ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

Privacy retrieval method of big data in mobile network based on edge computing

Pingping Jiao, Xianchun Zhou

School of Information and Intelligence Engineering, Sanya University, Sanya, Hainan, China
zhouzishun2005@163.com

Abstract: *In order to better achieve the goal of big data privacy retrieval and ensure user data security, a mobile network big data privacy retrieval method based on edge computing is proposed. Combined with the principle of edge computing, identify the privacy characteristics of mobile network big data, build a feature database for data management, optimize the privacy data security encryption algorithm, and simplify the privacy retrieval process of mobile network big data. Finally, experiments show that the mobile network big data privacy retrieval method based on edge computing has high security and effectiveness in the process of practical application, and fully meets the research requirements.*

Keywords: *edge calculation; Mobile network; Data privacy; Data retrieval*

1. Introduction

When carrying out mobile network big data retrieval service, users are most concerned about whether the security and privacy of data are well protected. In the process of data retrieval, users lose their physical control over the data[1]. The security and privacy of data depend on the security protection measures taken by cloud service providers, If the security measures are damaged by external hackers or internal personnel of cloud service providers, users' sensitive data may be exposed, and the security and privacy of data will be seriously damaged. There are many kinds of data security and privacy protection, the most important of which is the use of cryptography, but this method also brings two main problems: one is how to query and search the ciphertext status data and how to accurately share the ciphertext to the designated users after the data is encrypted[2]. The second is how to protect the differential privacy of data to prevent users from mining sensitive information from publicly published data. In the process of big data privacy retrieval, there are many researches at present, which can be divided into two categories: symmetric searchable encryption and asymmetric searchable encryption. In the process of searchable encryption, users submit query traps, entrust ECs to query and match on the encryption index, and return the corresponding ciphertext results to users. However, the above methods are safe, efficient. There are still some deficiencies in functionality. On the one hand, most of the traditional privacy protection ciphertext query protocols are committed to resisting untrusted cloud attacks, and need to rely on privacy computing or trusted third parties to authenticate the legitimacy of users, lack of effective access control strategies, and the security needs to be strengthened[3]. On the other hand, most of the existing searchable encryption technologies are based on the design of tight cipher algorithm. The calculation is usually large, and multiple rounds of interaction between users and ECs are required, which greatly increases the communication between users In addition, the existing ciphertext query system model is only suitable for single user system, and only pays attention to the precise query of single keyword However, in practical application, multi-user model and multi keyword similarity search are more common[4]. At present, there is a lack of effective methods for ciphertext query in multi-user model. Based on this, a privacy retrieval method of mobile network big data based on edge computing is proposed.

2. Mobile network big data privacy retrieval

2.1. Mobile network big data privacy feature recognition

In essence, mobile network big data is an event driven state determination program deployed on distributed database[5]. The working principle of mobile network big data designed and developed in the early stage is no different from that of other computer programs. It was not until it was integrated

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

into the blockchain technology framework by Ethereum platform that mobile network big data played a greater value, which also upgraded the blockchain from the 1.0 era to the 2.0 era[6]. The application concept of mobile network big data in blockchain is that it is effectively realized with the help of blockchain architecture, which has the characteristics of decentralization and distrust, and has an executable environment, as shown in the figure 1.

