Blockchain-Based Social Media Software Privacy Data Cloud Storage Method

Jianjun Tang(✉) and Xiaopan Chen

Jiangxi University of Software Professional Technology, Nanchang 330041, China
tangjianjun857@163.com

Abstract. At present, the leakage of private data stored on social media software has attracted the attention of the academic community. Therefore, it is necessary to discuss the cloud storage method of private data of social media software in detail. In the process of using the social media software privacy data cloud storage method, there is a problem that the file storage takes too long. In order to alleviate the above problem, a blockchain-based social media software privacy data cloud storage method is designed. Obtain the identity management mechanism of social media software, formulate identity restriction plans according to the available scope of accounts, classify the risk factors of privacy information, improve the data reading mode, adjust the independence of data, and use the blockchain to set up the cloud storage structure. Experimental results: The file storage time of the social media software privacy data cloud storage method and the other two social media software privacy data cloud storage methods are: 2.672 s, 4.229 s, and 4.727, respectively. After the cloud storage method of software privacy data is combined, the application effect of the method is better.

Keywords: Blockchain · Social media software · Private data · Cloud storage · Information technology · Personal information

1 Introduction

With the development of information technology and human civilization, the amount of data produced is increasing explosively. The traditional data storage and analysis model can not meet the existing needs. Social media has quickly become the dominant media on the Internet, thanks to the craze for social software such as Facebook and the development of computer and Internet technologies. From home to abroad, all kinds of social applications are coming out. However, the leakage of privacy information often causes users into a dilemma, and the information security problem has become an important factor restricting the development of cloud storage. Therefore, it is particularly important to take some protection measures for the privacy information of individual users under the cloud storage environment to effectively avoid the risk of privacy disclosure [1].

Speaking of the domestic, along with the new media technology development and the intense market competition, from initial person net, happy net, skyline, cat flutter. Up

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 469, pp. 376–389, 2023.
https://doi.org/10.1007/978-3-031-28867-8_28

to now, the development of Weibo, WeChat, Mo, Line, Youjia, social media from product positioning design, positioning and services, interesting, personalized features are increasingly evident. In order to get close to the users and realize the win-win of word-of-mouth and influence communication, many enterprises take advantage of the opportunity to infiltrate social elements into the communication of marketing and publicity. Secondly, the protection of citizen information security depends on the cooperation of all parties to build and maintain a harmonious social network environment, so it is necessary to build a user privacy information protection system. From the multi-dimensional point of view, we can comprehensively enhance the security of user privacy information. To the user, convenient, individual application experience, have powerful attraction. Whether from the perspective of work or life, most users of social applications, is not satisfied with the simple online communication and exchange, but look forward to online and offline integration. At the same time, the user's privacy security issues have become increasingly prominent.

From the multi-dimensional point of view, we can comprehensively enhance the security of user privacy information. To the user, convenient, individual application experience, have powerful attraction. Whether from the perspective of work or life, most users of social applications, is not satisfied with the simple online communication and exchange, but look forward to online and offline integration. At the same time, the user's privacy security issues have become increasingly prominent.

The essence of cloud storage is that users upload a large amount of information to the cloud, and can access information resources at any time without the limitation of devices and time. Therefore, the cloud storage platform has a large amount of user privacy information [2, 3].

In order to improve the efficiency of social media privacy data storage, this paper designs a blockchain-based social media software privacy data cloud storage method. First, the identity management mechanism of social media software is acquired. Secondly, an identity restriction scheme is formulated according to the available scope of the account, and the risk factors of private information are classified. Finally, improve data reading methods, adjust data independence, and use blockchain to build cloud storage structures.

