Eng Int Syst (2025) 2: 141–153

Engineering
Intelligent Systems

Coupling of Image Authentication and Identification of Logistics Blockchain Based on Cloud Computing

Shuting Liu[1]*

[1] *School of Information and Business, Shaanxi Energy Institute, Xianyang, 712000, Shaanxi, China*

There is a one-to-one correspondence between logistics information and express order numbers. If the logistics information is directly disclosed in the blockchain, it is easy to infer the addresses of the recipient and the sender, and the personal privacy of the user cannot be guaranteed. Once information leakage or information theft occurs, serious consequences can ensue. With regard to the protection of digital image copyright, transaction deposit and digital image copyright authentication in the management of existing logistics blockchain image authentication and identification, user privacy protection, personalized recommendation, etc., in this study, digital watermarking, blockchain technology and recommendation technology is applied to digital image transaction management. We propose an intelligent recommendation algorithm for personalized digital images based on weighted TextRank and SOM. A logistics blockchain image transaction management system is designed that can solve the current problems in the cloud computing environment. It benefits both buyers and sellers. The median filter attack experiment found that after the image to be detected is attacked by the median filter with the filter window size ranging from 2 to 99, all of the NC values of the extracted robust watermark are 1. The NC values of the extracted semi-fragile watermarks range from 0.9696 to 0.8909, and the TAF values of the semi-fragile watermarks range from 0.0676 to 0.1808. The trusted framework based on blockchain for outsourcing data entry (TFBO) in this paper is not only credible but also practical. This study helps to solve the privacy protection problem in the logistics process and improve the user's trust in the logistics company.

Keywords: logistics blockchain, image authentication recognition, cloud computing, user privacy protection

1. INTRODUCTION

With the advent of the Internet era, an increasing number of logistics companies and e-commerce companies have developed rapidly, and the economic advantages brought about by the timeliness and importance of goods distribution has become more and more prominent. The credibility level of China's traditional logistics industry is not high, mainly due to the fact that the data is not well protected. It can be tampered with easily, can be lost, and is easy to steal. The decentralization and distributed accounting features of blockchain technology constitute a new and disruptive computing model. It provides data transparency, data cannot be altered, and it requires anti-counterfeiting certification, all of which are needed by the logistics industry. All data on the blockchain-based logistics platform is stored in a stable and credible big data warehouse, and these data are open, transparent and reliable on the chain. This paper starts by explaining the most important consensus algorithm in the blockchain, and tries to alleviate and solve issues related to data security, tampering, loss, and theft to the greatest extent, so as to promote the application and development of blockchain technology in the cloud computing environment.

*Corresponding author's Email: lsht1984@126.com

During multi-level logistics blockchain transportation, user information is stored in the database in plaintext, which is prone to privacy leakage. Suryalakshmi discussed the importance of blockchain in logistics and the related opportunities and challenges [1]. In regard to the feasibility of blockchain technology in the logistics service supply chain, Dai constructed a logistics service supply chain model. He also studied the application of blockchain technology in logistics service management supply chain in terms of object domain, functional domain and attribute domain [2]. Younus conducted a critical review of the characteristics of the current research framework for implementing blockchain technology in logistics [3]. Midaoui proposed a method for effectively assessing and ensuring the traceability and transparency of blockchain-based transactions. In addition to a configurable system based on IoT, he also used a distributed ledger (blockchain) to take into account all required data [4]. Hackius analyzed data obtained from 24 semi-structured interviews with experts, and a large amount of secondary data. The study provides a comprehensive view of the activities of existing companies in regard to blockchain adoption [5]. However, the logistics blockchain transportation scheme they proposed does not improve user privacy protection. In this study, cloud computing is used to optimize it.

The cloud computing environment can assist in the digital transformation of cargo information. Xia proposed a scheme to support CBIR on encrypted images without leaking sensitive information to cloud servers [6]. Deng studied the trade-off between power consumption and transmission delay in fog cloud computing systems [7]. Focusing on the competitive characteristics of multi-tenant environment in cloud computing, Wei proposed a cloud resource allocation model based on incomplete information Stackelberg game (CSAM-IISG) [8] by using Hidden Markov Model (HMM). Jin devised a new attribute-based, data-sharing scheme to address this challenging problem. It is suitable for mobile userFs with limited resources in cloud computing [9]. Tsai proposed an efficient distributed mobile cloud computing service authentication scheme. This scheme provides security and convenience for mobile users to access multiple mobile cloud computing services provided by multiple service providers using only a single private key [10]. However, the cloud computing solution they proposed is not very commonly applied in the logistics industry.

Recent advancements in blockchain and cloud computing have greatly impacted logistics. Zhao et al. [11] proposed a Blockchain and Palm Scanning Integrated System for workplace access control, showcasing blockchain's role in secure data management. Mao [12] developed an IoT-based social management system, highlighting the synergy between blockchain and IoT. Additionally, Wei [13] introduced a deep learning method for image recognition on edge cloud computing, which is crucial for image authentication in logistics blockchain. These studies emphasize the potential of these technologies in improving logistics security and efficiency.

In this paper, a cloud computing-based logistics blockchain image authentication and identification method is proposed, and obtains the best decision with the least cost. By reasonably allocating computing resources, the suggested approach can minimize the total cost of users and improve user satisfaction. A pricing strategy is designed based on task requirements and server real-time resource requirements to leverage the benefits of edge server networks. It combines the average distribution and proportional distribution to allocate edge server computing power to balance the task execution time of different needs. An analysis of the traditional logistics system revealed that the data chain is incomplete, the information is easily tampered with, and information about goods and commodities is disjointed In this paper, a recommendation algorithm is proposed based on blockchain technology and combined with portrait data. A decentralized intelligent logistics platform is built to solve the problems of incomplete logistics data and easy tampering of information. The platform permanently stores the goods circulation data generated by logistics enterprises; this data cannot be tampered with, thereby providing enterprises and users with guarantees of security for data integrity and reliability. The focus of this paper is on digital image watermarking technology in the "cloud" environment. In this paper, a variety of new digital watermarking models and algorithms are proposed and implemented by means of programming tools. Also, an attack experiment was carried out on the watermarked image, verifying the feasibility and reliability of the new algorithm. If the arbitration result shows that the malicious party does have malicious behavior, it will pay 50% of the malicious party's deposit in the public account to the other party as compensation according to the pre-agreed smart contract. The TFBO does have the ability to handle malicious events. That is, it can transfer 50% of the deposit of the malicious party in the public account to the other party.

2. LOGISTICS BLOCKCHAIN IMAGE AUTHENTICATION AND IDENTIFICATION COUPLING

2.1 Logistics Blockchain

Blockchain is a chain data structure that connects blocks containing transaction data in chronological order and combines them through hash encryption technology. It is used to record transaction information and data, and to ensure the security and immutability of transactions in a cryptographic manner. This distributed ledger is available to all participants in the P2P network. After the participants calculate the accounting rights, they use encrypted signatures to add a new transaction to the existing list on the blockchain, forming a secure, continuous, and immutable chained data structure. In a blockchain network, a suitable consensus protocol must be established to ensure that any interference from adversaries can be denied by the majority of participants.