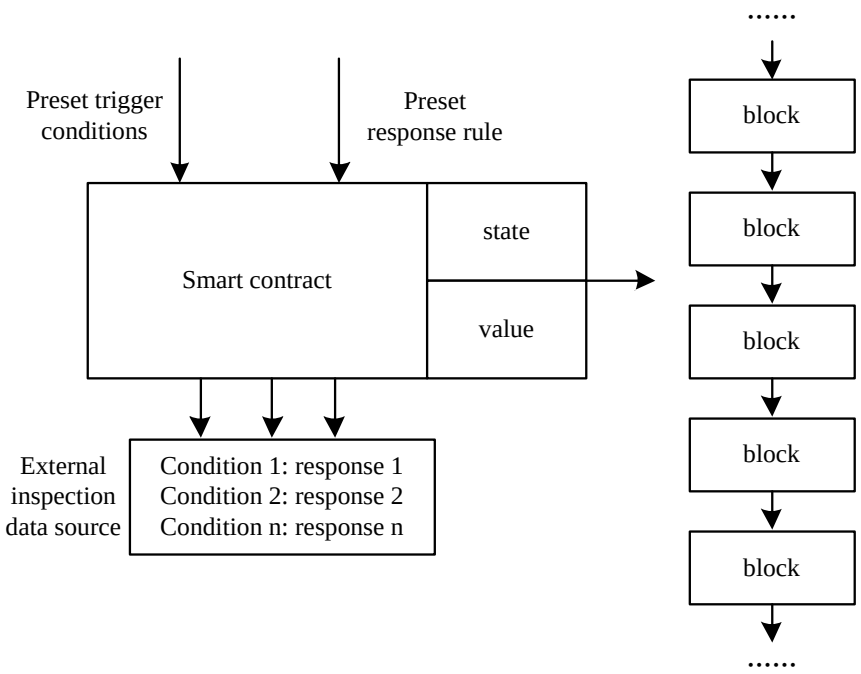

Figure 1: Mobile network big data workflow

Mobile network big data usually understands the script code agreed by multiple nodes and stored in the transaction in the blockchain after verification. Users can call mobile network big data after obtaining the contract address and interface through the service call of the application layer. Nodes execute the contract code and verify the results under a certain incentive mechanism[7]. After the contract is triggered, a special transaction form is formed. After the transaction is verified to be effective, it is packaged into a new block. With the continuous development of the Turing complete blockchain platform, mobile network big data is becoming more and more "smart" in the blockchain architecture. There are many transactions of different sizes in the blockchain network, and a certain number of transactions will be packaged into blocks after verification[8]. The block structure is divided into block header and block body. The block header contains the basic information used to identify the block. The block body is mainly composed of many transactions. As shown in the figure 2. These blocks take time as the axis and are finally connected into a blockchain.

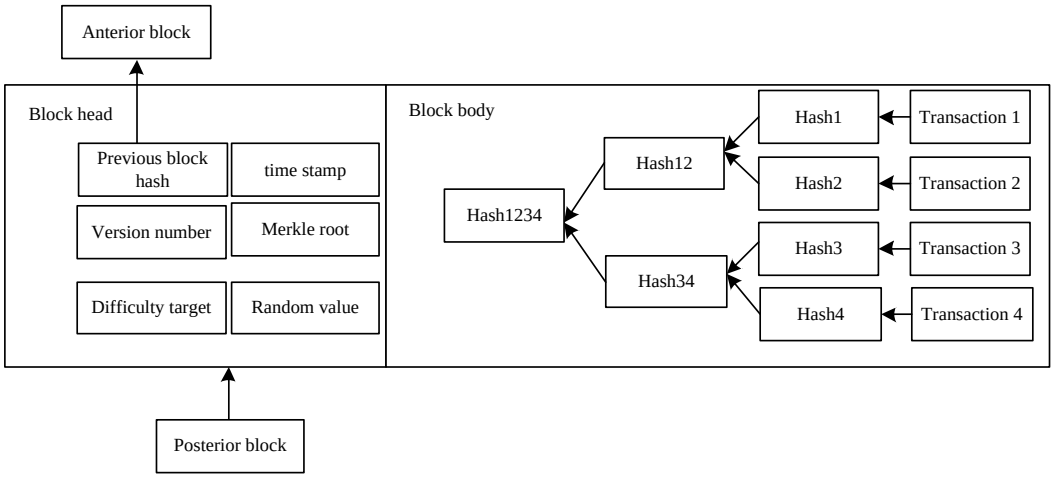

Figure 2: Blockchain privacy protection

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

In blockchain privacy protection, transaction privacy and identity privacy, as the core content of privacy protection, are at risk of disclosure at all levels of blockchain architecture. Therefore, it is necessary to propose new privacy protection technical means to effectively strengthen the data security capability of blockchain architecture[9]. According to the hierarchical characteristics of blockchain architecture, the privacy protection schemes currently studied are divided into network like privacy protection. The focus of network layer privacy protection is to limit the access of distributed nodes to blockchain data, resist network monitoring and network attacks. Privacy protection at the transaction level. The purpose of transaction layer privacy protection is to hide the plaintext transaction information and sensitive information behind the data without changing the existing consensus algorithm and verification mechanism of the blockchain[10]. Application layer privacy protection means mainly include enhancing security awareness, improving information protection ability, and improving the server defense ability of blockchain service providers.The specific classification of privacy protection schemes is shown in Table 1.

Table 1: Classification of privacy protection schemes

Network hierarchy	Privacy attack risk	Privacy protection scheme
network layer	IP monitoring: network topology analysis;	Network layer data confusion; Network access restriction; Malicious node location and shielding
Transaction layer	Transaction address analysis; Disclosure of transaction data;	Based on data encryption technology; Based on data distortion technology; Provider service security
application layer	The service safety factor of the provider is low: the user's operation is not standardized	Reasonably select blockchain platform: use blockchain client with high protection ability

In order to enhance the privacy and security of data on the blockchain and meet the efficient sharing of data, as well as the privacy and security of users, this scheme selects the alliance chain to propose the underlying blockchain network service. Compared with the public chain, the alliance chain is only open to designated users and third parties, which has more advantages in efficiency and flexibility[11]. The efficiency of pbft consensus algorithm used in the alliance chain is much higher than that of POW and POS consensus algorithm used in the public chain environment. In addition, the data collaboration scheme on and off the chain proposed in this paper should also meet the following design objective[12]. Privacy: the data of data providers should not be shared and downloaded by everyone, and corresponding access rights should be set to be open to limited data requesters to ensure the basic data privacy and security. Synergy: the storage space on the blockchain is extremely valuable and limited, Generally, the specific content of the data cannot be stored on the chain. The specific data is stored off the chain, while the scheme of storing the corresponding pointer on the chain needs to ensure the consistency of the data on the chain and off the chain[13]. The two parts form a system as a whole, which is efficient: in order to package the blocks efficiently, the underlying blockchain network service needs to build an efficient block transaction structure, To improve the performance, efficiency and expansibility of data sharing: when adding and deleting nodes in the blockchain system, it has less impact on the functions of the existing system. It is necessary to design a consensus algorithm matching the functions to realize the scalability of the system.