1.1 Access to Social Media Software Identity Management Mechanisms

With the popularity of social media and the development of e-commerce, targeted marketing, precision marketing has been sought after. Over-collection of personal privacy means that the merchant collects personal information in many ways in order to store and develop more potential users for the need of self-profit. Mainly in two ways, one is to register or fill in the form of the relevant forms. Second, through the form of technical tracking collection. Digital identity is identity, too. Its difference is that it is virtual, invisible and untouchable. Therefore, against the digital identity may be false identity attacks, identity theft attacks and witch attacks. As far as the current usage of social media is concerned, whether it's a simple social networking application or a forum, a shopping site, etc., you have to provide personal information: name, phone number, email address, home address, like WeChat Wallet, etc., you have to bind personal bank card information. False identity, refers to the attacker using other people's information,

or using incorrect information to obtain the account. Identity theft, refers to the attacker in the case of unauthorized use of other people's accounts, as long as you know that other people's accounts can embezzle their identity. Witch attacks are attacks where the attacker actually controls many identity accounts, and you might think that there are many accounts "flooding" the forums, but there may be only one person behind those accounts.

In order to prevent these three attacks, we need to restrict the digital identity. Traditionally, an identity manager distributes digital identities. Users need to submit personal information and set an account password to obtain digital identities. Only after the manager confirms, can the account be owned. The secondary development and utilization of personal privacy data refers to the use of data processing or information mining and other methods to process the collected user information by adopting the CRF algorithm and search for the content with commercial value [4, 5]. In the field of marketing, the secondary development and utilization of personal information has been highly praised as a new business model. Personal information submitted by users is typically identified or stand-alone, such as an ID number, a mobile phone number, or an email address registered on a different server, thus ensuring that different users have different accounts that can only be used by the owner through a password. Depending on the available scope of the account, these identity restrictions are shown in Fig. 1:

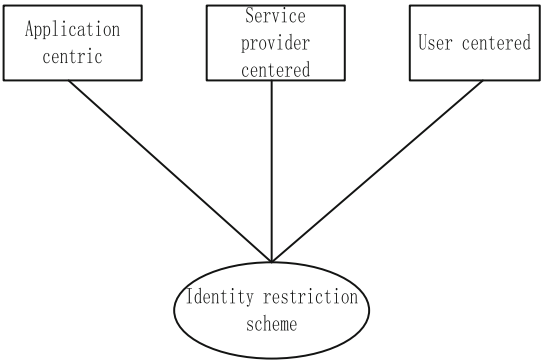

Fig. 1. Schematic diagram of identity restriction scheme

As you can see from Fig. 1, there are three identity restriction schemes: application-centric, service-provider centric, and user-centric. Application-centric identity management scheme: This scheme refers to the way people interact socially, and allocates accounts around different activities. In real life, people go to school, drive a car, work, get married respectively need a student card, driver's license, work permit, marriage certificate. For some businesses, through consumer information analysis and secondary development, we can better understand user needs, and then perfect and optimize their own services, or launch new services, for their own and users are win-win. Each application only needs to manage its own account, and users can only use the corresponding

service after registering their account, and these accounts can only be used in the application services. Because of its simplicity, each application can embed the identity management module directly and provide services directly without maintaining the identity management module separately.

Currently, privacy deals in social media and even the entire Internet are conducted in two ways. One is information-sharing through business cooperation, each taking what he or she needs. Service-centric identity management solutions: As the business expands, the same service provider may develop multiple applications, such as Alibaba has Taobao, Alipay, Aliwanwang, Tencent has QQ, WeChat and many games. From the user's point of view, they are separate, different, and provide different services for the user. But we do know that there is more than one partner, and there are other partners, and so on, and we see the horror in the process, that if the scope of information sharing is not effectively regulated and controlled, the user's information will be known to more merchants. This is undoubtedly a disguised invasion of users' personal privacy. But from the service provider point of view, they are unified, the same, are controlled and managed by the same service provider. User-centric identity management: As long as a user has an account, it's like getting an ID card and can log in to all applications without having to sign up for a separate account.

1.2 Categorizing Privacy Information Risk Elements

The main function of cloud storage is to help users to store information, manage data and share information. So it is different from other Internet related services. As far as the privacy protection policy is concerned, most of our social media privacy protection policies have no obvious location, which is difficult to attract users' attention. In particular, with the development of mobile Internet technology, users mainly download App to the mobile terminal for direct use, with little attention to privacy protection policies. In order to better identify the risks of user privacy information in the cloud storage environment and conduct in-depth research on the protection of user privacy information, we classify the user privacy information involved in the process of cloud storage services into basic personal information and personal activity data [6]. This paper considers that the risks of user privacy information in cloud storage include.