In this paper, consider that each user has only one computing task, A_i, and the user chooses the decision-making scheme with the minimum cost through calculation. The user's decision-making is set as S_n:$S_n = \{S_1, S_2, \ldots, S_n\}$, S_i represents the decision of the ith user. After calculation, if the user decides to calculate locally, then the user's decision $S_i = -1$. The local computation time of task A_i is calculated with [14]:

$$t_i^0 = \frac{R_i}{f_i^0} \tag{1}$$

The energy consumption is related to the number of CPU cycles required by the task. The energy consumed by the execution of the task A_i is calculated with [15]:

$$e_i^0 = \theta_i R_i \tag{2}$$

In the case of local computing, the final logistics cost includes the time cost and energy cost required for the task, and the final cost of the local computing task is calculated with:

$$COST_i^0 = T_1 * t_i^0 + T_2 * e_i^0 \tag{3}$$

where T_1 is the weight of logistics time, and T_2 is the weight of logistics energy.

When the user's local residual energy cannot meet the energy demand required by the user to perform the task, or the cost of local computing is too high, the user will completely transfer the task to the edge server, and the edge server will perform the calculation. The user's decision $S_i = j$, j is the target server that the user decides to unload after calculation, and the task is calculated on this server with the lowest cost. The calculation time of the logistics blockchain task is found with [16]:

$$t_{i,j} = \frac{R_i}{f_j^S} \tag{4}$$

In this paper, combined with the two methods of average distribution and proportional distribution, part of the computing power is distributed evenly to each task according to the number of tasks. It then allocates another part of the computing power to each task in proportion to the task demand, and the calculation process is as follows [17]:

$$\rho_i^j = \frac{R_i}{2(R_{total} + R_i)} + \frac{1}{2N^j} \tag{5}$$

In the logistics industry, blockchain technology can be used to permanently preserve important data that cannot easily be tampered with. It can thus improve the trustworthiness of the goods at every point in the logistics system. In a blockchain network, all participating nodes jointly maintain the same ledger. The ledger completely records the data generated in each link of the logistics, so the circulation data can be permanently stored in the blockchain network and these data are difficult to be tampered with. All nodes in the Ethereum network process the same smart contracts, and the status of these smart contracts is recorded on the public blockchain ledger, resulting in poor system efficiency. It is precisely due because of the inadequate performance of Ethereum's consensus algorithm that the network is blocked and transactions are delayed. However, in the blockchain system, a large amount of data information generated within a certain period of time through cryptography can be processed, and then is packaged and stored in a block.

In the blockchain network, the data exchange between any nodes is transparent and executed in a trusted environment. The generation of new blocks in the blockchain is supervised by all participating nodes. Once the new block is verified, it will be permanently stored, and the nodes in the network can call the public interface to access the data at any time. The operation of the entire job chain of the blockchain is jointly maintained by all participating nodes. Any node can upload, download and access data, and the generation of each block requires all node authentication, so the entire job chain must be jointly maintained by the nodes. Since the blockchain adopts a distributed architecture, each participating node can be regarded as a data warehouse. It also enables data exchange between nodes [18].

2.2 Image Authentication and Recognition

The logistics information collection system based on the mobile platform uses the image processing technology of numbers and English characters, and a convenient and safe solution is proposed. The staff of the logistics management company use the mobile phone installed with the logistics information collection software to take pictures of the local cargo list. The system also uses the recognition software in the mobile phone to process the captured images to extract information such as the location of the goods and the current time. It then sends the information to the database of the logistics head office through a mobile phone short message, and finally the head office sends the goods circulation information to the customer's mobile phone in real time. This allows customers to easily see the flow of goods. The flow chart of logistics management is shown in Figure 1.

When using the mobile phone camera to capture the image of the cargo list, it is generally best for the user to have the mobile phone camera facing the cargo list. The list image information obtained in this way is complete, and the characters on the image are relatively uniform, so when the mobile phone processes the character image, it is convenient and quick to extract useful cargo list information. The resources it provides can be dynamically transformed and adjusted. According to the needs of each cloud computing user, the corresponding resources are obtained from the huge resource reserve pool and allocated to the users. In terms of computing, it can decompose a huge program into several subroutines running in parallel. It is handed over to different computers by the cloud distribution mechanism to calculate separately, and finally the results are aggregated and submitted to the users of cloud computing services. These advantages make cloud computing services one of the most valuable services in the current Internet industry.

In order to ensure the quality of the image and the concealment of the watermark information, the watermark must not be recognized by the naked eye. And after a certain attack (such as shearing, rotation, compression, etc.), the watermark signal continues to exist. In order to ensure the sensitivity to tampering, when image watermarking technology is used to authenticate image content, fragile watermarks are usually used, although these have the lowest stability. Whether it is illegal copying or illegal tampering, the ultimate purpose of digital image pirates is to use the important information that is contained in the boundary points of the image. If the information of these boundary positions is destroyed, the tampered image will also lose its practical

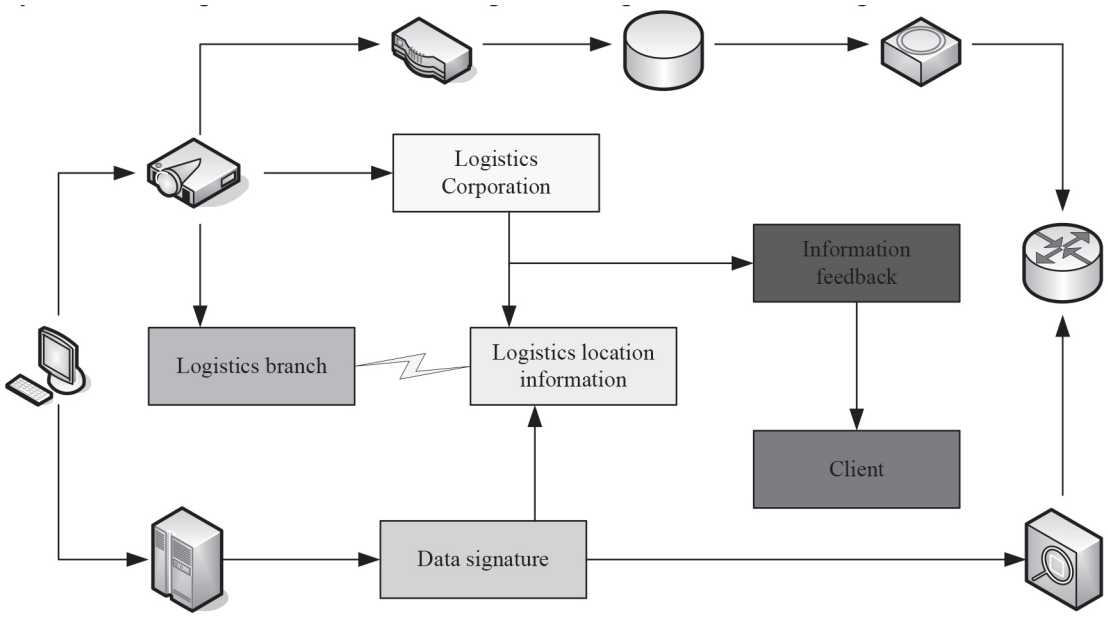

Figure 1 Flow chart of logistics management.

