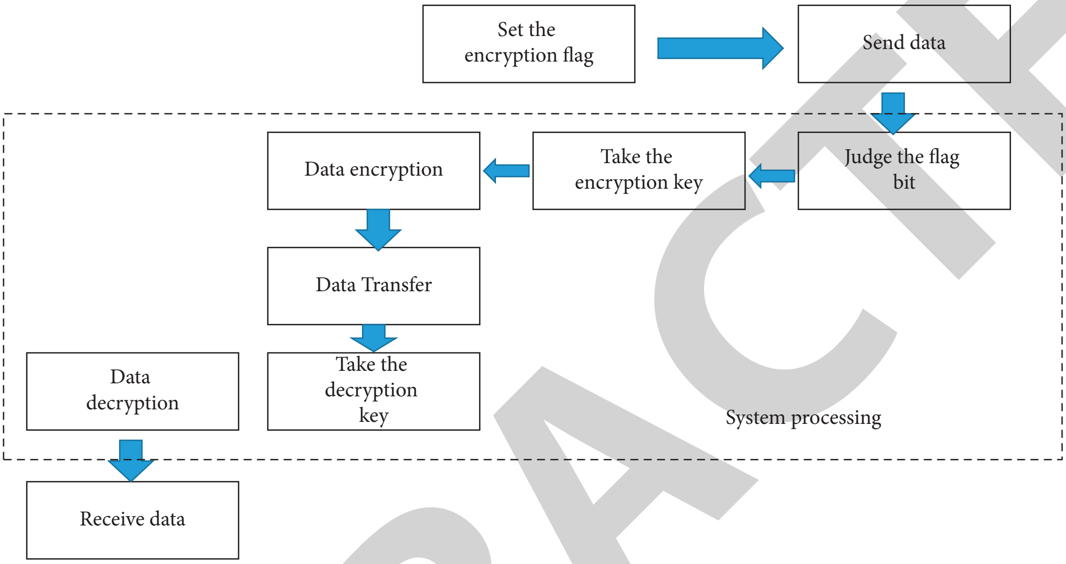


Figure 9: System implementation process.

Therefore, according to the formula $\begin{cases} zi = a\theta(a\theta x1) \\ zi + 1 = yi\theta(yi\theta xi + 1) \\ = xi + 1, i = 1, 2, \ldots, i - 1 \end{cases}$

so, $D(E(x1x2\ldots xi)) = x1x2\ldots xt$

For character set a, a postexchangeable quasi group $\odot$ can be constructed. Through the aforementioned method, we can define transformation e for encryption and transformation D for decryption respectively, and then give an initial value B to form an encryption unit (A, $\odot$, α, E) and a decryption unit (A, $\odot$, α, D). If given n postcommutative quasi group operations $\odot_1$, $\odot_2$, $\odot_3$,. . ., $\odot_N$, based on set a, map E_1, E_2, E_3, . . ., E_N, D_1, D_2, D_3,. . ., D_N according to the formula, and then select the fixed element α_1, α_2, α_3,. . ., $\alpha_N \in A$. So that E_k, D_k, $\odot_k$, α_k correspond one-to-one, $1 \leq K \leq n$. Then we get n encryption units and decryption units, as shown in formula (8);

$$\begin{aligned} E &= E^{(n)}_{a\times ax-1} = E_n o E_{n-1} o \cdots o E_1, D \\ &= D^{(n)}_{a\times an-1} = D_n o D_{n-1} o \cdots o D_1. \end{aligned} \tag{8}$$

Here O is the synthesis of ordinary mappings, and it is not required that all quasi groups must be the same. As described earlier, E is connected by n encryption units, and D is connected by n decryption units, as shown in Figure 8.

Let $\odot_1$, $\odot_2$, $\odot_3$, . . ., $\odot_N$ be n (postexchangeable) quasi groups based on A. As mentioned earlier, let's call multivariate groups post $(A, \{\sigma_1, \sigma_2, \ldots, \sigma_n\}, \{a_1, a_2, \ldots, a_n\}, E, D$ exchangeable quasi group cryptosystems based on set A.

