Journal of Global Information Management
Volume 30 • Issue 11

Ciphertext Database Audit Technology Under Searchable Encryption Algorithm and Blockchain Technology

Jin Qiu, Guangdong University of Science and Technology, China*

ABSTRACT

The study aims to solve the problems in auditing ciphertext data, improve audit efficiency, and increase the security of audit data in the audit server. First, the existing encryption algorithms are analyzed. Second, the searchable encryption algorithm is proposed to audit the ciphertext data, and an audit server scheme is made based on blockchain technology (BT). Finally, the two schemes are compared with the traditional audit technology. The results show that the server's inspection efficiency of the searchable encryption algorithm is higher.

KEYWORDS

Blockchain, Ciphertext Audit, Homomorphic Encryption, Searchable Encryption

1. INTRODUCTION

With the development of computer technology, more and more data security problems are exposed (Pajany and Zayaraz, 2021). In 2018, network security incidents worldwide had caused a total loss of more than 45 billion US dollars. In 2019, a Philippine financial service company is attacked by hackers, resulting in data leakage. Nearly 900000 users' data are stolen and sold on the network. The reason for this is that database security is not guaranteed. Database audit is an essential technology to ensure data security. It can record all the actions that have operated on the database in real time and analyze these operations. If there is a problem during the audit, it can help maintenance personnel quickly analyze and locate the problem in time, preventing data leakage and protecting data security (von Sanden and Neideck, 2021). With the development of the era of big data, Blockchain Technology (BT) has penetrated into all walks of life and gained much attention in auditing. BT first appeared in the form of Bitcoin. BT is the underlying technology of Bitcoin and was first used in Bitcoin. At present, the research of BT in audit database servers is relatively shallow (Feng & Chen, 2022) (Wang et al., 2020).

Although it can audit users' information efficiently, the plaintext audit scheme also causes user privacy disclosure. In contrast, the security of the ciphertext audit scheme is more reliable. With the

DOI: 10.4018/JGIM.315014 *Corresponding Author

improvement of the theoretical system, searchable encryption's application to audit work is getting more and more increasing. Jiang et al. (2018) proposed an audit protocol of principal-agent outsourcing data in the scenario of cloud computing. He used the asymmetric encryption algorithm to verify the integrity of data blocks and Hashtable to construct the index for the keyword dictionary of a data set to realize rapid search of keywords (Jiang et al., 2018). Li et al. (2021) proposed the searchable encrypted audit log in cloud storage system. The information to be audited is encrypted and transmitted by the asymmetric searchable encryption algorithm. The client is identified after the cloud service provider verifies the searchable encrypted audit log. This method protects the user's privacy and allows cloud service providers to monitor the behavior of clients in real time (Li et al., 2021). Hao et al. (2021) proposed an audit method based on a knowledge map. As a big data technology, the knowledge map has visualization characteristics and can analyze the relationship between entities. This method improves the audit efficiency, but the internal attack is not addressed in the audit (Hao et al., 2021). Li et al. (2021) put forward a search encryption scheme based on BT (Blockchain Technology). A searchable encryption algorithm based on symmetric encryption builds a distributed storage server. It can solve the problem that the search results of cloud service providers cannot be verified in an untrusted cloud server environment, resulting in incorrect information return (Li et al., 2021).

Through the research and comparison of cloud computing-based asymmetric encryption algorithm, knowledge graph-based audit algorithm, and symmetric encryption algorithm to improve audit efficiency and stability, there are two main database audit methods: (1) improving the existing encryption audit algorithm; (2) combining data audit with other technologies. However, these two types have a common problem. They do not take into account the security of user's information. In the audit, auditors have a large amount of confidential information. If auditors are not trusted, there appear serious information security accidents. In view of this, a database audit technology based on a searchable encryption algorithm is proposed. According to all the behaviors of users, the audit database is constructed. With the increase or decrease of the client, the audit database is updated automatically in real time, and the key phrases are generated on the audit server. The audit keywords are obtained through the audit algorithm to complete the user behavior audit. The audit technology can help auditors complete the audit without the secret order key, ensuring data security. All operation processes are clear and transparent, and auditors cannot modify the audit server maliciously.

2. INTRODUCTION TO DATABASE AUDIT THEORY AND AUDIT-RELATED ALGORITHMS

2.1 Database Audit Theory

2.1.1 Database Audit Concept

Audit means the inspection and verification of the integrity and accuracy of the target, and it verifies whether the data comply with the set initial rules, especially the audit of some false data and fraud. It was first applied to the financial system and widely used in the financial statement of financial companies or banks, most of which are enterprises or organizations. The financial audit is conducted in its financial system. It also promotes the development of audit information technology (Maso et al., 2020). One of the main aspects of the audit is the judgment of the information system. The assessment includes whether the existing information system can protect data security, whether the data integrity can be maintained, whether the audited objectives can be completed efficiently, and whether the audited resources can be used fully (Stoel and Havelka, 2021). Database audit can completely record all relevant operations of the database. When they check the use of the database, the system security officers can get all information through the audit records, such as monitoring the operation behavior of designated users and checking the access status in the database. Database audit can track the operation of the user and ensure the using effect (Overman et al., 2019; Chen, 2020).

Because of its unique characteristics, database audit becomes an indispensable item in the database security mechanism. Specifically, the main functions of database audit are shown in Figure 1:

From Figure 1, the main functions of database auditing are divided into 5 categories. It can analyze the operating status of database systems, generate evidence to track illegal intruders, analyze the causes of dangerous operations and repair system vulnerabilities, facilitate database recovery and backup, and act as a deterrent to those who attempt to break the law.