As can be seen from Fig. 2, the types of user privacy information risk in a cloud storage environment include: management risk, technical risk, and legal risk. The management risks of users' privacy information in cloud storage environment refer to the risk factors that lead to the disclosure of privacy information in the process of cloud storage services due to poor management and poor security quality of the relevant organizations and individuals that have the management responsibility for users' privacy information. As far as the content is concerned, it is a pile of terms, and users need enough time to understand and digest it. But the author also found that nearly 40% of users never read the privacy policy, and directly accept it, which is related to the piling up of these terms.

Cloud service is a kind of network technology service, which has been springing up in recent years. Its government management has overlapping functions, unclear rights and responsibilities, and the relative lack of laws and regulations has brought difficulties to the supervision and management of law enforcement departments. Privacy policies rarely describe the approach to the use of personal data and the privacy management of

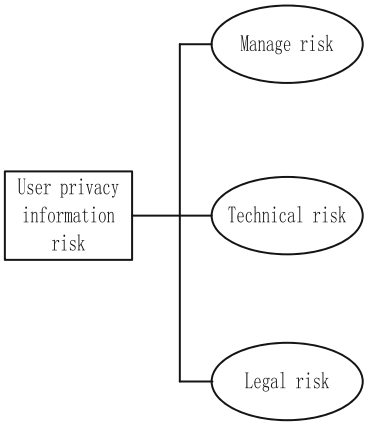

Fig. 2. Risk types of user privacy information in cloud storage environment

the platform. As far as privacy permissions are concerned, the default privacy permissions for social media platforms are mostly open to everyone. The management risks of cloud service providers refer to the operational errors caused by the server interruption caused by the lack of management and maintenance of servers, networks and other equipment, the malicious theft of user privacy data by internal employees caused by the lax internal management of employees, and the non-standardized internal operation and inadequate staff training of enterprises. And the location of the privacy settings feature is also different.

At present, WeChat, Weibo, Tencent and other large enterprises, in the settings function, there are obvious "privacy", "privacy and security" settings. Like Hungry, this location-based, commonly used ordering software doesn't have a "privacy" setting. In order to obtain convenient services, cloud storage users often ignore the privacy information security considerations, lack of sensitivity and protection skills necessary to face information risks. Therefore the user to the personal privacy protection omission is also causes the information disclosure the important factor. Similarly, people in cyberspace to use QQ, Weibo, Alipay and other applications to provide services, chat with QQ to register the QQ account, Weibo messages will be registered Weibo account, Alipay money will be registered Alipay account. The technical risks of users' privacy information in cloud storage environment refer to the technical risk factors that lead to the disclosure of privacy information in the process of cloud storage services, such as the limitations of cloud storage security technology and the lack of research and development capability for emerging security technologies. But do not think so to the user however, the secondary development goal that the businessman develops to information above all whether proper infer hard. Second, when a user's mailbox is full of ad emails. When users in the process of browsing the Web to see the scrolling ads have been browsed on the product information, it will have a personal privacy leak, personal domain is violated feeling. A computer expert, especially a programmer, who used to be keen on computer technology. After deduction, especially refers to the use of system security vulnerabilities on the network to attack and destroy or steal data.

Wireless Internet is the most common way for cloud storage users to connect to the Internet. Even if the transmission signal adopts information encryption technology, but the signal exposed in the air will be intercepted. The virtual storage unit technology used in cloud storage makes it impossible to detect the data exchanged between virtual systems, and also enhances the possibility of Trojan virus attack due to virtualization. Most of the information stored in the personal cloud is stored in the public cloud, if the data is not isolated properly, the information between users will interfere with each other. Hacker's existence, no matter to the enterprise, the individual even the country, is the enormous threat. Hackers can invade computer systems, steal and tamper with user information, through the design of the Trojan program into the target system, break the permissions directly log in. Survey found that nearly 40% of users have encountered the problem of social account password theft. But the address book or the document divulges, phenomenon and so on handset computer poisoning also has the occurrence. Therefore, the unstable Internet environment and virtualized storage technology increase the risk of leakage of privacy information of individual users in cloud storage.