4. Experimental Discussion

Encryption and decryption of the data of the digital education resources co construction and sharing system. First, the corresponding flag bit can be set in the header of the transmitted data packet. The flag bit can be set to 1, indicating that the flag bit to be encrypted is 0, indicating that encryption is not required. When the system receives the data packet to be transmitted, it will automatically judge the flag bit, encrypt the data to be encrypted, and decrypt the data after transmission. Then submit it to the program. The process is shown in Figure 9.

This process can represent two different encrypted transmission processes: one is to use Des symmetric key to encrypt and decrypt plaintext; the other is to use RSA asymmetric key to encrypt and decrypt Des session key and digital signature.

We adopt the implementation of three-tier distributed object architecture, namely client layer, server layer, and database access layer [33]. Further subdivide and refine the three-tier structure. Data encryption is to ensure the security of communication, so the encryption module should be in

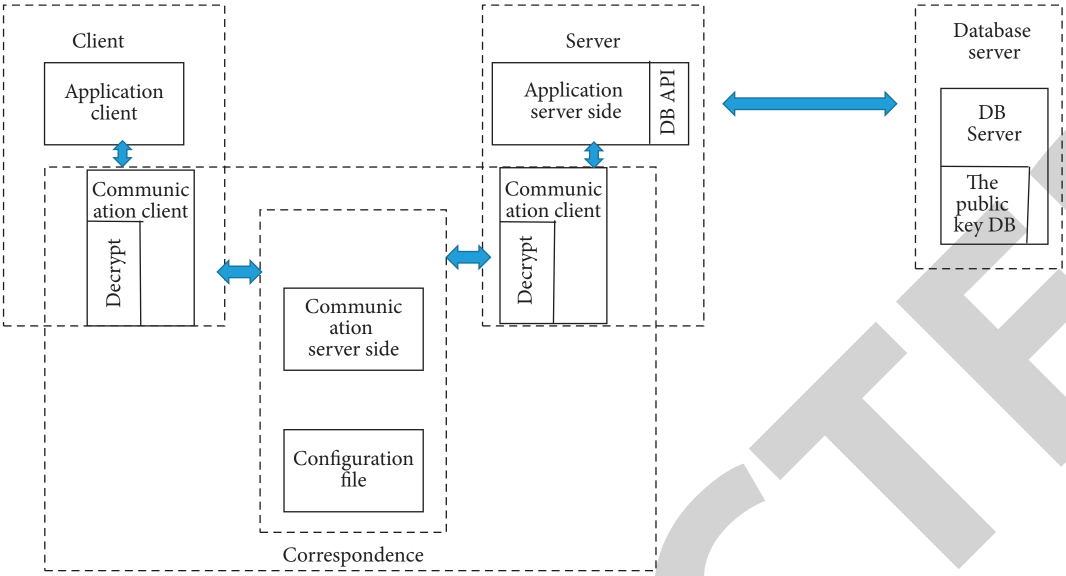


Figure 10: Detailed three-layer structure.

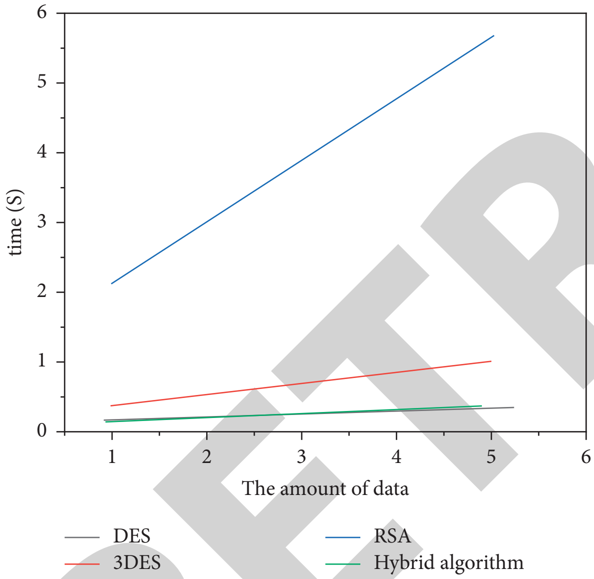


Figure 11: Broken line diagram of encryption algorithm time.