2.1.2 Data Audit Model

The database audit system model includes the client, database server, general switch, firewall, equipment, and third-party auditors under supervision and audit. The specific entity interaction is shown in Figure 2:

The operation instructions that users need to execute are collected and encrypted with the searchable encryption algorithm, and a user behavior database for auditors is obtained. And the keyword of the operation instruction is encrypted into a password and sent to the database server. This process is for information encryption, ensuring data security in transmission, and preventing internal eavesdropping. It can be carried out by audit equipment for completing the audit of Structured Query Language (SQL) statements without decryption (Wu et al., 2022). The server's main function is to provide users with data storage and to encrypt or decrypt the data. First, the server decrypts the

Figure 1. Main functions of database audit

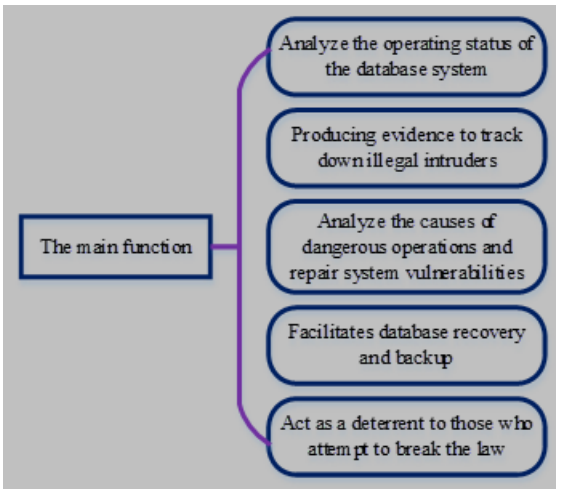
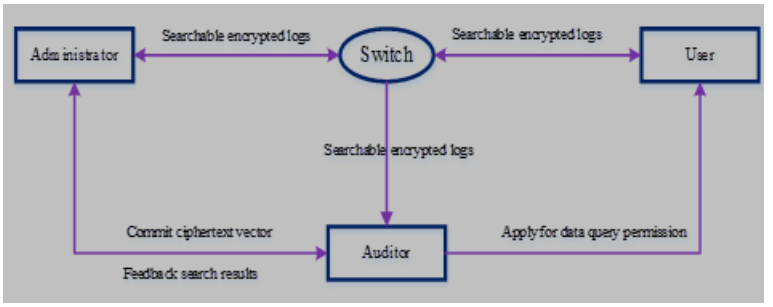


Figure 2. Entity interaction process of the data audit model



received data or ciphertexts sent by the user. Then, the searchable encryption algorithm is executed to verify whether the user's audit certificate is forged. After the authenticity of the audit certificate is confirmed, the decrypted plaintext is stored in the database. When they need to search some information, the auditors send a search request to the database. The database server performs the correlation algorithms according to the search keywords provided by the auditors. The data with a high correlation coefficient will be returned to the auditors, and decryption will be completed, so that the server can execute SQL statements normally (Srivaishnavi et al., 2021; Daniel et al., 2021; Tian and Wang, 2020; Yu et al., 2022).

The audit server is deployed in the bypass listening mode. BT is used to build a distributed audit database and execute relevant audit algorithms on the smart contract. The audit server obtains the data packet of the interaction between the user and the database server, parses the audit certificate in the packet, executes the audit algorithm, matches the key user behavior information, forms the audit data, and links the audit data. When they need to investigate and collect evidence from user data, auditors should get the license certificate at the user end, take the certificate as the input, execute the homomorphic encryption search vector generation algorithm, and send the search vector to the database server to obtain relevant user data. In this process, the role of the searchable encryption algorithm is to decrypt the trap gate in the audit certificate, and the decrypted plaintext is used for database audit by the audited equipment (Earnhart and Harrington, 2021; Shot, 2020).

After the abnormal data are detected, the auditors access the encrypted data in the database. First, they ask the data owner for the search vector of the relevant ciphertext and submit the search vector to the database administrator. The administrator calculates the correlation coefficient between the search vector and the ciphertext to obtain the ciphertext with the most significant correlation coefficient and feedback to the third-party auditors to decrypt and complete the audit work (Yan et al., 2019)(Chen & Zhang, 2022).

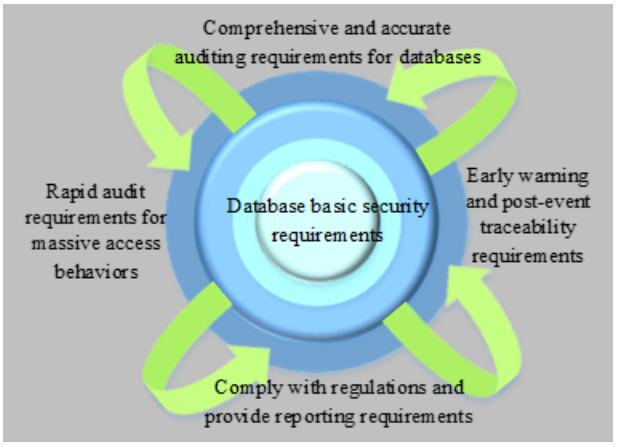
2.1.3 Database Audit Security Requirements

The audit function of databases is very powerful, and its security should also be guaranteed. The security requirements of the database are shown in Figure 3:

2.2 Relevant Algorithms

Relevant algorithms specifically refer to searchable encryption algorithms, homomorphic encryption algorithms, and algorithms based on BT.

Figure 3. Security requirements of database



2.2.1 Searchable encryption algorithm

In a data security audit, the key to the security of the database is to encrypt the data and complete the normal audit work. Data security should be guaranteed even if they are stored in third-party applications. Even on special application occasions, auditors should obtain ciphertext information and complete the audit work (Tolba and Al-Makhadmeh, 2021) (Liu et al., 2022).