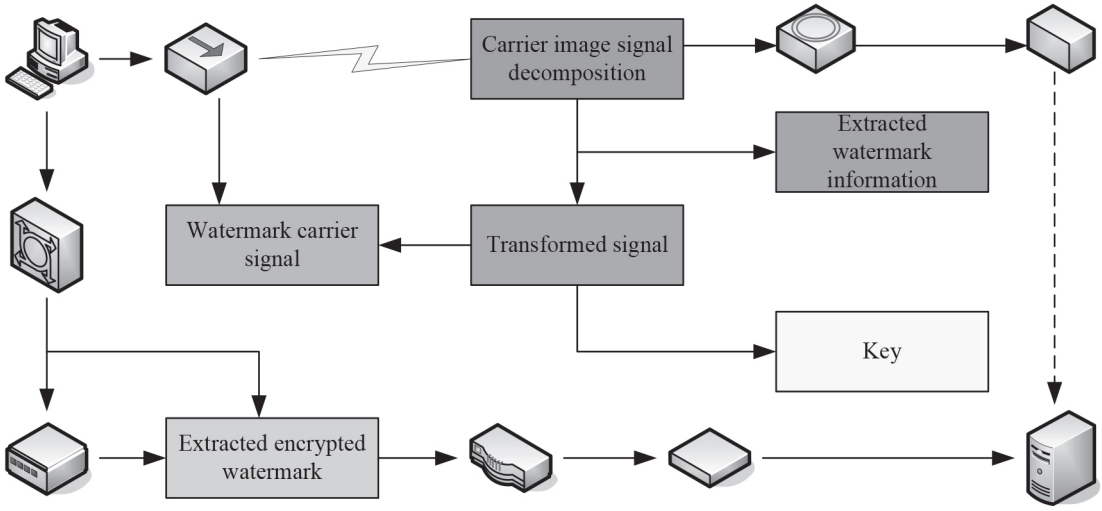

Figure 2 Digital image watermark extraction process.

significance. Therefore, the digital watermarking algorithm based on boundary information has good stability and is the research focus of digital watermarking technology.

In general, watermarks embedded in digital images comprise copyright, author's name, affiliation and other information identifying ownership. This requires that the watermarked carrier image be able to still detect the watermark information under the condition of compression, transmission and even tampering. This is the main purpose of embedding robust digital watermarks. However, sometimes the watermark needs to be sensitive to signal changes and be able to locate the changes. In these cases, a fragile watermark needs to be embedded. When embedding a watermark, the embedded content can be either text or image. Usually, these words and images mark the ownership of digital works. Such watermarks are known as 'meaningful watermarks'. In practical applications, even if the meaningful watermark is damaged, its actual meaning can still be deduced from its appearance. However, once the meaningless watermark is destroyed, it completely loses its identification function. One can only determine whether there is watermark information by counting the correct rate of the watermark sequence, which is prone to missed detection and false detection. In general, meaningless watermarks have larger embedding space than meaningful watermarks. The digital image watermark extraction process is shown in Figure 2.

Peak signal-to-noise ratio is a common criterion for measuring digital image watermarking in the coupled model of image authentication and recognition in logistics blockchain. It is used to describe the error between the watermark image and the original carrier image, and its formula is as follows [19]:

$$\mathrm{PSNR} = \log \frac{D^2 MN}{\sum (I(x, y) - I'(x, y))} \tag{6}$$

where D is the maximum value of the pixel, M and N are the number of pixels in the row direction and the number of pixels in the column direction of the image, respectively.

Assuming that the lengths of the two watermark signals $x(m)$ and $y(n)$ are M and N, respectively, there are [20]:

$$NC = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N} x(m)y(n)}{x(m)^2 y(n)^2} \tag{7}$$

Let $f(x, y)$ be the pixel value matrix of the $M \times N$ pixel image, and x, y are the pixel coordinates, then the discrete cosine transform is [21]:

$$f(0,0) = \frac{1}{\sqrt{MN}} \sum_{x=1}^{M+1}\sum_{y=1}^{N+1} f(x, y) \tag{8}$$

The least effective embedding algorithm consists of replacing the least significant bit plane with watermark information, with the amount of watermark information being [22]:

$$\sigma = \tag{9}$$

For the discrete wavelet transform (DWT) of the signal $f(t)$ in the coupled model of logistics blockchain image authentication and recognition, it can be expressed as [23]:

$$F_{j,k} = \langle f, \tau_{j,k} \rangle \tag{10}$$

The distance between any two pixels in the coupled model of logistics blockchain image authentication and recognition can be expressed as follows [24]:

$$d(i, j) = \sqrt{(x_i - y_i)^2} - \sqrt{(x_j - y_j)^2} \tag{11}$$

The pixel scrambling degree in a certain pixel set U in the logistics blockchain image authentication and recognition coupling model is expressed as follows:

$$\mathrm{SH} = \frac{\mathrm{E}(i, j)}{\mathrm{Var}(E(i, j))} \tag{12}$$

The conditional probability $P(h|v)$ of the hidden layer is expressed as [25]:

$$P(h|v) = \prod_{j}^{n=1} (c_j + \sum_{i} w_{ij}) \tag{13}$$

The logistics blockchain trains a single hidden layer neural network to minimize the output error, which is expressed as:

$$\prod_{j=1}^{N} \|o - t\| = 0 \tag{14}$$

2.3 Cloud Computing

To deal with the latency problem of cloud computing, a new concept of mobile edge computing has emerged, which is applied to mobile, wireless and wired scenarios. It integrates mobile edge computing into the sharing economy model; edge server nodes with idle computing resources are called resource providers. They contribute their computing resources to acquire profits. Idle computing equipment may be personal computers, computer rooms, servers, etc. Those with resource requirements are called 'resource demanders' and apply for computing resources offered by resource providers. The general digital signature process involves the information sender first generating the information digest through the SHA one-way encryption function. It then uses the private key to encrypt the message digest to form a digital signature, and then sends the message and its digital signature to the receiver. The receiver uses the SHA one-way encryption function to generate a digest, decrypts the received digital signature with the sender's public key to obtain a digest, and compares the two digests to see if they are consistent. Digital signatureguarantees data traceability in cloud computing, which is very important for tracking data generated by operations in the cloud computing environment. The traditional data traceability technologies applied to cloud computing often use the method of comparing the recorded data generated by executing software on physical or virtual resources with audit data for data traceability. These traditional data traceability technologies are not scalable in the cloud environment, are costly, and lack transparency. Therefore, a transparent and tamper-proof method was required to record traceability data that can operate across multiple trust boundaries and multiple stakeholders, and that maintains data traceability in the cloud computing environment. Subsequently, Block Cloud, a cloud data traceability model that applies blockchain technology, emerged.

In CloudDPoS, each user who owns the logistics blockchain cloud computing resources is defined as a node participating in the blockchain consensus process. The resources of cloud users will be mortgaged to maintain the normal operation of the blockchain system. This part of user resources will be used in the traditional DPoS consensus algorithm to determine the stake required by a node to become a block producer. In order to ensure the normal business operation of cloud users, this algorithm will reserve a certain amount of resources for cloud computing users according to the amount of logistics blockchain resources used by cloud computing users. The algorithm also establishes a greedy factor for each cloud computing user, and the user can decide how much idle resources to invest in the blockchain consensus process as equity through the set size. The calculation formula of the greedy factor of the logistics blockchain is [26]:

$$\mu_i = \sigma_{icpu} + \sigma_{imem} + w_1 * w_2 \tag{15}$$

In the formula, σ_{icpu} represents the CPU component corresponding to the greedy factor of the logistics blockchain, and σ_{imem} represents the memory component corresponding to the greedy factor.