2.2. Privacy data security encryption algorithm in mobile network

Among many information retrieval models, edge computing model is the most popular method of correlation measurement. It is widely used in plaintext multi keyword retrieval, and supports both connection search and disjunctive search. Where TF refers to word frequency, that is, the frequency of keyword w in the data, NW divided by the total number of words contained in data F. DDF represents the inverse data frequency, that is, the number of data n divided by the number of all data containing the keyword n. The data vector F and the query vector Q are vectors of the same length generated by the keyword w through the mapping of the keyword dictionary N, where each dimension in N is the W value after the standardization of the corresponding keyword $N_{f,w}$, and each dimension in Q takes the IDF value after the standardization of the keyword f. The calculation formula of $IDF_w^{'}$ value and R value after keyword w standardization is as follows:

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

$$IDF_w^{'} = \ln W\left(1 + N / N_w\right) \tag{1}$$

$$TF_{f,w}^{'} = \left(1 + \ln N_{f,w}\right) / |f| \tag{2}$$

$$TF_{f,w} = TF_{f,w}^{'} / \sqrt{\sum_{w \in W}\left(TF_{f,w}^{'}\right)^2} \tag{3}$$

$$IDF_w = R / \sqrt{\sum_{w \in W}\left(IDF_w^{'}\right)^{2N}} \tag{4}$$

Edge computing is an important measure for distributed systems to maintain data consistency, and edge computing used by various blockchain systems is mainly divided into two categories: proof consensus and voting consensus. There is also a kind of cooperative consensus, and the entrusted equity certificate has its own advantages and disadvantages. Edge computing POW consumes resources, and POS consumes "capital liquidity". Dpos votes for nodes as agents. Similar to permanent members, edge computing without consumption is basically impossible[14]. Among them, the workload proves that it has high stability and safety after time, but the consensus speed is slow and energy consumption is serious. Moreover, mining is also prone to computational force centralization, but it is still the most mainstream consensus algorithm.The differences of different consensus encryption algorithms are shown in Table 2.

Table 2: Comparison of consensus encryption algorithms

	PoW	PoS	PBFT	CFT
Applicable blockchain types	Public chain	Public chain	Alliance chain	Alliance chain
Consensus efficiency	low	commonly	higher	high
Consensus finality	Probability class	Probability class	Determine class	Determine class
Computing power / resource consumption	high	commonly	Lower	low
Applicable trust environment	Untrusted	Untrusted	Semi credible	credible
Error tolerant node rate	<=26%	As the case may be	<=35%	<55%

The query complexity, regardless of the reconstruction operation, is the mapping set size of the query label: $O\{\#MM[\ell]$, while the query time complexity is when dynamic update is supported：

$$O\{\#MM[\ell] + del(\ell, e)\} \tag{5}$$

Among them, $del(\ell, e)$ is the number of recently searched tags deleted since the last reconstruction cycle e (epoch), and the spatial complexity is the sum of the sizes of all existing tag l edges:

$$O\left\{\sum_{\ell \in LMM}(\#MM[\ell] + del(\ell, e)\right\} \tag{6}$$

Edge computing sharing scheme is one of the important tools of modern cryptography, also known as (TN) secret sharing scheme, in which t ≤ n. The main description is as follows: the secret owner divides the secret s into n shares and distributes it to n secret requesters through polynomials. The secret s can be recovered only when the secret requester has t shares. The specific process is as follows: let p be the set of all secret participants, let x_i be the ith participant in n participants, let the secret to be shared by the secret owner be a random number s ∈ Z, then a random polynomial j with order s_i is required, and $L_{i,S(x)}$ is the secret share s = P (x) of the ith participant $P(I)$. If the secret requester in

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

the secret requester subset is defined as $L_{i,S(x)}$, the following can be calculated:

$$\begin{cases} L_{i,S(x)} = P(I)\Pi \dfrac{x_i - j}{s_i - z_j}, j \in S, j \neq i \\ p(j) = P(x)\sum s_i * L_{i,S(x)} \end{cases} \tag{7}$$

Different from the construction concept of identity encryption, the edge computer system provides an access structure strategy to indicate what characteristics the accessed data requester should have. The object of decryption is a collection of data requesters with some of the same characteristics, not a specific individual[15]. The early encryption sharing mode is usually one-to-one, and the proposal of edge computing expands it to one-to-many, It is safe, efficient and flexible. In the edge computing scheme, the data provider encrypts the data after formulating the access policy. If the data requester meets the specified attribute characteristics, it can calculate and decrypt the ciphertext data. The calculation of edge computing encryption and decryption data is related not only to the length of the ciphertext, but also to the scale of the number of attributes. There is no need for interaction between encryptors and decryptors, Through the setting of access policy, data can be shared safely[16]. Bloom filter has such a high efficiency performance, but also has a disadvantage that can not be ignored, that is, the false alarm rate m, that is, the probability that the calculation result of the element that should be judged not to exist exists. Assuming that the size of the bloom filter array is m and the hash function set has $e^{-\frac{kn}{m}}$ hash functions, the probability that a bit of the array is not set to 1 in the mapping process is:

$$\left(L_{i,S(x)} - \left(1 - \frac{1}{m}\right)^{kn} \right)^k \approx p(j)\left(1 - e^{-\frac{kn}{m}}\right)^k \tag{8}$$