Based on the above, the searchable encryption algorithm comes into being. It is the most frequently used cryptographic algorithm. It can make it very convenient for users to find the ciphertext keywords stored in the database. It can meet the retrieval needs quickly and efficiently but requires less retrieval computing power. It can make the database accurately locate the required files without contacting the user's specific content data, improving operation efficiency and increasing the user's data security. Searchable encryption enables users to enjoy convenient search services and protects the security and privacy of outsourced data. The potential threat of malicious servers hacking into data is eliminated by delivering the computational process to a decentralized and transparent blockchain system (Han et al., 2022). Data interconnection is achieved through encryption technology, which ensures the privacy of encrypted data and detection and prevents malicious adversaries from interfering with device interconnection (Xu et al., 2021) (Gholami et al., 2021).

The searchable encryption algorithm needs to get keywords according to the data characteristics and process the data characteristics using the random function to randomize the data. When they need to retrieve the information on the server, the auditors process the keyword to be queried, and then calculate the similarity with the encrypted information in the server. After receiving the data package, the third-party auditors can perform audit calculations on the audit certificate in the data package and extract the audit information (Lu et al., 2020) (Zhang et al., 2021B) (Cheng et al., 2019). parse the audit certificate from obtained data packet $AuditLogData = \left\langle \mathrm{L}, \mathrm{c} \right\rangle$, and the program contains audit keyword dictionary $\mathrm{D}\left[M : C\right]$. The hash value is calculated according to the first 8 bits of the keyword dictionary:

$$\theta_i^5 = H\left(C_i\left[0:7\right]\right) \tag{1}$$

In equation (1), C_i is the ciphertext keyword in the i-th audit dictionary.
Review audit certificate c and obtain trap gate c_i. The lengths of c_i and C_i are consistent, and their exponential operations are performed by:

$$G_i\left[x\right] = C_i\left[x\right]^{c_i[x]} \tag{2}$$

In equation (2), c_i is the i-th trap gate of audit certificate c.
take the last 8 bits of G_i and assign them as $R_i = G_i\left[-7:0\right]$. The remaining bits are assigned as $L_i = G_i\left[0:7\right]$ and the hash value is calculated by L_i and θ_i^5:

$$\theta_i^6 = H\left(L|\theta_I^5\right) \tag{3}$$

Step 4: judge whether the first 8 digits of θ_I^6 and R_i are equal. If equal, the match is successful, the corresponding audit ciphertext of c_i is C_i. If not, repeat step 2 and the exponential operation of C_i and C_{i+1} are performed until the matching is successful.

perform step 2, and the exponential operation is performed from next trap C_{i+1} and C_i bit by bit:

$$G_i\left[x\right] = C_i\left[x\right]^{c_{i+1}\left[x\right]} \tag{4}$$

All audit plaintext information can be obtained after all trap gates in the audit certificate are reviewed.

2.2.2 Homomorphic Encryption Algorithm

The conventional encryption scheme also has a homomorphic encryption algorithm. In addition to the storage security of the encrypted data, the user's operation or modification of the ciphertext should also be considered. If the decryption operation fails, this encryption scheme will fail. The homomorphic encryption algorithm can solve the problem. When the user processes the encrypted data with various algorithms, any plaintext content will not be disclosed in this process (Kölsch et al., 2019; Vengadapurvaja et al., 2017; Min et al., 2019). Through the server provider, the user processes the whole data with the homomorphic encryption algorithm:

1) The user encrypts the data and sends the encrypted data to the server provider;
2) The processing method of data submitted by the user to the server provider is represented by function *f*;
3) The server provider processes the data under function *f* and sends the processed result to the user;
4) The user decrypts the data and obtains the result.

The Ciphertext vector generation algorithm randomly generates matrix *RM* with $m * 1$ random numbers, and eigenvector f_v is multiplied by random number w, and added with *RM* to obtain new vector-matrix *VM*. The equation is:

$$VM = \left(f_v * w\right) + RM_2 \tag{5}$$

The inverse matrix *IM* of the generated key is obtained and multiplied with *VM* to obtain *HC*. HC is the ciphertext vector after homomorphic encryption, expressed as equations (6) and (7).

$$IM = key^{-1} \tag{6}$$

$$HC = IM * VM \tag{7}$$

The plaintext data are encrypted into the ciphertext data, as equation (8).

$$L_1 = AES_{K_1}\left(L_1\right) \tag{8}$$

Finally, the encrypted data are inserted into the SQL statement, and then the encryption algorithm is performed, as equation (9).

$$L = AES_k\left(l\right) \tag{9}$$

Plaintext SQL l is encrypted into ciphertext L, and ciphertext vectors HC and L are packaged and sent to the database server.