The purpose of introducing the greedy factor is to ensure that cloud computing users will not mortgage the same resources as rights, which brings heterogeneity to the voting in the consensus. Therefore, the equity function is defined as:

$$f(R, R^U) = \sigma(R + R^U) \tag{16}$$

In CloudDPoS, for any logistics blockchain node (user) $N_i (i \in [1, k])$, the larger the value of the stake $|\alpha_i|$, the higher the probability of becoming a witness. This probability is defined as the bias probability P_i, which is calculated with [27]:

$$P_i = \frac{\theta_i}{\bigcup_{k=1}^{j} \sqrt{\theta_j}} \tag{17}$$

To ensure that the test results of the CloudDPoS consensus algorithm are more representative, the program is set to start 500, 700, 900, 1100, 1300 and 1500 threads. It simulates a blockchain environment with a corresponding number of nodes, fixes the size of each generated block to 1M, and sets the upper limit of the biased timer to a random number between 150ms and 300ms. The period of node election is set to 10min, and the running time of the control CloudDPoS consensus algorithm is 10min. It observes and records the data generated during the execution of the CloudDPoS consensus algorithm. After that, the number of nodes was fixed to 1000, the running time of the program was set to 10, 20, 30, 40, 50 and 60 min, and the obtained data were recorded and analyzed. In this paper, SPB (Seconds Per Block) is used as a measure of block speed. Its calculation formula is:

$$\text{SPB}=\frac{\text{Total } t}{\text{Total block}} \tag{18}$$

The simulation experiment program adopts multi-thread technology. It simulates the distributed multi-node environment of the blockchain by assigning multiple threads. This paper simulates the communication process between nodes by using multiple message queues. It controls the state switching between nodes by using semaphore, and stores the blockchain content of each node by using the BoltDB database. When the program starts running, it will enable a corresponding number of nodes participating in the consensus according to the user's initial settings. It initializes the blockchain information of each node. When the program is running, information such as the node serial number of the block, the hash value of the newly generated block, and the time when the block was generated (accurate to microseconds) will be printed on the screen and recorded in the log file. It serves as an important data source for this experiment.

Let the output layer of the logistics blockchain be the L layer, and the gradient of the output layer (full connection) is:

$$\partial \frac{E^i}{\alpha_{kj}} = \sigma_k^j h_k^{L-1} \tag{19}$$

In the formula, ω_{kj} is the connection weight of the $(L-1)$ layer j unit and the L layer k unit. The degree of dissimilarity between logistics blockchain images can be represented by TAF. TAF is calculated with:

$$\text{TAF}(W, \hat{W}) = \sum_{i=1}^{M \times N} W(i) \times \hat{W}(i) \tag{20}$$

where W and $\hat{W}$ represent the original watermark image and the extracted watermark image, respectively, and the size of the watermark image is $M \times N$. When TAF $= 0$, the extracted watermark image is exactly the same as the original watermark image. The degree of tampering of the watermarked image can be expressed by TAF; the larger the TAF value, the greater the degree of tampering of the watermarked image.

3. RESULTS OF THE COUPLING OF LOGISTICS BLOCKCHAIN IMAGE AUTHENTICATION AND IDENTIFICATION

As the number of attributes increases, the runtime of the system is still within a reasonable range. The algorithm proposed in this paper uses the member management center in the Hyperledger to replace the key generation center in the traditional algorithm. Secondly, it uses layered strategy encryption to encrypt ciphertext data. Compared with the traditional ciphertext policy attribute-based encryption algorithm, the proposed algorithm can shorten the user's decryption time. Because in this scheme, the user does not need to decrypt all the data, but only needs to decrypt the part of the data that he needs. Secondly, when the user sends a transaction request to the blockchain module, the blockchain calls the chaincode to respond to the request. It then returns the result of the response. As the function of the blockchain module changes, the response time of the blockchain module will also change. The response time of the blockchain module will change with the function of the module. However, the change in response time is not very different since the response time is basically maintained between 2.2 seconds and 2.4 seconds. This response time is still within a reasonable range. Therefore, this scheme can also be used in practical applications. The blockchain response and decryption time are shown in Figure 3.

Considering the efficiency of logistics transfer and the convenience of courier delivery of parcels, this paper will classify the privacy data of logistics users into security levels. The division method is shown in Table 1. The types of privacy data are divided into sender information (name, phone number, address), recipient information (name, phone number, address (excluding end address)), commodity information (mainly the goods purchased or received by the recipient information), logistics transit route (transit route information obtained by the system automatically parsed after the user submits the address information. It includes the place of departure, the place of transit and the place of arrival; the area is divided into provinces, cities, counties/districts, townships/towns), and end address information (specific community and house numbers, etc.). It is automatically parsed and segmented by the system to determine the specific point where the package arrives. The security level is divided into low, medium and high corresponding to level 1, level 2 and level 3 respectively. Visitors with different access rights access different levels of information, and the corresponding access levels are established when the access rights are set. After the classification, the data is encrypted by the AES and RSA hybrid encryption method and uploaded to IPFS for safe storage. It obtains different storage addresses, Addri, and returns the saved address hash value to the blockchain, which is convenient for users who have passed identity authentication to obtain the information.

The performance overhead in the private data hierarchical encryption mechanism is incurred mainly by the data encryption and decryption operations. This mechanism takes a specific piece of personal information as an example,

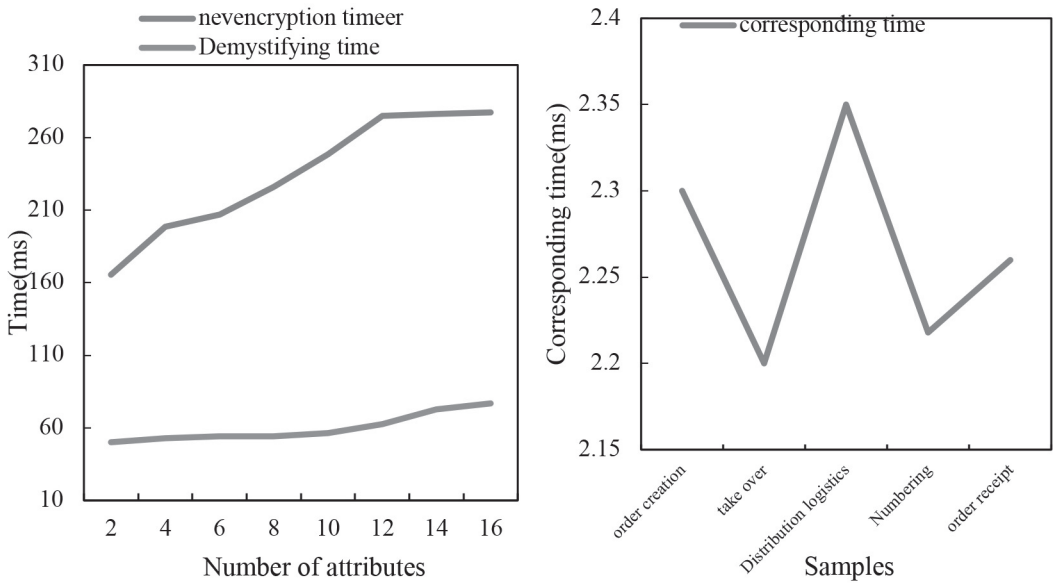

Figure 3 Blockchain response and decryption time.

Table 1 Security classification of private data.