1.3 Improve Data Read Mode

The data in the program exists in the form of objects, but the additional data of the blockchain transaction only accepts the form of hexadecimal strings. Therefore, the program cannot directly read and write data on the chain, but requires a conversion process from hexadecimal strings to objects and objects to hexadecimal strings. This section will describe the entire process of reading and writing blockchain data. And the data conversion mechanism is introduced. The SQL language covers many functions such as data query, data manipulation, data definition and data control. The language style is unified, and all activities of the database life cycle can be completed independently. Users can use SQL language to define, modify and delete relational schemas, define and delete views, insert data, and create databases. At the same time, the data in the database can be queried and updated.

Data writing is initiated by a program to store objects in memory at run time on a chunk chain. The first step in writing data to a chunk chain is to serialize the in-memory object into a recognizable JSON string, and add the state information of the data header to form a complete data structure. Because of its high degree of non-procedural, users in the process of using SQL can directly complete specific operations without concern about the underlying complex encapsulation operations, reduce user burden, adjust the independence of data. The second step transcodes the entire data structure into a hexadecimal string, and adds the identifier "0x" before the hexadecimal string to form a form that can be stored by a block chain. The final step is to construct a new transaction in which the converted data structure is attached to the transaction and submitted to the block chain to save the data. In the data reading mechanism, the expression formula of the encryption parameter is.

$$D = \frac{\varepsilon}{W} \times \exp\|W - 1\|^2 \tag{1}$$

In formula (1), W represents the original plaintext document set, and ε represents the number of documents in the original plaintext document set W. In an encrypted database,

data is stored in ciphertext. So it brings great technical challenge to the calculation and retrieval of data. Traditional ciphertext data retrieval based on ciphertext matching can not meet the requirements of database such as conditional query, ranking, fuzzy query, and so on. Specifically, the program first selects a node in the blockchain network in the final step. Using the key file corresponding to the built-in account of the node, the private key of the account is calculated. Then a new transaction is constructed using the address of the account and the converted data. Finally, the transaction API of Ethereum is called to submit the transaction to the block chain to write the data, and the hash of the transaction returned by the API is obtained. On the basis of the above description, the formula for calculating the keyword set generation process is derived.

$$\beta = \sum_{j=1}^{i} \frac{\sqrt{d_i + t_j}}{2} \times \mu_{ij} \tag{2}$$

In formula (2), d represents the topic set extracted from W. t represents the number of topics in the topic set d. μ represents the set of keywords extracted from W. i, j represents the number of keywords in the keyword set μ and the total number of keywords, respectively. Therefore, according to the different security levels of database columns, an adaptive and customizable data column security level encryption method is designed to balance data security and system efficiency. Through the self-defined encryption interface, under the premise of ensuring data security, the operability of ciphertext is improved, and the running efficiency of database system is ensured.

Block chain access to data is public, and each transaction in the chain has a unique hash value. As long as you hold the hash of a transaction, you can access the data stored on that transaction. Thus, the first step in reading the data from the blockchain is to use the transaction hash to get the transaction data through the Ethernet API and read the value of the input field in the transaction. Because users have different security requirements and operation requirements for different columns in the data table. Therefore, the data table should support the different strength encryption algorithm to the different column according to the user demand, or uses the encryption algorithm which supports the inquiry and the computation. The second step removes the flag "0x" from the hexadecimal string header and decodes it as a stored data structure. Finally, according to the description of the data structure, the JSON string stored in the data body is deserialized to the object in the program context, and the data is read.

1.4 Blockchain Setup Cloud Storage Structure

Block chain is a combination of cryptography, consensus mechanism and other mature technologies. It works in a decentralized mode, in which all the nodes in the network participate in the billing process. It also provides sophisticated scripts to support different business logic. Cloud server is only responsible for the cloud server data storage operations, and provide retrieval services, it will not take the initiative to update ciphertext document collection, will not actively update the security index. A blockchain is a chain-like structure composed of a series of blocks. Blocks are the places where the data are packaged and stored, and are the basic units of a block chain, which are added to the chain in the order in which they are generated [7].