2.2.3 BT

As the name suggests, a blockchain is a combination and arrangement of blockchains. The permanent storage of electronic records is called blocks. Each block records the useful information of relevant trading activities. And the information is generated, sorted, and summarized into a collection in chronological order. Blockchain connection is based on a time sequence. If the next block cannot get the transaction information of the previous block, the next block cannot be generated. In other words, the generation of new blocks depends on all transactions of the previous block. If the block header contains the information compression value of the previous block, it can form a long data link from the first block to the current block. In this way, the information is packaged into a vast database. And the unique cryptography method and equations are used to ensure its non-imitation. All other nodes must be updated when each new transaction occurs, and all nodes have read-only rights to the public ledger (Srinivasu et al., 2021) (Islam et al., 2021). Blockchain technology is widely used in finance, business, industry, voting, education, and medical fields. It has features for peer-to-peer transfer, data ownership, data sharing, data protection, and transaction processing (De Filippi et al., 2022). The blockchain-based multi-dimensional traceable privacy protection scheme is safe and practical. It has an effective role in preventing tampering with health code information and improving the traceability of the virus transmission chain. Attribute encryption can protect residents' private information and achieve fine-grained access control (Yao et al., 2022). Integrating blockchain technology into existing enterprise environments can improve the security of enterprise Internet of Things (IoT) information, resist IoT attacks, and play a maintenance role (Stodt et al., 2021). Using blockchain as homomorphic encryption technology for distributed databases can ensure the security of databases, achieve a triple combination of high security, high transparency, and high efficiency, and contribute to improving cost-effectiveness (Ali et al., 2022) (Zhang et al., 2021A).

The block and hash values are in one-to-one correspondence. The hash value is solved by the block header containing important information. The blocked hair changes the hash value on the block. As the time sequence also changes the hash value of the next block once it is tampered with. And all blocks behind the block must be modified, which will consume a lot of time. Continuity ensures that data writing cannot be tampered with unless a supernode with strong computing power is encountered. The hash tree includes multiple nodes, among which there is a parent node and a group of middle and leaf nodes. The leaf node is located at the bottom. Once the lower node changes, it will extend upward to the tree root. All nodes contain hash values (Mercuri et al., 2021; Sarkar and Singh, 2021).

There are various blockchain underlying technology architecture schemes. Although they have differences in a specific implementation, the overall architectures have many commonalities (Banach, 2021). A common architecture framework has 9 dimensions, as shown in Figure 4:

2.3 Algorithm Flow and Blockchain System Architecture

The operation process of the searchable encryption algorithm is shown in Figure 5:

The specific steps of the searchable encryption algorithm are as follows. Step 1: initialize all the data. Step 2: develop a dictionary of audit keywords. Step 3: generate packets. Step 4: generate packets. The server checks for decryption, generates ciphertext keywords, traverses ciphertext keywords, traverses audit certificates, assigns, and judges. Step 5: the audit. Step 6: analyze the data for feasibility.

The system flow of the homomorphic encryption algorithm is shown in Figure 6:

The process of homomorphic encryption algorithm is as follows: (1) The user one uploads their data information, the original file is encrypted by data vector, homomorphic encryption, and dense

Figure 4. Framework of blockchain underlying technology

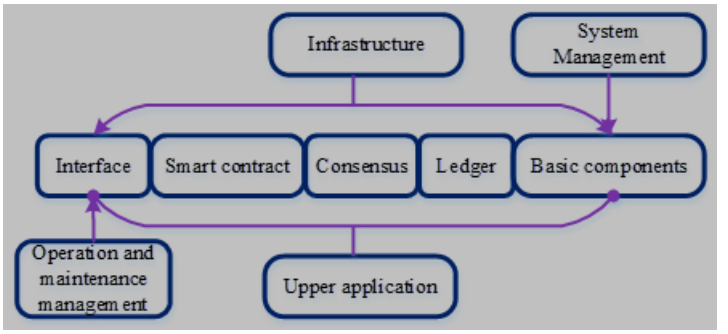
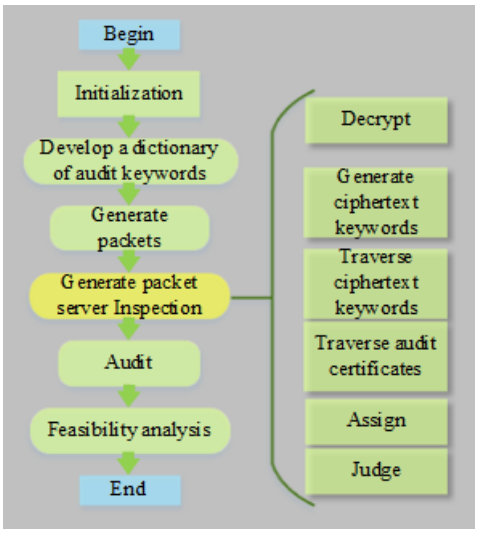


Figure 5. Operation flow of the searchable encryption algorithm



document vector. Finally, the ciphertext file is uploaded. (2) After searching the vector, perform homomorphic encryption and ciphertext search for the vector and submit the vector to the server. The server transmits the data to the user two through correlation analysis, and the second user makes a request for data download.

When the user uploads the data, the database initializes the original file data to get a group of data vectors. It processes this group of data vectors twice to obtain the data vector in the form of ciphertext. The client encrypts the plaintext data to ensure its security. Finally, the plaintext data and encrypted data are sent to the database in the form of data vectors.

When user 2 is retrieving files, it needs to obtain the data vector saved by user 1 and submit the vector to the server. The server compares the correlation coefficients between the data vector and the ciphertext vector, and a set of correlation coefficients are obtained, and the correlation coefficients are sent to the client. After user 2 decrypts, he determines the content corresponding to the required data group and sends a download request to the data server according to the specific correlation coefficients. The server selects the ciphertext according to the request and returns the file data to user 2 (Li et al., 2020) (Bag et al., 2022).