Privacy data type	Security Level	Visitor
Logistics transit route	1 (low)	recipient, sender, recipient
recipient information	2 (high)	transfer officer, dispatcher
sender information	2 (middle)	recipient, sender, recipient
Product information	3 (high)	recipient, sender
end address information	2 (high)	recipient, dispatcher

including name, phone number, ID number and address, and the phone number and ID number are a fixed length of 29 bytes. The name and address have a certain expansion and contraction. Taking a message of 117bytes (the maximum number of bytes that an RSA1024-bit key can accept) as an example, the time-consuming tests for 1 piece of data, 100 pieces of data, 1000 pieces of data and 10,000 pieces of data were compared, as shown in Table 2. The test found that the AES decryption efficiency is greater than the encryption efficiency, and the RSA decryption time is longer. It is far more efficient to encrypt data using AES; moreover, it does not reduce system performance significantly. For RSA, the efficiency of encryption key is higher and the encryption time is shorter, and the combination of AES and RSA has higher performance. Although RSA decryption speed is slower, it is within the waiting range of data decryption. It can also improve security to a certain extent.

This paper tests and analyzes the effectiveness of the cloud computing-based logistics blockchain image authentication and recognition model. It is tested based on the policy established in the standard policy conformance test package provided by XACML. The test compares the strategy judgment efficiency of the traditional logistics blockchain image authentication and recognition model and the cloud computing logistics blockchain image authentication and recognition model. The simulation results are shown in Figure 4. Five groups of testing samples (1–5) are used, corresponding to 1000, 2000, 3000, 4000, and 5000 single strategies, respectively. The policy decision delay increases with the increase of test samples. At the same time, a comparison between the traditional model for the cloud computing logistics blockchain image authentication and recognition and the proposed model shows the latter has better performance in terms of policy decision.

Ganache is used to build a private chain to deploy smart contracts, as Ganache can quickly initiate a personal Ethereum environment. It can clearly see any changes in the account status. The experiment was designed based on the Ethereum environment. The experimental software, hardware and version environment are shown in Table 3.

q sets the probability of the attacker's success, which represents the size of his attack capability. When at the same block distance, the higher the attacker's ability, the higher is the probability of block data being tampered with successfully; that is, the success rate varies with the size of the attack power. In order to improve its own anti-attack ability, the blockchain can set an appropriate block distance according to the attacker's ability. The probability of successfully tampering with the blockchain under different attack capabilities is shown in Figure 5.

The attribute 'privacy protection rate' refers to the ratio of the number of sensitive attributes for which individuals cannot be identified to the total number of sensitive attributes contained in the dataset. The experimental results of the respective attribute privacy protection rates of Outsourcing Data and Adult are shown in Figure 6. It can be observed that

Table 2 Time-consuming comparison.

The amount of data	AES time consuming(ms)	RSA time consuming(ms)
1	56	78
100	60	100
1000	120	170
10000	180	220

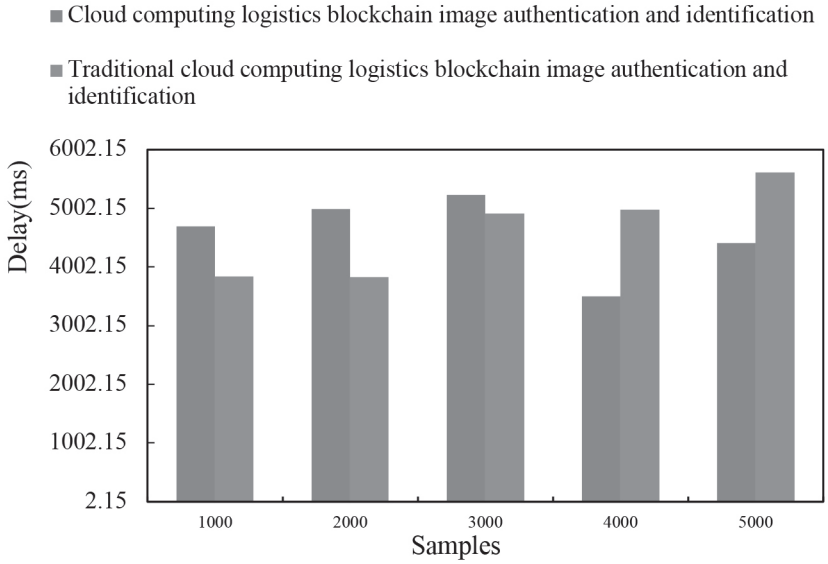

Figure 4 Policy Decision Efficiency.

Table 3 Experimental software and hardware and version environment.

Name	specific information
operating system	Windows 10 64-bit
Nodejs	v14.15.3v5.1.60
Remixsolidity	v0.6.1
Ganache	v2.4.4
IPFS	v0.4.16

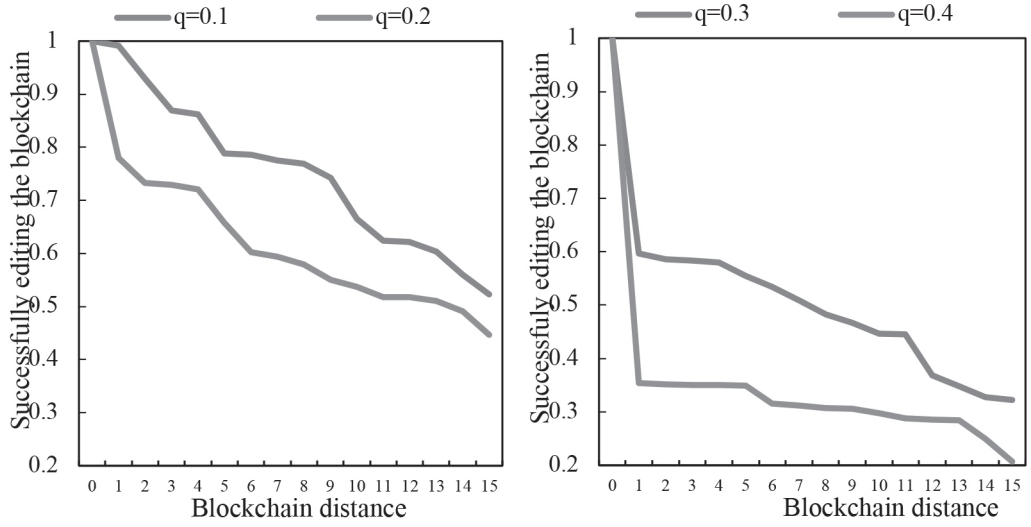

Figure 5 Probability of successfully tampering with the blockchain under different attack capabilities.

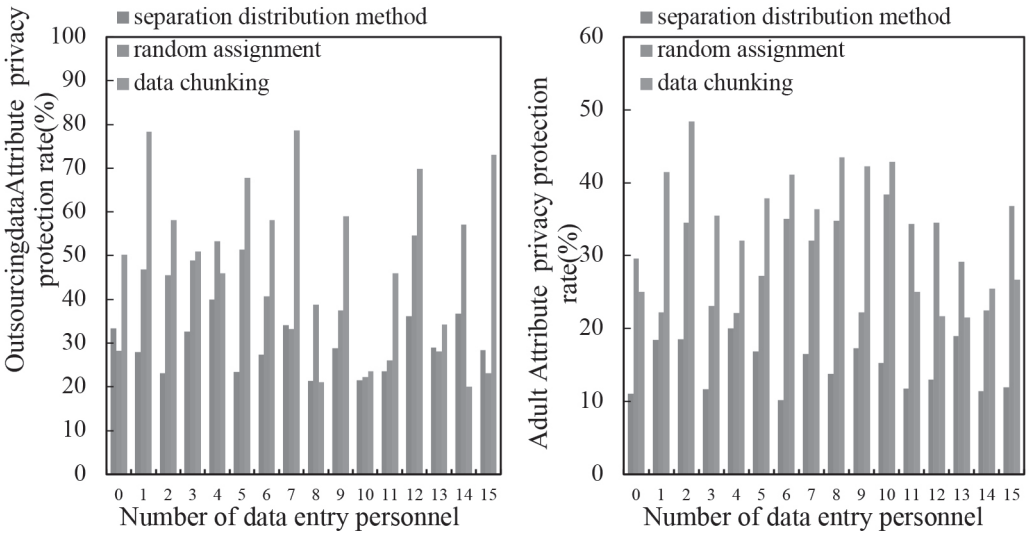

Figure 6 Experimental results of the respective attribute privacy protection rates of Outsourcing Data and Adult.