Counting query is the basis of many complex statistical queries. For the scene where the search record items are clustered in one data block, for the count query Q on the target data set. $q(E) + lap(1/a)$ will be returned α- Differential privacy, where $Q(E)$ is the accurate statistical result and lap (1 / Ag) is the noise consistent with the edge calculation (Note: the global sensitivity of count query is 1). For the counting query across multiple data blocks, the query can be classified as a batch linear query composed of a series of sub queries, in which the target records of each sub query are clustered in a data block[17]. Linear query The linear query can be regarded as the linear weighted algebraic sum of finite count queries, that is, given the weight vector $w_1, w_2, ..., w_m$, the linear query $Q(t_1), Q(t_2), \ldots, Q(t_m)$ returns the inner product between the weight vector and the count query vector:

$$Q(E) = w_1 Q(t_1) + w_2 Q(t_2) + \cdots + w_m Q(t_m) \tag{9}$$

Add the noise calculated based on the edge, and the corresponding compliance α- The search results of differential privacy mechanism are:

$$M(Q,E) = Q(E) + \sum_{i=1}^{m} \mathrm{Lap}(\Delta s_i / \alpha) \tag{10}$$

Batch linear query Batch linear search is a set of search tasks composed of m linear searches submitted at the same time. The search task set w_{1j} is represented by a weighting matrix W rows and T columns. Any element w in W is the j-th weight coefficient of linear query $Q(t_j)$ about record item t. Batch linear search Q (E) can be formalized as

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

$$\Delta Q(E) = WT - M(Q,E)\left(\sum_{j=1}^{n} w_{1j} Q\left(t_j\right), \ldots, \sum_{j=1}^{n} w_{mj} Q\left(t_j\right)\right) \tag{11}$$

Then:

$$\begin{cases} Q_1 = Q_1^{'} + 2Q\left(T_1\right) + Q\left(T_3\right) - Q_2^{'} / 2 \\ Q_2 = Q\left(T_1\right) + 2Q\left(T_3\right) n \\ Q_3 = 2Q_1^{'} + 2Q\left(T_3\right) + Q_2^{'} / 2 \end{cases} \tag{12}$$

Among them, Q1, Q2 and Q3 meet the L distance of additional noise of differential privacy. Therefore, for batch linear query, due to the difference of schemes to realize differential privacy, different data availability may be caused[18]. Replace r m-dimensional vectors in the encryption process into the above formula for coding calculation, so as to obtain R data packets after coding processing in time, which are recorded as $b_1, b_2, ..., b_r$, the calculation formula is:

$$b_i = \Delta Q(E)[w_i - b_r\left(a_1, a_2, ..., a_m\right)^t], i = 1, 2, ..., r \tag{13}$$

The information source node a completes the unified packaging processing of the encoded data and the corresponding encoded information vector, so that w encoded data packets can be obtained and transmitted to the target node[19]. The target node receives enough information, and the vector generated after coding is non-linear, so it can obtain the initial data matrix, as shown below:

$$\begin{bmatrix} \mathrm{a}_1 \\ \mathrm{a}_2 \\ \vdots \\ \mathrm{a}_m \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \ldots & w_{1\mathrm{m}} \\ w_{21} & w_{22} & \ldots & w_{21} \\ \vdots & \vdots & & \vdots \\ w_{r1} & w_{r2} & \ldots & w_{rm} \end{bmatrix} \begin{bmatrix} b_1 \\ \mathrm{b}_2 \\ \vdots \\ \mathrm{b}_r \end{bmatrix} \tag{14}$$

The initial fingerprint stored by the key user is selected according to the formula initial data matrix. The fingerprint is composed of 512 bytes, which is relatively safe for the device key storage. However, the solution space formed by the optimization strategy based on query decomposition is infinite. In the current edge calculation methods, finding the best denoising scheme is still an open problem, which is also the focus of cocktail's future scientific research work.