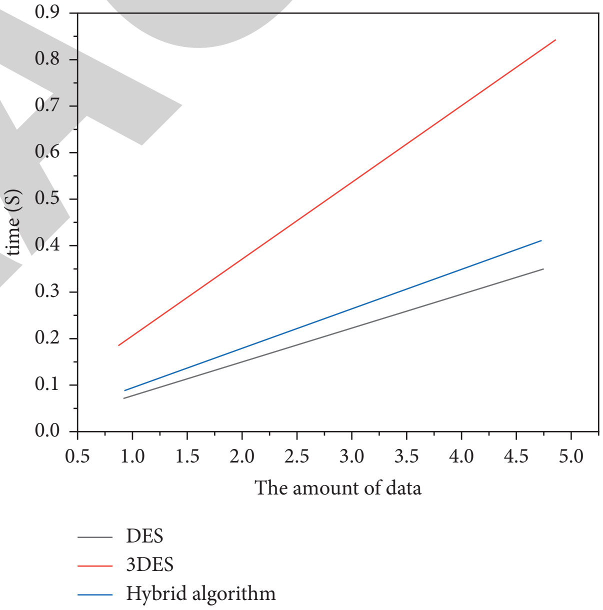


Figure 12: DES, 3DES, and hybrid algorithm.

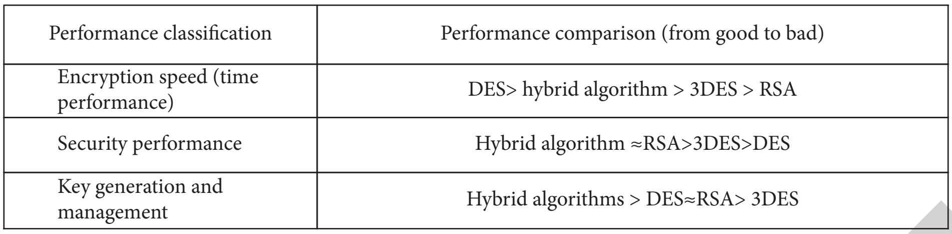
the communication program module. As shown in Figure 10.

The encryption and decryption module is in communication. Encryption and decryption programs of DES and RSA algorithms and digital signature programs are installed on each client and server. The data encrypt the data and digital signature at one end, decrypt and verify the end-to-end encryption method of the digital signature at the other end, so it is safe and confidential in the transmission of the whole communication channel. The database is placed on the server side. There is a public key database in the database, which specially stores the public keys of each transaction party. Each legitimate user can enter the database through his own password and get the other party's public key.

Through the previous theoretical analysis and program implementation, we have a certain understanding of the principle and performance of the hybrid algorithm. Next, we will compare the algorithm efficiency, algorithm security, key management, and other aspects in the sharing and co-construction of digital educational resources, and comprehensively analyze the performance of the algorithm.

4.1. Business Hours. We learned that the DES algorithm has the fastest encryption speed and is necessary to encrypt large amounts of data, while the speed of the DES algorithm depends on the number of keys. The broken line graph of encryption time of these algorithms is shown in Figure 11.

From the figure, we can see that the RSA algorithm takes much longer than other algorithms. To better evaluate the



Performance classification	Performance comparison (from good to bad)
Encryption speed (time performance)	DES> hybrid algorithm > 3DES > RSA
Security performance	Hybrid algorithm ≈RSA>3DES>DES
Key generation and management	Hybrid algorithms > DES≈RSA> 3DES

Figure 13: Algorithm performance comparison.

performance of DES, 3DES, and hybrid algorithms, we compare the three algorithms in one graph, as shown in Figure 12.

From the Figure 12, we find that the main difference between the hybrid algorithm and the DES algorithm is in encrypting the 64 bit des key. When the amount of data is large, the time of encrypting the key is very small compared with the overall time. From this, we can conclude that compared with DES, the time of 3DES algorithm increases exponentially.

4.2. Safety Performance. The RSA algorithm with 1024 bits as the public key encrypts the key of DES, and its security is also very high, which is almost impossible to be cracked. Therefore, the security of the hybrid algorithm is relatively high.

4.3. Key Management. RSA algorithm is difficult to generate key, and it is difficult to achieve the effect of one encryption for data at a time. The DES algorithm is different. The 64 bit key is very easy to generate, but the key must be distributed before communication, and the key must be changed from time to time. In this way, the key management consumes a lot of system overhead. 3DES also has the problem of key management due to the use of multiple keys.

In order to more intuitively reflect the performance of each algorithm, we rank the performance of several algorithms in the table, as shown in Figure 13.