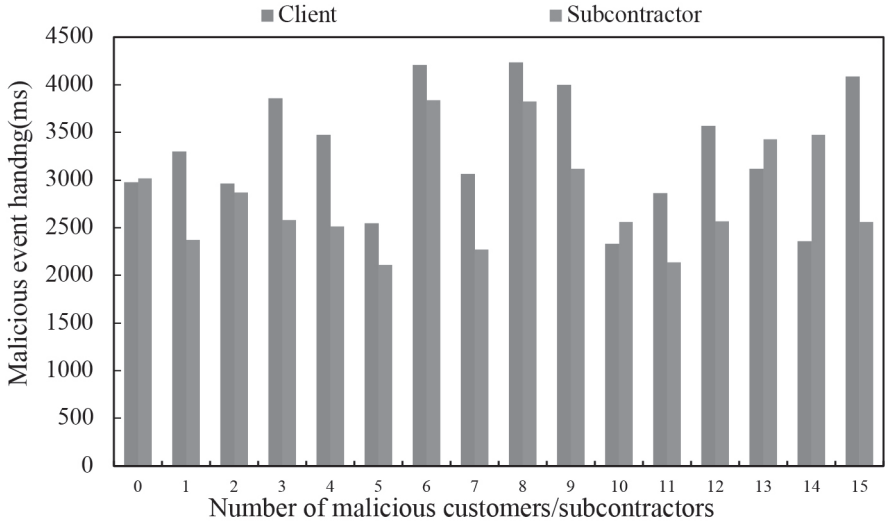

Figure 7 What happens when a malicious event occurs.

the attribute privacy protection rate remains 100% regardless of changes in the dataset or the number of input personnel. This is because the attribute privacy protection rate reflects the impact of sensitive attributes on user privacy. However, with this method, after image segmentation and privacy association separation, there is no sensitive attribute in PPM.

In this paper's TFBO, it is defined that the occurrence of malicious events means that either the customer is malicious, that is, when the entry result meets the demand, but refuses to pay commission to the subcontractor within the time t. Either the input result of the subcontractor does not meet the requirements, but the modification is refused within the time T. If this malicious event occurs, a dispute occurs, and all Orderer nodes in the blockchain network are required to arbitrate. If the arbitration result shows that the malicious party does have malicious behavior, the actions will be carried out according to the pre-agreed smart contract. It pays 50% of the malicious party's deposit in the public account to the other party as compensation. Regardless of whether the customer or subcontractor agrees or not, TFBO does have the ability to deal with malicious events, that is, it can transfer 50% of the deposit of the malicious party in the public account to the other party. It can be seen that the time spent by TFBO in dealing with customer malicious events is not much different from the time spent on subcontractor malicious events. The increase in the number of malicious events does lead to a slight increase in the processing time of malicious events, but it basically remains around 4 seconds. The four-second time will not cause a large delay and affect the user experience, so the TFBO in this paper is not only credible but also practical. The experimental results show that TFBO has good performance in terms of delay, time required for successful tampering and malicious event processing time. This shows that TFBO is not only practical, but also suitable for later accountability and malicious incident handling. Therefore, customers and subcontractors can be well controlled, which strengthens the credibility of the manual entry of outsourced image data. The processing of a malicious event occurs is shown in Figure 7.

The main difference between the weighted and unweighted TextRank and SOM's personalized digital image intelligent

Table 4 Obtaining similar user situations.

Name	Weighted TextRank and SOM	Unweighted TextRank and SOM
precision	0.932	0.882
recall	1	1
F1-SCORE	0.9256	0.7324
Actual number of similar users	18	18

Table 5 Weighted cross-entropy loss function BiLSTM experimental results.

Model	Sample category	Precision
Weighted cross-entropy loss function BiLSTM	digital image buying and selling	1.00
	digital watermarking service	1.00
	Authentication service class	0.87
	image processing service	0.93
Unweighted cross-entropy loss function BiLSTM	Tools	1.00
	digital image buying and selling	0.92

recommendation algorithms is the effect of acquiring similar users. In the simulation experiment, a total of 21 similar users to the current user were found by the weighted TextRank and SOM's personalized digital image intelligent recommendation algorithm. Three of them should not be users similar to the current user. A total of 33 users similar to the current user were found by the unweighted TextRank and SOM personalized digital image intelligent recommendation algorithm. Eighteen of them are correct lookalike users and 13 are wrong lookalike users. All 18 similar users it should have found were found. The similar users obtained by the two are shown in Table 4. The image information written into the database by the weighted TextRank and SOM's personalized digital image intelligent recommendation algorithm is the image of the first and second level consistent with the current user's last login to the system. That is, the image information of interest to the user i is written into the database recommendation table.

After experiments, the personalized digital image intelligent recommendation algorithm based on weighted TextRank and SOM finds all users similar to the current user, and finds a few dissimilar users. The personalized intelligent digital image recommendation algorithm without weighting TextRank and SOM also finds all users similar to the current user. However, there are many similar users who are wrong. Therefore, from the results of finding similar users, the weighted TextRank algorithm is obviously better than the unweighted TextRank algorithm. Judging from the last image information written into the database, because similar users have purchased more images than M/2 in this simulation experiment. Therefore, the personalized digital image intelligent recommendation algorithm based on weighted and unweighted TextRank and SOM selects the top five images and writes them into the recommendation table through the historical image information of similar users. From the candidate recommended images obtained from the database, the top five images with cosine similarity are selected and written into the recommendation table of the database. The results also verify that calculating the cosine similarity can exclude some images that are not of interest to the current user. The experimental results verify that the unweighted TextRank algorithm finds many similar users wrong. Therefore, the probability of writing into the database the image information that does not interest the user is greater than the result of using the weighted TextRank algorithm to write into the database.

The experimental results of the weighted cross-entropy loss function BiLSTM are shown in Table 5. When training the model with 800 smart contracts, the time is 531.22362 seconds. After training the model, it takes 1.185 seconds to classify 200 smart contracts. It can be seen that after the model is trained, the classification speed of smart contracts is faster. The F1-scores show that the value of each category is greater than 0.9. For the precision rate, the value of authentication service class is 0.83, while the value of other classes is 1. The recall rate results show that the values of each category are all greater than 0.9. Overall, the experimental results are good. The experimental results of the weighted and unweighted cross-entropy loss function BiLSTM model are equal. Compared with the smart contracts obtained from the Ethereum official website, the smart contracts used in the digital image transaction management system are not mixed with the smart contracts of the Ethereum official website. The classification effect of the weighted cross-entropy loss function BiLSTM is better than the classification effect of smart contracts obtained from the official Ethereum website. Comparison of the experimental results of the self-encoding random weight ELM network and the weighted cross entropy loss function BiLSTM model: The self-encoding random weight ELM network model training model takes less time than the weighted cross entropy loss function BiLSTM model.