Blockchain runs on a point-to-point distributed network, in which all nodes are peer to each other and there is no central node with special authority that can control other nodes. Each node completes the data processing through the consensus mechanism. Given the corresponding set of ciphertext, the server cannot learn anything about the original plaintext document from these ciphertext sets. This is typically done by using symmetric encryption schemes to encrypt documents or message blocks. In addition to the search results, the server can not learn more information about the open text accounts of the completion of verification written to the block chain data can be all nodes publicly accessible. But public access does not mean that the information itself is open to all nodes. Transaction data cannot be tampered with. No one can delete or modify the data once it has been saved to the chain through validation in the block chain. The cloud server cannot retrieve any keywords without the authorization of the data owner, which can be achieved by generating a keyword retrieval token using a pseudo-random function. The server cannot generate a valid retrieval token without the key provided by the data owner.

Collective maintenance, storage, transmission and verification of data in the chain are carried out by all the nodes in the blockchain under the mechanism of consensus. Even if some nodes in the blockchain network go offline or fail, the whole system will not be paralyzed. In addition, if two different miners perform the workload proof process for a new block almost simultaneously, the two blocks may be validated and accepted by two different subsets of the bitcoin network. Then a bifurcation is formed, and other miners need to choose the bifurcation with more blocks and longer chains for subsequent additions. The server cannot learn any information about the keyword to be retrieved from the retrieval token provided by the authorized user. If the server is a malicious server, in addition to the above requirements, the server can not forge encrypted data and related metadata. Then the addition field calculation formula for the metadata is.

$$F = \left|\frac{\varphi}{d}\right|^2 - \left|\frac{t}{\mu}\right| \times \varphi^{-1} \tag{3}$$

In formula (3), φ represents an identifier generation function. On the basis of formula (3), the calculation formula of the length of the retrieval vector is obtained as:

$$Q = \frac{1}{(H)} \times \sqrt{\frac{\lambda}{\mu}} - \varepsilon \tag{4}$$

In formula (4), H represents the set of topic distribution vectors, and λ represents the number of distributions in the vector. In order to adapt to the increasingly complex network environment, the traditional relational database has gradually developed into a distributed data management system through network interconnection. A single data storage node gradually becomes a cluster of distributed servers. In a multi-user scenario, a malicious user should not be able to query with any keyword without the authorization of the data owner, nor should he be able to learn additional information from the query submitted by the user. Key exchange, authorization control, access control and other technologies have been more mature, and widely used. Therefore, this chapter does not consider these security models. Compared with centralized database, distributed data

management system has more advantages in expansibility, reliability, availability and cost-effective.

The most important feature of distributed data management is the multi-node backup of redundant data to deal with the data recovery in the case of failure. Given a ciphertext model, an attacker can retrieve ciphertext information stored by the data owner on a cloud server. These include encrypted document collections, secure indexes, and retrieval tokens. But the attacker can not get the encryption key, and can only attack through the ciphertext information.

However, there may be conflicts between the redundant data backed up, and data consistency mechanisms are needed to ensure that the data backed up by different nodes are consistent, so data consistency mechanisms can be considered as the core of a distributed data management system. Given the background information model, the cloud server can not only obtain all the information in the known cryptograph model, but also analyze the query records, the relationship between different search tokens, mathematical statistics, etc. For example, according to the length of the search vector to get the total number of keywords and other information, so as to construct keywords for further attacks. It is guaranteed by the properties of the hash function that a lot of calculations must be made to get the required blocks, and the faster the calculations are, the earlier the results are likely to be. Nodes can only add blocks if they have "book-keeping rights," and all other nodes are updated according to the data of the node that has the book-keeping rights.