The architecture of the blockchain system is shown in Figure 7:

Figure 6. Flow of the homomorphic encryption algorithm

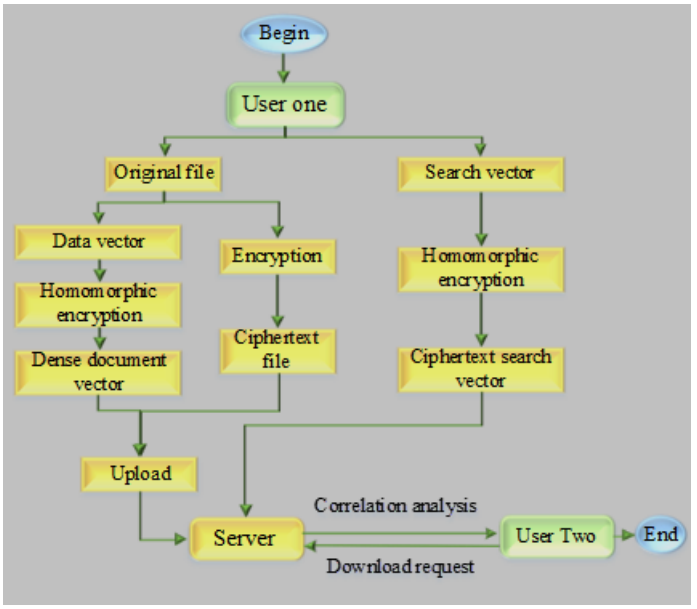
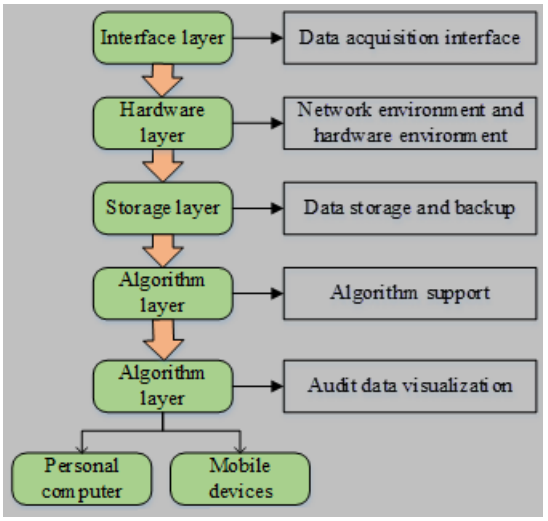


Figure 7. Architecture of the blockchain system



The architecture of the overall system has five layers: the application layer, algorithm layer, storage layer, hardware layer, and interface layer (Vladyko et al., 2021).

(1) The main function of the application layer is to visualize the audit data on the chain to facilitate the audit operation of the third-party auditors.
(2) The algorithm layer provides support for the application layer and realizes various encryption and decryption and semantic analysis, including audit data analysis, audit certificate decryption, and the homomorphic encryption retrieval of certificates.

(3) The storage layer is responsible for data storage and redundant data backup.
(4) The hardware layer includes the network environment and hardware environment supporting the operation of the platform.
(5) The interface layer has data acquisition interfaces, which are the only way for data to flow into the system.

The overall logical structure framework is as follows. The first is to establish a database audit dictionary. The second is to automatically generate keywords. The third is to generate the audit certificate through the trapdoor generation function of the searchable encryption algorithm. The fourth is to calculate the similarity of encrypted information. The fifth is to build a distributed audit database and install a virtual machine in the audit server. The sixth is to write audit server code and algorithms.

The system data collection process is as follows. The first is to collect database information in the network through network packet capture. The second is to use SQL data to filter packets related to database operations in the network. The third is to use session re-aggregation and restoration to analyze the characteristics of network packets to reassemble the filtered packets. The fourth is to use SQL statements to parse the data packets and store them (Han et al., 2018).

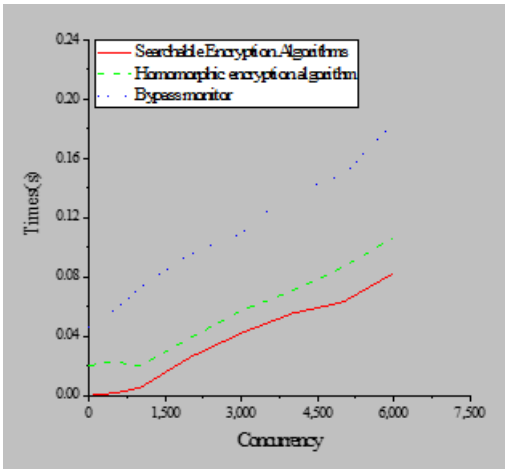
3. EXPERIMENTAL RESULTS

3.1 Comparison of Database Audit Retrieval Algorithms

The searchable encryption algorithm, homomorphic encryption algorithm, and database security audit algorithm based on bypass monitors are compared. The response time of the three algorithms under different concurrency is shown in Figure 8:

In Figure 8, the value of the abscissa depends on the throughput of the server, and the server threshold can be jointly determined by calculating the mean value and standard deviation. Searchable encryption algorithms combine cryptographic primitives with information retrieval techniques to encrypt data and a keyword index of the data. Homomorphic encryption algorithm satisfies the property of ciphertext homomorphic operation. After the data is homomorphically encrypted, the ciphertext is calculated. The bypass monitoring technology algorithm monitors network communication through switch mirroring technology or network card promiscuous mode to ensure that the data packets in the network are captured without affecting the normal transmission of the network. Besides, the security

Figure 8. Comparison of concurrency of three algorithms



of the network database is ensured. Compared with the three, the bypass monitoring technology algorithm has the longest response time, but its advantage is that it does not affect the basic business. Compared with homomorphic encryption algorithms, searchable encryption algorithms are efficient and secure in searching for information.