The individual and diverse consumption demands of users in the new era have continuously driven the development and innovation of the e-commerce industry, and the e-commerce industry in turn has played an important role in driving economic development. With the continuous improvement of Internet penetration and innovative sales models, the market size of e-commerce has increased year by year. The logistics development from 2017 to 2021 is shown in Figure 8. However, despite this growth, there are many problems that need to be solved urgently, one of the main

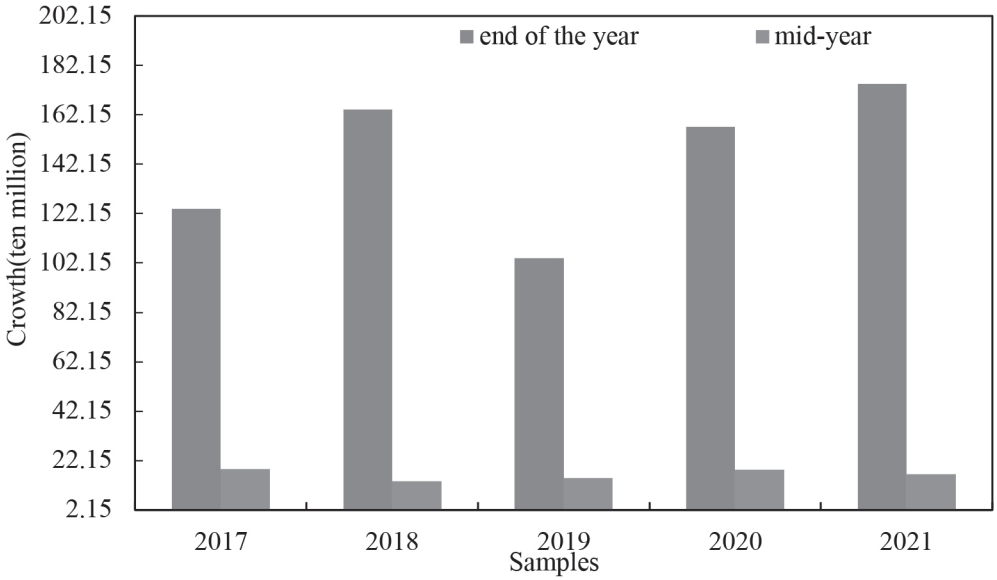

Figure 8 Logistics Development 2017–2021.

ones being the security of logistics information. In today's highly informatized world, users also pay more attention to the privacy protection of personal information. In the current logistics service industry, in order to meet the rapidly increasing user needs and demands, and improve the transportation and distribution efficiency of logistics enterprises, logistics companies store the user's personal information in the form of clear text on the logistics express list. Although this is convenient for the logistics transfer and distribution process, it also jeopardizes the security and privacy of logistics data. According to relevant reports, due to the online virtuality of e-commerce, the drawbacks of online shopping have gradually surfaced, giving rise to an increase in online shopping disputes. For example, due to the leakage of personal information, some users will receive products that do not belong to them, and some websites have personal information clearly marked for sale. However, the regulatory agencies and both parties to the transaction cannot effectively pursue and determine the responsibility for disputes, which is determined by the attributes of traditional regulatory agencies. The traditional supervision model cannot be directly applied to online transactions, so that users' private information cannot be guaranteed and, at the same time, user rights cannot be protected. Logistics involve many participating entities and the corresponding supervision mechanism is defective, making it impossible to issue relevant materials to prove that a particular company or other personnel leaked their own information.

Each record in this scheme involves seven-segment address encryptions and two-segment user information encryptions. Since each segment of encryption and decryption consumes the same time, in order to facilitate the calculation, the encryption and address decryption times are calculated according to a segment of the address of each record. Since the recipients, senders and specific points involved in our various express deliveryies are also different, when the number of specific delivery increases, the number of keys required also increases, and the time required also increases. We calculate the time required to generate all secret keys according to the number of express delivery, and calculate the total time consumption statistics of all express delivery required for one encryption and decryption according to the time each express delivery takes to encrypt and decrypt an address. When not attacked, the robust watermark image NC=1 and the semi-fragile watermark image NC=1 extracted by the cloud computing-based logistics blockchain image authentication and recognition model. When the attack intensity is large, the similarity NC of the robust watermark image reaches more than 90%. The experimental results of salt and pepper noise and rotation attack are shown in Figure 9.

Rotation attack experiment: When the counterclockwise rotation angle of the image to be detected is 10 to 1000, the NC value of the extracted robust watermark is between 1 and 0.9782. The NC (Normalised Cross-correlation) value of the extracted semi-fragile watermark is between 0.8452 and 0.7063, and the TAF (Tamper Assessment Function) value of the semi-fragile watermark is between 0.2507 and 0.4315. Median filter attack experiment: After the image to be detected is attacked by median filter with a filter window size of 2 to 99, the NC value of the extracted robust watermark is all 1. The NC values of the extracted semi-fragile watermarks range from 0.9696 to 0.8909, and the TAF values of the semi-fragile watermarks range from 0.0676 to 0.1808. The median filter attack results are shown in Figure 10.

4. CONCLUSION

The personalized recommendation algorithm for digital images proposed in this paper is based on the different levels of interest of users according to different sources of historical data. The proposed algorithmcan better mine users' purchasing orientation. The research ideas and methods can be extended to other e-commerce platforms. This paper uses a neural network to design a personalized recommendation algorithm combined with the impact of user historical data on

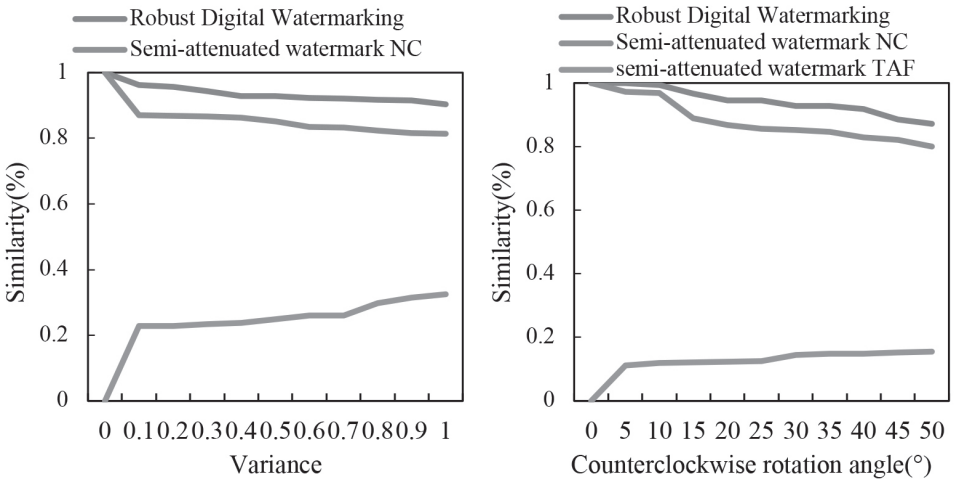

Figure 9 Experimental results of salt and pepper noise and rotation attack.