2 Experimental Test

2.1 Build an Experimental Environment

In order to avoid the impact of external network fluctuations on the experiment, all experiments in this chapter are carried out in a distributed system composed of multiple virtual hosts, each virtual machine configuration is the same. The cloud encrypted database system consists of three parts: user application client, encrypted database agent and cloud database server. Client and cryptographic database agents for user applications are deployed on workstations, cloud database systems are deployed on Alibaba cloud servers, and network bandwidth is 100 MB/s. Three physical hosts were used to virtualize 8 virtual hosts, and 4 virtual hosts were distributed on each physical machine. Among them, 4 virtual hosts are used to construct distributed file storage module, 2 virtual hosts are used to construct blockchain network, 1 virtual host is used to run Web server, and the other one is used as test machine. Using Openstack to set up the cloud environment, the encrypted database agent Qin-Router is deployed on the private cloud and is responsible for encrypting and decrypting the data. The MySQL database stores the user's information. The virtualization software used in the experiment was the Oracle VM Virtual Box.

2.2 Experimental Results

This experiment uses the experimental comparison way to verify the performance of the privacy data cloud storage method of the social media software. Choose the privacy data

cloud storage method of social media software based on encryption algorithm and the privacy data cloud storage method of social media software based on neural network. Taking the case of opening block chain storage as an example, the storage experiment selected files of 64 MB, 128 MB, 256 MB and 512 MB in size as subjects, and the storage time consumption of the three methods were tested. The experimental results are shown in Tables 1, 2, 3 and 4.

Table 1. 64 MB file storage time (s)

Number of experiments	Social media privacy data cloud storage method based on encryption algorithm	Storage method of social media privacy data cloud based on neural network	This paper describes the privacy data cloud storage method for social media software
1	0.851	0.845	0.313
2	0.748	0.769	0.225
3	0.916	0.855	0.364
4	0.815	0.771	0.205
5	0.744	0.692	0.308
6	0.569	0.701	0.231
7	0.899	0.825	0.305
8	0.736	0.644	0.199
9	0.812	0.793	0.347
10	0.903	0.851	0.258
11	0.688	0.962	0.367
12	0.716	0.774	0.284
13	0.814	0.855	0.369
14	0.951	0.946	0.422
15	0.879	0.831	0.361

As can be seen from Table 1, the storage time of the privacy data cloud of the social media software is 0.304 s, 0.803 s and 0.808 s, respectively, compared with the other two methods.

Table 2. 128 MB file storage time(s)

Number of experiments	Social media privacy data cloud storage method based on encryption algorithm	Storage method of social media privacy data cloud based on neural network	This paper describes the privacy data cloud storage method for social media software
1	2.645	2.255	0.988
2	2.066	2.361	1.032
3	2.482	3.055	1.525
4	1.306	3.444	1.204
5	1.987	2.616	1.516
6	1.008	2.152	1.377
7	1.254	3.008	1.259
8	1.366	2.145	1.306
9	1.487	2.263	1.425
10	1.288	1.546	1.228
11	1.316	2.162	1.137
12	1.219	3.554	0.998
13	1.015	2.845	0.857
14	2.114	3.116	0.966
15	1.352	2.582	0.963

As can be seen from Table 2, the storage time of the privacy data cloud of the social media software is 1.185 s, 1.594 s and 2.607 s, respectively, compared with other two storage methods.

As can be seen from Table 3, the storage time of the privacy data cloud of the social media software is 1.908 s, 3.925 s and 4.024 s, respectively, compared with other two storage methods.

Table 3. 256 MB file storage time(s)

Number of experiments	Social media privacy data cloud storage method based on encryption algorithm	Storage method of social media privacy data cloud based on neural network	This paper describes the privacy data cloud storage method for social media software
1	4.615	3.131	2.615
2	3.485	4.206	1.948
3	4.163	3.054	2.331
4	3.848	4.163	2.664
5	3.919	3.456	1.564
6	3.055	4.912	2.006
7	4.647	3.714	1.948
8	3.612	5.002	2.174
9	4.001	4.693	1.566
10	3.665	3.855	2.133
11	4.163	4.162	1.847
12	3.787	3.787	2.021
13	4.699	4.336	1.225
14	3.105	3.855	1.021
15	4.112	4.027	1.554