2.3. Implementation of data privacy call retrieval

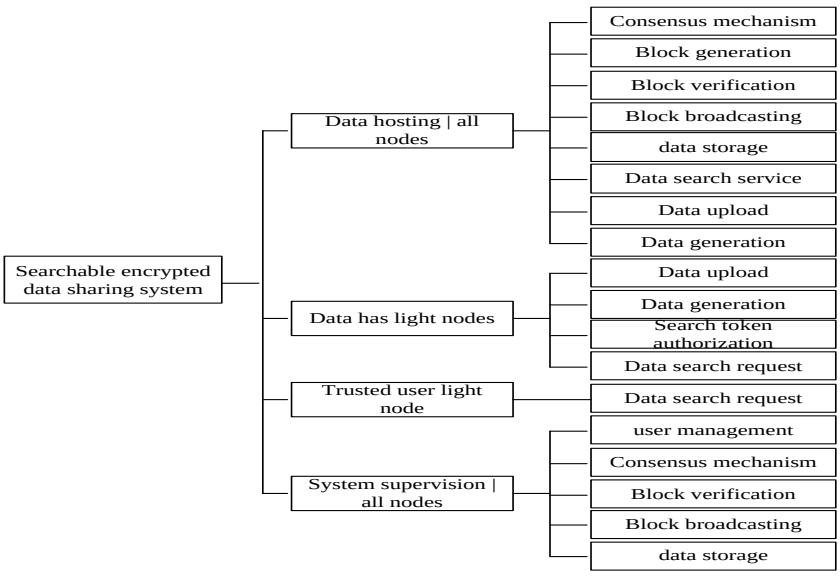

Figure 3:Network data privacy information management system

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

All operations need to be announced throughout the network to prevent regulatory nodes from doing evil. Because of its large authority and great destructiveness, it needs to test the data. Even if the scheme supports verifiability, it can also be used as an arbitration institution for verification[20]. Therefore, it is necessary to retain complete data and participate in the specific node division of consensus, as shown in the figure 3.

The automatic resource situation retrieval module includes a number of physical retrieval operation equipment such as virtual machine and physical machine, which can realize the retrieval index acquisition operation of resource situation in task layer and function layer. The physical machine is an important component of the edge computing and retrieval platform. It can generate the occupancy index related to the resource retrieval situation, and judge whether the current resource node is in the retrieved state according to the specific physical difference between the value and the resource occupancy threshold. The virtual machine structure in the abnormal connection state will have a strong blocking effect on the physical machine resource retrieval node. When the database is not enough to support the current operation status of the system, the virtual machine can release the abnormal connection state, which is also the main reason why the data in the new system can quickly reach the upper limit of retrieval occupancy. The query request is the core function of the system, which is mainly divided into two types of node requests: data owner and non data owner. The first type only involves the interaction with the service node, and the second type requires three-party interaction. The process of query service is shown in the figure. When the client receives the query request, it first determines whether it is the data owner. If not, it needs to request the owner to obtain the search voucher. If the request fails, the process ends directly; Then, if it is authorized (or the owner generates the search voucher), the client will send the search voucher to the server, and the search server will perform the search operation according to the voucher and return the results to the user. The request is successful, and the process ends.

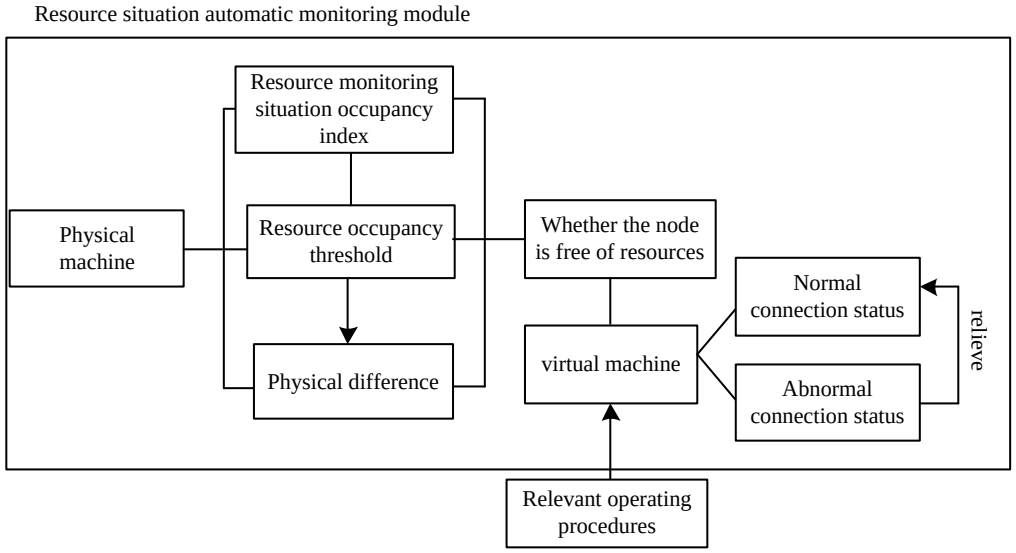

Figure 4: Privacy data query process

Through the implementation of the prototype system, according to the basic functional requirements, some test cases are designed and simple functional tests are carried out. This prototype system realizes the automatic parsing of documents to obtain text, and then divides the data according to certain rules. This paper uses the inverted index construction according to each transaction as a data, and the actual use can be modified according to the specific needs; after the index is built, other operations are similar to general searchable encryption. Attention should be paid to edge calculation. The function of the system is tested through five test cases, and the realized functions are shown in the table 3.

Table 3: Function test results

Function name	User oriented	Available
Members join the Alliance	Data owner and data keeper	yes
Data search query	Data owner, authorized data user	yes
Member management	Data Supervisor	yes
Data upload	Data owner or data custodian	yes

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

Member management is directly implemented on the basis of fabric's member service MSP. Currently, data storage directly exists in the server. In the future, we can consider using IPFs protocol for decentralized storage to alleviate the pressure. If the data hosting has an incentive mechanism, it can promote the data hosting node to actively save data and provide query services for users. In this way, it can be closer to the practical application. Consider using filecoin for improvement.