Figure 8 shows that the response time of the homomorphic encryption algorithm is about 0.02 seconds when the concurrency reaches the server threshold of about 1000, and it begins to rise linearly because its execution efficiency depends on the throughput of the server. The audit equipment limits the performance of the database security audit algorithm based on bypass monitors, and its threshold is lower. When its concurrency is between 0-500, the response time increases linearly. Moreover, this scheme needs to perform encryption and decryption two times in the transmission process, which will take a longer time. Although the searchable encryption algorithm also reaches the server threshold when the concurrency is about 1000, its response time is about 0.005 seconds, four times less than that of the homomorphic encryption algorithm. Therefore, the searchable encryption algorithm has advantages in concurrency and response time.

The inspection efficiency of the searchable encryption algorithm, homomorphic encryption algorithm, and database security audit algorithm based on bypass monitors is compared. The results are shown in Figure 9:

Figure 9 shows that the inspection efficiency of the searchable encryption algorithm is much higher than that of the database security audit algorithm based on bypass monitors and homomorphic encryption algorithms. If there are 150 data, the execution time of the searchable encryption algorithm is 2.88 seconds, that of the homomorphic encryption algorithm is 9.61 seconds, about 3.3 times that of searchable encryption algorithm, and that of database security audit algorithm based on bypass monitors is 51.5 seconds, approximately 17.9 times that of the searchable encryption algorithm.

The time taken by the three algorithms to audit the elements in the keyword dictionary is compared. If the execution efficiency of the audit data is 50, the time that the execution is shown in Figure 10:

Figure 10 shows that the time required by the searchable encryption algorithm is less, especially in the first three groups. The data audit time of the first group is about 0.04 seconds, which is nearly half of that of the homomorphic encryption algorithm and less than one-third of that of the database security audit algorithm based on bypass monitors. The audit time of the fourth group of the homomorphic encryption algorithm is about 0.13 seconds, that of the fifth group is about 0.15 seconds, and that of the sixth group is about 0.16 seconds, which are close to the searchable encryption algorithm. But its running time in the first three groups is much longer than the searchable encryption algorithm. The execution time of the database security algorithm based on bypass monitors is significantly longer

Figure 9. Comparison of the inspection efficiency of three algorithms

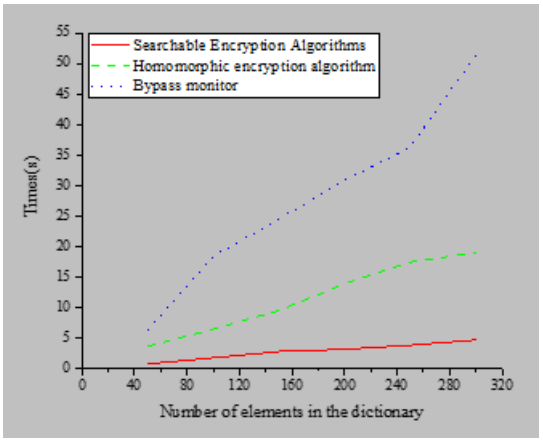
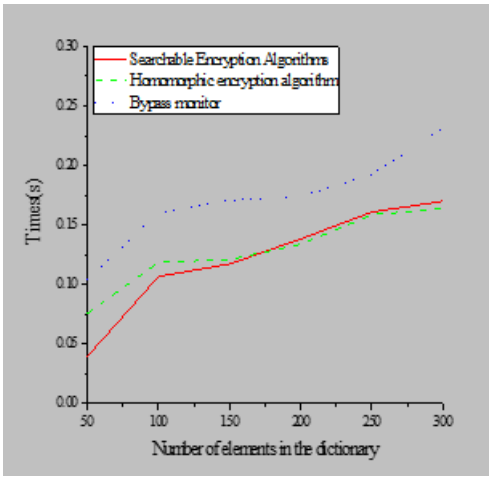


Figure 10. The time taken by the three algorithms



than that of the first two algorithms. In the sixth group, the time required by the database security algorithm based on bypass monitors reaches 0.23 seconds, about 0.07 seconds more.

From the comparison of the calculation conditions of the three algorithms in Figure 9 and Figure 10, the execution time of the searchable encryption algorithm is the shortest, and the verification efficiency on the server side is the fastest. In the case of ensuring the security of network information and data, the searchable encryption algorithm is the most appropriate method.

3.2 Comparison of Database Audit Servers

The size of the audit certificate is fixed at 128KB to test the processing efficiency of the data audit system based on BT. When the user's total amount of the same operation statements is 50, 100, 150, and 200, the average audit time for the BT scheme and the traditional TPA is counted. The results are shown in Figure 11:

Figure 11. Average audit time of two schemes when the total amount of operation statements changes

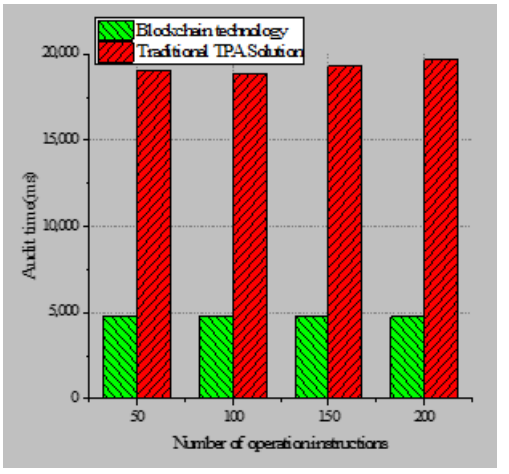


Figure 11 shows that the BT scheme is more stable and has a shorter audit time. The average audit time is stable at about 4800ms, of which the minimum audit time is 1754 seconds and the maximum audit time is 4819 seconds. The average audit time of the TPA scheme is more than 19000ms, of which the minimum is 18875 seconds, and the maximum is 19653 seconds, which is more than four times the BT scheme.