5. Conclusion

Digital education resources include all kinds of audio, video, courseware, text and other resources, as well as various management software, database resources, and hardware resources. Teaching resources have the characteristics of large number, different forms, and complex structure, as well as the defects of DES and RSA digital information encryption. This paper proposes a hybrid digital information encryption algorithm based on the combination of DES and RSA to solve the security problem of digital education resources. The results show that compared with traditional DES, RSA, and 3DES encryption, hybrid encryption can effectively provide DES encryption speed while meeting the requirements of RSA security and key management and effectively solve the collaborative security problem. Share digital educational resources.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

References

[1] A. Almeida-Santana, T. David-Negre, and S. Moreno-Gil, “New digital tourism ecosystem: understanding the relationship between information sources and sharing economy platforms,” *International Journal of Tourism Cities*, vol. 6, no. 1, pp. 1–7, 2020.

[2] Z.-F. Liu, Y.-Z. Zhang, C.-B. Yang, Z.-G. Huang, C.-X. Zhang, and F.-G. Xie, “Generalized distributed four-domain digital twin system for intelligent manufacturing,” *Journal of Central South University*, vol. 29, no. 1, pp. 209–225, 2022.

[3] P. Byron, “Apps are cool but generally pretty pointless: LGBTIQ+ young people’s mental health app ambivalence,” *Media International Australia*, vol. 171, no. 1, pp. 51–65, 2019.

[4] N. N. Evtikhiev, V. V. Krasnov, D. Y. Molodtsov, V. G. Rodin, R. S. Starikov, and P. A. Cheremkhin, “Application of a digital micromirror device for optical encryption with time integration,” *Optoelectronics, Instrumentation and Data Processing*, vol. 56, no. 2, pp. 134–139, 2020.

[5] H. Tian, L. Wei, Y. Yao, Z. Zeng, X. Liang, and H. Zhu, “Analysis of the anti-inflammatory and analgesic mechanism of shiyifang vinum based on network pharmacology,” *Evidence-based Complementary and Alternative Medicine*, vol. 2021, no. 3, pp. 1–10, 2021.

[6] K. Mirkovski, R. M. Davison, and M. G. Martinsons, “The effects of trust and distrust on ICT-enabled information sharing in supply chains,” *International Journal of Logistics Management*, vol. 30, no. 3, pp. 892–926, 2019.

[7] H. Chen and H. Ma, “The cooperation mechanism of the formal and informal recyclers based on information sharing,” *Journal of Digital Information Management*, vol. 3, no. 3, pp. 209–224, 2021.

[8] J. Dong, H. Li, Y. Wang, and Y. Zhang, “Characteristics and monitoring-based analysis on deformation mechanism of jianshanying landslide, guizhou province, southwestern China,” *Arabian Journal of Geosciences*, vol. 14, no. 3, p. 184, 2021.

[9] Yohei and Seki, “Sharing information of mfca in the supply chain: a study based on the theory of inter-organizational management accounting,” *The Journal of Management Accounting, Japan*, vol. 27, no. 1, pp. 19–34, 2019.

[10] J. Lee, H. Lee, and J.-G. Park, “Exploring the impact of empowering leadership on knowledge sharing, absorptive

capacity and team performance in it service," *Information Technology & People*, vol. 27, no. 3, pp. 366–386, 2014.

[11] P. Amat, W. Puech, S. Druon, and J. P. Pedeboy, "Lossless 3d steganography based on mst and connectivity modification," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 400–412, 2010.

[12] R. Lu and Z. Cao, "Erratum to "Non-interactive deniable authentication protocol based on factoring"[Computer Standards & Interfaces 27 (2005) 401-405]," *Computer Standards & Interfaces*, vol. 29, no. 2, p. 275, 2007.

[13] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-edge: a lightweight authentication protocol for iot devices in an edge-cloud environment," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 57–63, 2022.

[14] Z. G. Zhang, I. Bothe, F. Hirche et al., "Interactions of primary fibroblasts and keratinocytes with extracellular matrix proteins: contribution of $\alpha 2\beta 1$ integrin," *Journal of Cell Science*, vol. 119, no. 9, pp. 1886–1895, 2006.

[15] A. Shahidinejad, M. Ghobaei-Arani, and L. Esmaeili, "An elastic controller using colored petri nets in cloud computing environment," *Cluster Computing*, vol. 23, no. 2, pp. 1045–1071, 2020.