3. Analysis of experimental results

The experimental environment adopts hybrid Cloud Architecture, in which the public cloud contains three nodes connected by ws-c3750x24ts switch, and each node adopts Xeon f5506core2 13 GHz CPU, 16G dual channel 133 GHZ memory, and in Hadoop 0 Hive0 is built on 20.203 7.1; The private cloud contains two nodes. Each node has the same configuration as the nodes in the public cloud. One node executes jobtracker for namenode In Hadoop, 8 map tasks and 8 reducetasks are configured for each node. The following table reflects the setting of relevant experimental parameters of the experimental group and the control group.The experimental parameter setting table is shown in Table 4.

Table 4: Experimental parameter setting table

Parameter name	numerical value
Host type	Client / server host & Client / proxy / server host
Cloud platform type	Oracle cloud
Database organization	mysql
Experimental time	60min
Resource monitoring coefficient	0.76 (transverse) 0.85 (longitudinal)
Data fixed point interaction limit	85.67%
Resource scheduling integrity limit	73.15%

The operating system is Ubuntu 11 04。 Three test data sets 23 were used in the experiment, including POS, WVI and wv2, as shown in the table 5.

Table 5: Description of experimental data set

data set	Number of records	Number of record items	Maximum record length	Average record length
POS	515,598	1,658	165	6.6
WV1	59,603	498	268	2.6
WV2	77,526	3,365	162	5.1

Through the experimental analysis of the retrieval method in this paper, the maximum number of child nodes pointed to by the middle node of the index tree is analyzed α, Retrieve the number of returned data, data sub cluster threshold μ, The relationship between the number of retrieval keywords QW and retrieval efficiency is experimentally measured: at the same time, the index space is compared with the traditional bdmrs index tree and bmuse index tree. N is the number of all data contained in the experimental data set. We conducted experiments on 12000 real data sets. The operating system is windows10 and the running environment is eclipse. The figure shows the experimental results with a data set of 120000.

In order to effectively verify the effectiveness of data multi round refinement privacy algorithm, compared with the classical distributed dak method, three groups of comparative experiments are designed (for ease of description, the experiment takes two-way data fusion as an example). The experiment first constructs a data table containing 22 attributes, 1 × Data set of 10^5 records. The attribute A1 is the record ID and the attribute A2 is the class attribute. The pseudo machine is used to generate 1 in the value field of each attribute × 105 records, where a represents the generalization distance of attribute layer a, and the distance of all record values in the same class formed by attribute layer generalization shall not be greater than dak. For different privacy degrees k{10,20,30,40,50}, the corresponding time is shown in the figure. The multi round refinement algorithm is not sensitive to privacy (i.e. the time to maintain a relatively constant), while the time of DKA algorithm increases linearly with the increase of privacy.