Table 4. 512 MB file storage time(s)

Number of experiments	Social media privacy data cloud storage method based on encryption algorithm	Storage method of social media privacy data cloud based on neural network	This paper describes the privacy data cloud storage method for social media software
1	10.65	11.312	7.615
2	9.316	10.879	6.102
3	8.237	12.645	6.887
4	9.487	11.011	7.411
5	10.122	10.561	8.025
6	11.066	11.217	7.163
7	12.447	12.699	6.548
8	11.555	11.502	6.906

(*continued*)

Table 4. (*continued*)

Number of experiments	Social media privacy data cloud storage method based on encryption algorithm	Storage method of social media privacy data cloud based on neural network	This paper describes the privacy data cloud storage method for social media software
9	12.061	10.377	5.877
10	11.499	12.515	6.199
11	12.554	11.026	6.311
12	10.948	10.369	8.463
13	9.648	11.549	9.745
14	8.697	12.566	8.642
15	10.612	11.825	7.480

As can be seen from Table 4, the storage time of the privacy data cloud of the social media software is 7.292 s, 10.593 s and 11.470, respectively, compared with the other two methods.

The above experimental data show that the present method has a good cloud storage function of private data. We formulated the user identity restriction scheme according to the scope of account availability, and classified the risk factors of privacy information. We have improved the data reading mode, adjusted the data independence, used the blockchain to build the cloud storage structure, and improved the cloud storage performance of the data.

3 Conclusion

The design of social media software privacy data cloud storage method, improve the data in the block chain storage structure. This paper clarifies the connotation and classification of privacy information of individual users in cloud storage environment, and summarizes its risk categories as management risk, technical risk and legal risk. In addition, the data and interface of block chain transaction are adapted and encapsulated, and the method of reading and writing data on the chain is defined. On this basis, we have improved the way data is read and adjusted for data independence. Using the blockchain to build a cloud storage structure, an identity management mechanism for data access on the chain is designed to strengthen the protection of related data. In the cloud storage environment, the main ways of users' privacy information disclosure are overingestion by cloud storage service providers and theft of privacy information caused by hacker attack or management vulnerability. To strengthen the internal staff's professional ethics education, in the business level to balance commercial profits and privacy protection of the contradictory two levels have a role in promoting. At the same time, the technical level to establish a self-inspection mechanism to eliminate hidden dangers. We define the sharding storage method and optimize the access mode of file data, improve the

efficiency of data synchronization of distributed file storage module, and reduce the time consumption.

References

1. Hai-chun, Z., Xuan-xia, Y., Xue-feng, Z.: Cloud storage data integrity audit based on an index-stub table. Chin. J. Eng. **42**(4), 490–499 (2020)
2. Shi, C., Lai, M., Li, S., et al. Integrity verification of dynamic multiple-replica data in cloud storage. J. Chengdu Univ (Natl. Sci.) **39**(1), 64–68 (2020)
3. Li, S.-Q., Liu, L., Zhu, D.-Y., et al.: Protocol of dynamic provable data integrity for cloud storage. Comput. Sci. **47**(2), 256–261 (2020)
4. Wang, L., Xu, Y., Kang, Y.: Simulation of node-level data privacy protection mining method in cloud computing. Comput. Simul. **37**(10), 433–436, 460 (2020)
5. Liu, G.-J., Xiong, J.-B., Zhang, L.-N., et al.: An efficient privacy-preserving data auditing scheme for regenerating-code-based cloud storage. J. Southwest Univ. (Natl. Sci.) **42**(10), 37–45 (2020)
6. Zhu, Y.-J., Yao, J.-G., Guan, H.-B.: Blockchain as a service: next generation of cloud services. J. Softw. **31**(1), 1–19 (2020)
7. Wang, Q.-C., Chen, Q.-Y., Zhang, C., et al.: Study of medical privacy data security protection in 5G cloud-side collaboration scenarios. Telecom Eng. Tech. Stand. **33**(12), 64–67 (2020)