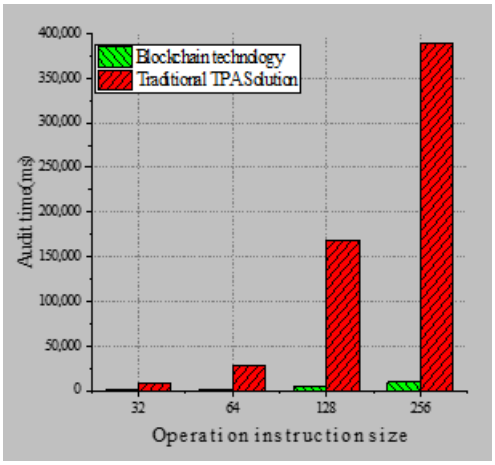
When the total number of fixed operation statements sent to the database is 100, and the size of a single operation statement is 32 KB, 64 KB, 128 KB, and 256 KB, the average audit time of the BT scheme and traditional TPA scheme under single operation statement is counted. The results are shown in Figure 12 below:

Figure 12 shows that the BT and TPA scheme's execution efficiency increases with the increase of the number of operating instructions. But the rising speed of the TPA scheme is faster, and its execution efficiency is lower. When a single operation statement is 256KB, the execution efficiency of this scheme is close to 400000s. This shows that the BT scheme is superior to the TPA scheme in terms of stability and efficiency.

4. CONCLUSIONS

The searchable encryption algorithm is used to solve the problem of ciphertext data audit from the audit log algorithm and ciphertext data retrieval algorithm. An audit server scheme based on BT is proposed to solve the security problems of the audit system and prevent the data from being tampered with or leaked. The results show that the searchable encryption algorithm has higher inspection efficiency, which takes nearly three times less time than the homomorphic encryption algorithm, 17 times less time than the database security audit algorithm of bypass monitors, and the time required in the execution process is also shorter. In the first three sets of data auditing process, the searchable encryption algorithm takes the least execution time. When the number of elements reaches 150, the execution time of the searchable encryption algorithm is nearly the same as that of the homomorphic encryption algorithm (Zhang et al., 2022). The execution time of the database security audit algorithm based on bypass monitoring is the highest from beginning to end. Compared with the BT scheme, the average audit time of the TPA scheme is more than four times that of the BT scheme when the total amount of operation statements and the size of a single operation statement change. The BT audit server scheme is proportional to the number of operation instructions, but its growth rate is lower than that of the TPA scheme, and the execution efficiency is fast, up to 400000ms. The BT

Figure 12. Average time of two schemes when the size of a single operation statement changes



scheme is superior to the TPA scheme in terms of stability and efficiency. However, there are still some shortcomings. For example, the execution efficiency of each algorithm is only compared, but the execution time of the complete audit process is not discussed. Therefore, reducing the time of each algorithm is still the focus of future research. In future research, the execution efficiency comparison of multiple algorithms can be added to supplement the insufficient execution time of the audit process to improve the efficiency and stability of the audit.

ACKNOWLEDGMENT

Guangdong Provincial Philosophy and Social Sciences "13th Five-Year Plan" 2020 Disciplinary Co-construction Project (Grant No: GD20XGL54). Project Title: Research on the Application of the Three-Level Model of Environmental Cost Control for Manufacturing Enterprises in the Guangdong-Hong Kong-Macao Greater Bay Area-Taking SMN's innovative ecological product chain as an example.

REFERENCES

Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., Teo, J., & Zakarya, M. (2022). An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors (Basel)*, *22*(2), 572. doi:10.3390/s22020572 PMID:35062530

Bag, S., Srivastava, G., Gupta, S., & Taiga, S. (2022). Diffusion of Big Data Analytics Innovation in Managing Natural Resources in the African Mining Industry. *Journal of Global Information Management*, *30*(6), 1–21. doi:10.4018/JGIM.297074

Banach, R. (2021). Blockchain applications beyond the cryptocurrency casino: The Punishment not Reward blockchain architecture. *Concurrency and Computation*, *33*(1), e5749. doi:10.1002/cpe.5749

Chen, M., & Zhang, L. (2022). Application of Edge Computing Combined with Deep Learning Model in the Dynamic Evolution of Network Public Opinion in Emergencies. *The Journal of Supercomputing*. Advance online publication. doi:10.1007/s11227-022-04733-8 PMID:35915780

Chen, Q. (2020). Research on the Implementation Method of Database Security in Management Information System Based on Big Data Analysis. E3S Web of Conferences, 185, 02033. doi:10.1051/e3sconf/202018502033

Cheng, L. C., Wu, C., & Chen, C. (2019). Behavior Analysis of Customer Churn for a Customer Relationship System: An Empirical Case Study. *Journal of Global Information Management*, *27*(1), 111–127. doi:10.4018/JGIM.2019010106

Daniel, E., Durga, S., & Vijila, M. (2021). A Continuous Sampling Method for Batch Data Auditing in Cloud Storage. *International Journal of Information Systems in the Service Sector*, *13*(2), 1–12. doi:10.4018/IJISSS.2021040101

De Filippi, P., Mannan, M., & Reijers, W. (2022). The alegality of blockchain technology. *Policy and Society*, *41*(3), 358–372. doi:10.1093/polsoc/puac006

Earnhart, D., & Harrington, D. R. (2021). Effects of audit frequency, audit quality, and facility age on environmental compliance. *Applied Economics*, *53*(28), 3234–3252. doi:10.1080/00036846.2020.1854449