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

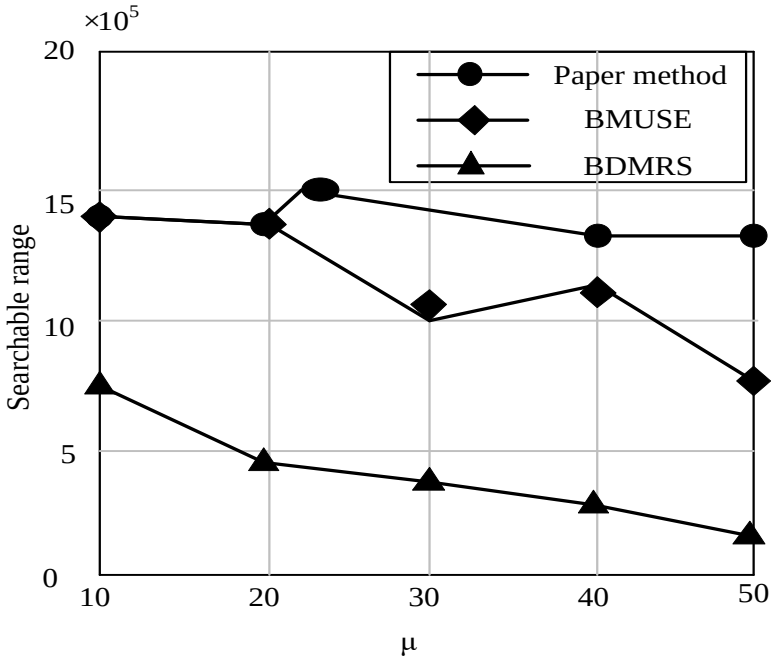

Figure 5: Effect of data sub cluster threshold on index space

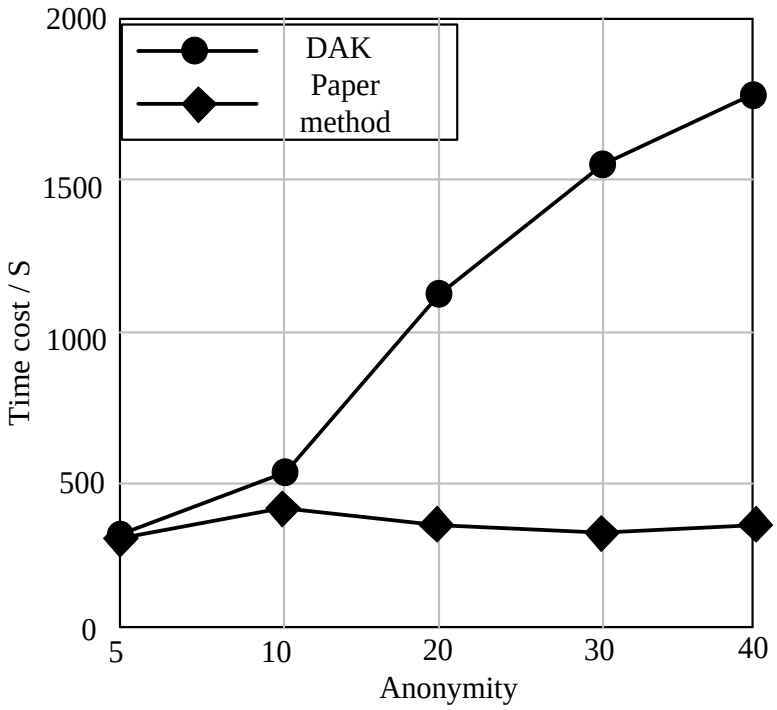

Figure 6: retrieval time of the same data with different degrees of privacy

Set the privacy k = 20 and select 5 different data sets. The generation method of the data set is the same as above, and the scale is from 5×10^4~25×10^4. The time is shown in the figure: the multi round refinement algorithm is not sensitive to the number of records, that is, it maintains a constant time, while the time of dak algorithm increases superlinearly with the increase of the size of the data set to be fused.

Under the same retrieval conditions, the space of index trees constructed under different conditions is compared by changing the influence factor a. The figure shows the experimental results with a data set of 120000.

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

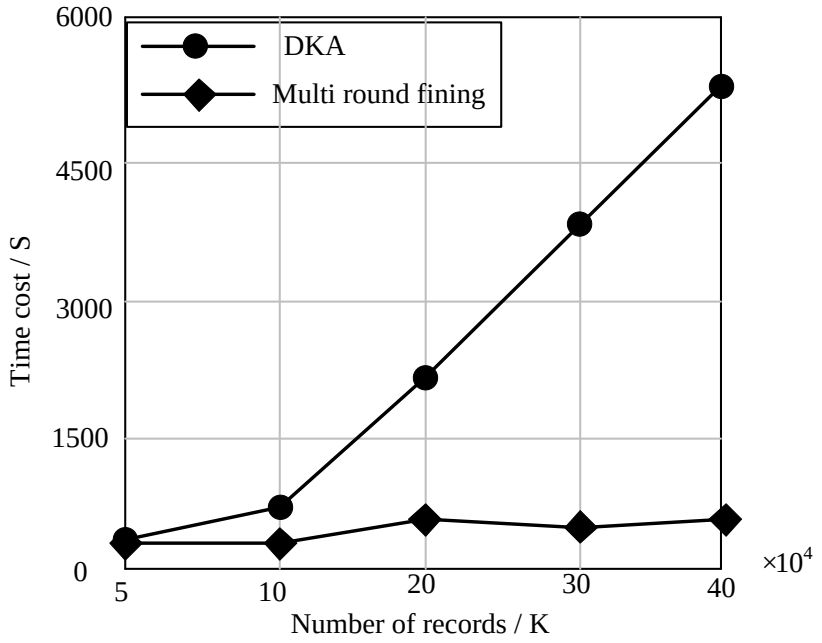

Figure 7: Data retrieval time of different data volume with the same privacy

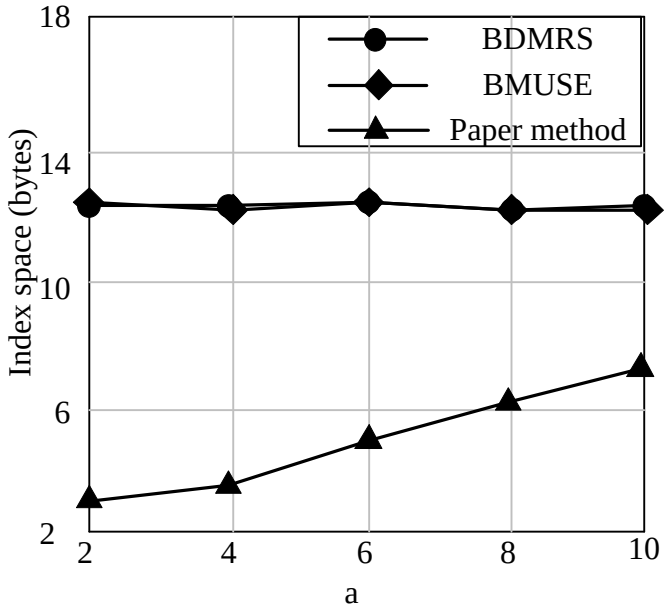

Figure 8: Information security impact of variable a on index space

It can be found from the figure that when the data set is kept constant and the influence factor A is changed, the index space decreases first and then increases, and reaches the minimum when $\propto = 3$. This is because with the increase of a, the number of child pointers of each intermediate node becomes more, resulting in the larger space occupation of a single node. It can be seen that under the same conditions, the larger the data set, the longer the retrieval time of traditional methods: when the total number of data remains unchanged, the retrieval method proposed in this paper fluctuates unsteadily with the increase of time, and has a gradually increasing trend. On the whole, the retrieval efficiency of the method proposed in this paper is significantly higher than that of bdmrs index tree and bmuse index tree.