[16] A. Dakhil, Z. Naji, and O. Al-Salih, "The Applicability of Using Automation in Construction in Iraq," *Basrah Journal for Engineering Sciences*, vol. 21, no. 2, 2021.

[17] A. Mazidi, M. Golsorkhtabaramiri, and M. Y. Tabari, "Autonomic Resource Provisioning for Multilayer Cloud Applications with K-Nearest Neighbor Resource Scaling and Priority-Based Resource Allocation," *Software: Practice and Experience*, vol. 8, 2020.

[18] S. Zhang, B. Huang, X. Song, T. Zhang, H. Wang, and Y. Liu, "A high storage density strategy for digital information based on synthetic dna," *3 Biotech*, vol. 9, no. 9, p. 342, 2019.

[19] S. N. Kersey, "Student perceptions on teaching and learning using open educational resources in college calculus," *Journal of Computers in Mathematics and Science Teaching*, vol. 38, no. 3, pp. 249–265, 2019.

[20] J. Wang, D. E. Tigelaar, and W. Admiraal, "Connecting rural schools to quality education: rural teachers' use of digital educational resources," *Computers in Human Behavior*, vol. 101, no. Dec, pp. 68–76, 2019.

[21] J. Li, M. Lan, Y. Tang, S. Chen, F.-Y. Wang, and W. Wei, "A blockchain-based educational digital assets management system," *IFAC-PapersOnLine*, vol. 53, no. 5, pp. 47–52, 2020.

[22] V. Konrad and E. Brunet-Jailly, "Approaching borders, creating borderland spaces, and exploring the evolving borders between Canada and the United States," *Canadian Geographer/Geographe Canadien*, vol. 63, no. 1, pp. 4–10, 2019.

[23] L. Shi, *The Effects of Interactive AI Design on User Behavior: An Eye-Tracking Study of Fact-Checking COVID-19 Claims*, https://arxiv.org/abs/2202.08901, 2022.

[24] J. D. Teachman, "Family background, educational resources, and educational attainment," *American Sociological Review*, vol. 52, no. 4, p. 548, 1987.

[25] S. Dietze, S. Sanchez-Alonso, H. Ebner, H. Q. Yu, D. Giordano, and I. Marenzi, "Linked education: interlinking educational resources and the web of data," *Program Electronic Library & Information Systems*, vol. 47, no. 1, pp. 261–274, 2016.

[26] V. Camel, M.-N. Maillard, N. Descharles, E. Le Roux, M. Cladière, and I. Billault, "Open digital educational resources for self-training chemistry lab safety rules," *Journal of Chemical Education*, vol. 98, no. 1, pp. 208–217, 2021.

[27] P. Lafitte, K. Lince-Barrere, M. Marchand, and J. D. Cohen, "Le numérique au service de l'ETP: à propos d'un programme polypathologies," *Education Thérapeutique du Patient-—Therapeutic Patient Education*, vol. 12, no. 1, Article ID 10401, 2020.

[28] S. Y. Al-Imamy, "Blending printed texts with digital resources through augmented reality interaction," *Education and Information Technologies*, no. 9, pp. 1–16, 2020.

[29] A.-a. Silamut and S. Petsangsri, "Self-directed learning with knowledge management model to enhance digital literacy abilities," *Education and Information Technologies*, vol. 25, no. 6, pp. 4797–4815, 2020.

[30] M. V. Makokotlela, "An e-portfolio as an assessment strategy in an open distance learning context," *International Journal of Information and Communication Technology Education*, vol. 16, no. 4, pp. 122–134, 2020.

[31] S. Burkhart and D. Craven, "P161 digital workbooks to develop and evidence learning in a flipped nutrition classroom in higher education," *Journal of Nutrition Education and Behavior*, vol. 52, no. 7, pp. S92–S93, 2020.

[32] H. Jacinto and S. Carreira, "Digital tools and paper-and-pencil in solving-and-expressing: how technology expands a student's conceptual model of a covariation problem," *Journal on Mathematics Education*, vol. 12, no. 1, pp. 113–132, 2021.

[33] B. Pepin, "Connectivity in support of student co-design of innovative mathematics curriculum trajectories," *ZDM—Mathematics Education*, vol. 53, no. 6, pp. 1221–1232, 2021.