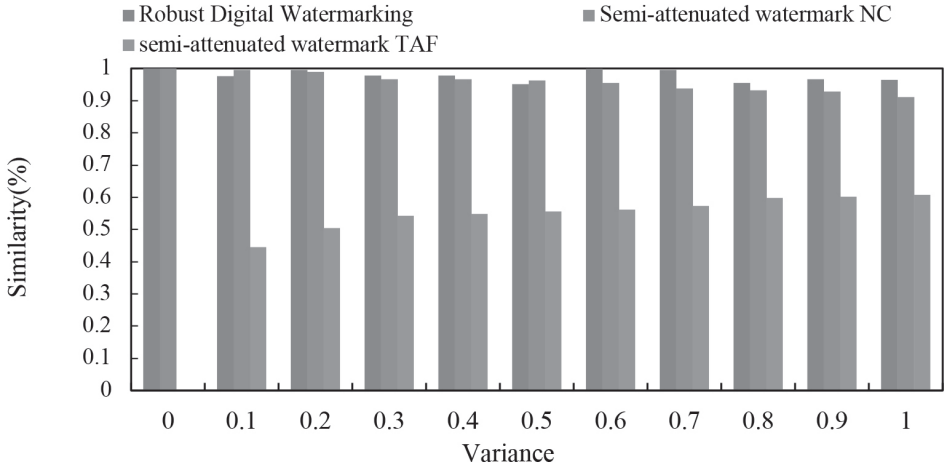

Figure 10 Median filter attack results.

user shopping. It suggests using neural network and other computer technologies to solve marketing problems more intelligently for customer management in business marketing. The digital image personalized intelligent recommendation algorithm proposed in this paper is applied to the customer management of business marketing management. It can enable merchants to effectively use user historical data to accurately recommend digital images to users. It encourages users to buy more digital image products, thereby increasing the business profits of merchants. This paper gives solutions to several links that may cause privacy leakage in logistics, and basically solves the problem of data leakage in the logistics process. The above solutions can solve the privacy protection problem in the logistics process and have certain applicability, timeliness and verifiability. However, the proposed approach still has several shortcomings which should be addressed by future research in order to further improve its applicability and comprehensiveness.

REFERENCES

1. Suryalakshmi S M, Elayaraja M, Vijai C. Blockchain Technology in Logistics: Opportunities and Challenges. Asia Pacific Business Review, 2021, 13(7):147–151.
2. Zhong, C. & Yue, Q. (2025). Flexible and Efficient Multi-Authorization Data Sharing Scheme With Enhanced Privacy Protection. International Journal of Intelligent Information Technologies (IJIIT), 21(1), 1–27.
3. Xu, Z., Jain, D.K., Neelakandan, S. et al. Hunger games search optimization with deep learning model for sustainable supply chain management. Discov Internet Things 3, 10 (2023).
4. Midaoui M E, Laoula E, Qbadou M. Logistics tracking system based on decentralized IoT and blockchain platform. Indonesian Journal of Electrical Engineering and Computer Science, 2021, 23(1):421–430.
5. Hackius N, Petersen M. Translating High Hopes into Tangible Benefits: How Incumbents in Supply Chain and Logistics Approach Blockchain. IEEE Access, 2020, 8(1):34993–35003.
6. Xia Z, Wang X, Zhang L. A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing. IEEE Transactions on Information Forensics & Security, 2017, 11(11):2594–2608.
7. Deng R, Lu R, Lai C. Optimal Workload Allocation in Fog-Cloud Computing Toward Balanced Delay and Power Consumption. IEEE Internet of Things Journal, 2017, 3(6):1171–1181.
8. Wei W, Fan X, Song H. Imperfect Information Dynamic Stackelberg Game Based Resource Allocation Using Hidden Markov for Cloud Computing. IEEE Transactions on Services Computing, 2018, 11(99):78–89.

9. Jin L, Zhang Y, Chen X. Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 2018, 72(JAN.):1–12.
10. Tsai J L, Lo N W. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services. IEEE Systems Journal, 2017, 9(3):805–815.
11. Zhao P, Zhang Y, Chang E. Blockchain and Palm Scanning Integrated System (BPIS) for Workplace Access Control and Contact Tracing. Engineering Intelligent Systems, 2021, 29(6):353–361.
12. Mao Q. Architecture and Simulation of a Social Management Service System Based on the Internet of Things Information Model. Engineering Intelligent Systems, 2021, 29(2):117–127.
13. Wei R. A Deep Learning Image Recognition Method Based on Edge Cloud Computing. Engineering Intelligent Systems, 2022, 31(1):5–12.
14. Humayun M, Jhanjhi N Z, Hamid B. Emerging Smart Logistics and Transportation Using IoT and Blockchain. IEEE Internet of Things Magazine, 2020, 3(2):58–62.
15. Merka Z, Perkov D, Bonin V. The Significance of Blockchain Technology in Digital Transformation of Logistics and Transportation. International Journal of E-Services and Mobile Applications, 2020, 12(1):1–20.
16. Nautiyal N, Bisht S, Joshi B. Blockchain Design for Logistics & Supply Chain Management in Developing Regions. International Journal of Recent Technology and Engineering, 2020, 8(6):1711–1716.
17. Stergiou C, Psannis K E. Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey. International Journal of Network Management, 2017, 27(3):1–12.
18. Hirai T, Masuyyama H, Kasahara S. Performance analysis of large-scale parallel-distributed processing with backup tasks for cloud computing. Journal of Industrial & Management Optimization, 2017, 10(1):113–129.
19. Sudarsan V, Satyanarayana N. Secure and Practical Outsourcing of Linear Programming in Cloud Computing: A Survey. International Journal of Computer Applications, 2017, 159(4):1–4.
20. Wang S, Zhou J, Member. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2017, 11(6): 1265–1277.
21. Barsoum A F, Hasan M A. Provable Multicopy Dynamic Data Possession in Cloud Computing Systems. IEEE Transactions on Information Forensics & Security, 2017, 10(3):485–497.
22. Yi H, Chan J, Alpcan T. Using Virtual Machine Allocation Policies to Defend against Co-Resident Attacks in Cloud Computing. IEEE Transactions on Dependable & Secure Computing, 2017, 14(1):95–108.
23. Rodrigues T G, Suto K, Nishiyama H. Hybrid Method for Minimizing Service Delay in Edge Cloud Computing Through VM Migration and Transmission Power Control. IEEE Transactions on Computers, 2017, 66(5):810–819.
24. Abdel-Basset M, Mai M, Chang V. NMCDA: A framework for evaluating cloud computing services. FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE, 2018, 86(SEP.):12–29.
25. Cai H, Xu B, Jiang L. IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. IEEE Internet of Things Journal, 2017, 4(1):75–87.
26. Du J, Zhao L, Jie F. Computation Offloading and Resource Allocation in Mixed Fog/Cloud Computing Systems with Min-Max Fairness Guarantee. IEEE Transactions on Communications, 2018, 66(4):1594–1608.
27. Tawalbeh L A, Mehmood R, Benkhelifa E. Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications. IEEE Access, 2017, 4(99):6171–6180.

Shuting Liu was born in Fuping, Shaanxi, P.R. China, in 1984. She received a Master's degree from Xi'an Jiaotong University, P.R. China. Currently, she is working at the School of Information and Business, Shaanxi Energy Institute. Her research interests include cloud computing, computer software and big data analysis.
E-mail: lsht1984@126.com