4. Conclusions

Focusing on the problems of data security and privacy protection in the edge computing

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

environment, it is pointed out that the important methods to ensure data security and privacy are encryption and differential privacy protection, and further expounds the research status of edge computing data security and privacy protection at home and abroad from three aspects: ciphertext query, ciphertext sharing and differential privacy; Then, it focuses on the spatial keyword ciphertext query technology and fine-grained ciphertext sharing technology across cryptosystems proposed by the research team, and gives the main research ideas. However, at present, there are still some problems to be solved in data security and privacy protection in the edge computing environment, such as spatial multi keyword search for dynamic update of user location and keywords Forward secure and backward secure multi keyword searchable encryption, adaptive secure cross cryptosystem ciphertext sharing, and high availability differential privacy protection technology.

Acknowledgments

[1]The Natural Science Foundation of Hainan Province:Research on Key Technologies of malware homology determination based on maximum frequent subgraph gene (No:620MS064)

[2]Sanya University and medical special science and technology plan project：esearch on smart tourism construction in Hainan Province Based on big data（No.:2021GXYL54）

References

[1] Zhang W, Chen X, Liu Y, Xi Q. 2020, A Distributed Storage and Computation k-Nearest Neighbor Algorithm Based Cloud-Edge Computing for Cyber-Physical-Social Systems. IEEE Access, PP (99):1-1.

[2] Sun Y, Song C, Yu S, Liu Y, Zeng P. 2021, Energy-Efficient Task Offloading Based on Differential Evolution in Edge Computing System With Energy Harvesting. IEEE Access, 9:16383-16391.

[3] Xie Y. 2021, Research on Vertical Search Method of Multidimensional Resources in English Discipline Based on Edge Computing. Mobile Information Systems, 2021(1):1-10.

[4] Kim J, Lee J, Kim T. 2021, AdaMM: Adaptive Object Movement and Motion Tracking in Hierarchical Edge Computing System. Sensors, 21(12):4089.

[5] Martino B D, Venticinque S, Esposito A, D'Angelo S. 2020, A Methodology Based on Computational Patterns for Offloading of Big Data Applications on Cloud-Edge Platforms. Future Internet, 12(2):28.

[6] Andrejev A, Orsborn K, Risch T. 2020, Strategies for array data retrieval from a relational back-end based on access patterns. Computing, 102(5):1139-1158.

[7] Cw A, Fang Q B, Djsr C. 2020, Cloud assisted big data information retrieval system for critical data supervision in disaster regions - ScienceDirect. Computer Communications, 151(56):548-555.

[8] Li Z F. 2021, Research on mobile network coverage quality evaluation method based on grid and big data. Wireless Internet technology, 18 (09): 24-25.

[9] Gezawa A S, Zhang Y, Wang Q, Lei Y. 2020, A Review on Deep Learning Approaches for 3D Data Representations in Retrieval and Classifications. IEEE Access, 8(6):57566-57593.

[10] Marcos-Pablos S, FJ Garc ́a-Pealvo. 2020, Information retrieval methodology for aiding scientific database search. Soft Computing, 24(8):5551-5560.

[11] Seeling P. 2020, WWW Retrieval Handling Optimization wp3: A metric for webpage timeout setting performance evaluation and comparison - ScienceDirect. Future Generation Computer Systems, 110(3):1055-1066.

[12] B Y W A, A J L, B W D, Xiaolong Xu c, Buqing Cao a, Jinjun Chen a d. 2020, Scheduling workflows with privacy protection constraints for big data applications on cloud. Future Generation Computer Systems, 108(3):1084-1091.

[13] Liu J M, Zhao H Q, Liu C, Jia QQ. 2021, Privacy Data Security Policy of Medical Cloud Platform Based on Lightweight Algorithm Model. Scientific Programming, 2021(4):1-9.

[14] Sheikhalishahi M, Saracino A, Martinelli F, Marra AL. 2021, Privacy preserving data sharing and analysis for edge-based architectures. International Journal of Information Security, 34(12):1-23.

[15] Zapechnikov S. 2021, Contemporary trends in privacy-preserving data pattern recognition. Procedia Computer Science, 190(4):838-844.

[16] Aivazpour Z, Rao V. 2020, Information Disclosure and Privacy Paradox: The Role of Impulsivity. The data base for advances in information systems, 51(1):14-36.

[17] Hua J. 2020, A privacy-enhancing scheme against contextual knowledge-based attacks in location-based services. Frontiers of Computer Science, 14(3):1-4.

ISSN 2616-5775 Vol. 5, Issue 9: 65-76, DOI: 10.25236/AJCIS.2022.050911

[18] Kousika N, Premalatha K. 2021, An improved privacy-preserving data mining technique using singular value decomposition with three-dimensional rotation data perturbation. The Journal of Supercomputing, 34(6):1-9.

[19] Gsa B, Xx A, Zq A, Wei LLB. 2021, Edge computing assisted privacy-preserving data computation for IoT devices. Computer Communications, 166(4):208-215.

[20] Hussain A, Lasrado L A, Mukkamala R R, Tanveer U. 2021, Sharing Is Caring – Design and Demonstration of a Data Privacy Tool for Interorganizational Transfer of Data. Procedia Computer Science, 181(PB):394-402.