Feng, Z., & Chen, M. (2022). Platformance-Based Cross-Border Import Retail E-Commerce Service Quality Evaluation Using an Artificial Neural Network Analysis. *Journal of Global Information Management*, *30*(11), 1–17. Advance online publication. doi:10.4018/JGIM.306271

Gholami, R., Nishant, R., & Emrouznejad, A. (2021). Modeling Residential Energy Consumption: An Application of IT-Based Solutions and Big Data Analytics for Sustainability. *Journal of Global Information Management*, *29*(2), 166–193. doi:10.4018/JGIM.2021030109

Han, J., Huang, Y., Kumar, K., & Bhattacharya, S. (2018). Time-Varying Dynamic Topic Model: A Better Tool for Mining Microblogs at a Global Level. *Journal of Global Information Management*, *26*(1), 104–119. doi:10.4018/JGIM.2018010106

Han, J., Li, Z., Liu, J., Wang, H., Xian, M., Zhang, Y., & Chen, Y. (2022). Attribute-Based Access Control Meets Blockchain-Enabled Searchable Encryption: A Flexible and Privacy-Preserving Framework for Multi-User Search. *Electronics (Basel)*, *11*(16), 2536. doi:10.3390/electronics11162536

Hao, X., Ji, Z., Li, X., Yin, L., Liu, L., Sun, M., Liu, Q., & Yang, R. (2021). Construction and Application of a Knowledge Graph. *Remote Sensing*, *13*(13), 2511. doi:10.3390/rs13132511

Islam, M., Kang, M., & Haile, T. T. (2021). Do Hedonic or Utilitarian Types of Online Product Reviews Make Reviews More Helpful? A New Approach to Understanding Customer Review Helpfulness on Amazon. *Journal of Global Information Management*, *29*(6), 1–18. doi:10.4018/JGIM.20211101.oa52

Jiang, H., Xie, M., Kang, B., Li, C., & Si, L. (2018). ID-based public auditing protocol for cloud storage data integrity checking with strengthened authentication and security. *Wuhan University Journal of Natural Sciences*, *23*(4), 362–368. doi:10.1007/s11859-018-1335-9

Kölsch, J., Heinz, C., Ratzke, A., & Grimm, C. (2019). Simulation-based performance validation of homomorphic encryption algorithms in the internet of things. *Future Internet*, *11*(10), 218. doi:10.3390/fi11100218

Li, J., Kuang, X., Lin, S., Ma, X., & Tang, Y. (2020). Privacy preservation for machine learning training and classification based on homomorphic encryption schemes. *Information Sciences*, *526*, 166–179. doi:10.1016/j.ins.2020.03.041

Li, M., Qin, Y., Liu, B., & Chu, X. (2021). Enhancing the efficiency and scalability of blockchain through probabilistic verification and clustering. *Information Processing & Management*, *58*(5), 102650. doi:10.1016/j.ipm.2021.102650

Li, Y., Cao, Q., Zhang, K., & Ren, F. (2021). A secure index resisting keyword privacy leakage from access and search patterns in searchable encryption. *Journal of Systems Architecture*, *115*, 102006. doi:10.1016/j.sysarc.2021.102006

Liu, Z., Panfilova, E., Mikhaylov, A., & Kurilova, A. (2022). Assessing Stability in the Relationship Between Parties in Crowdfunding and Crowdsourcing Projects During the COVID-19 Crisis. *Journal of Global Information Management*, *30*(4), 1–18. doi:10.4018/JGIM.297905

Lu, Y., Li, J., & Wang, F. (2020). Pairing-free certificate-based searchable encryption supporting privacy-preserving keyword search function for IIoTs. *IEEE Transactions on Industrial Informatics*, *17*(4), 2696–2706. doi:10.1109/TII.2020.3006474

Maso, L. D., Lobo, G. J., Mazzi, F., & Paugam, L. (2020). Implications of the joint provision of CSR assurance and financial audit for auditors' assessment of going-concern risk. *Contemporary Accounting Research*, *37*(2), 1248–1289. doi:10.1111/1911-3846.12560

Mercuri, F., della Corte, G., & Ricci, F. (2021). Blockchain technology and sustainable business models: A case study of Devoleum. *Sustainability*, *13*(10), 5619. doi:10.3390/su13105619

Min, Z., Yang, G., Sangaiah, A. K., Bai, S., & Liu, G. (2019). A privacy protection-oriented parallel fully homomorphic encryption algorithm in cyber physical systems. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 1–14. doi:10.1186/s13638-018-1317-9

Overman, D. M., Jacobs, M. L., O'Brien, J. E. Jr, Kumar, S. R., Mayer, J. E. Jr, Ebel, A., & Jacobs, J. P. (2019). Ten years of data verification: The Society of Thoracic Surgeons congenital heart surgery database audits. *World Journal for Pediatric & Congenital Heart Surgery*, *10*(4), 454–463. doi:10.1177/2150135119845256 PMID:31307308

Pajany, M., & Zayaraz, G. (2021). A Robust Lightweight Data Security Model for Cloud Data Access and Storage. *International Journal of Information Technology and Web Engineering*, *16*(3), 39–53. doi:10.4018/IJITWE.2021070103

Sarkar, A., & Singh, B. K. (2021). A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. *Multimedia Tools and Applications*, *80*(1), 799–829. doi:10.1007/s11042-020-09375-7

Shot, A. P. (2020). Analyzing the Impact of the Internal Audit Service on the Activities of Economic Entities. *Business Info*, *1*(504), 278–284. doi:10.32983/2222-4459-2020-1-278-284

Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics (Basel)*, *10*(12), 1437. doi:10.3390/electronics10121437

Srivaishnavi, D., Arjun, T., Dhyaneshwaran, K., & Deepak, R. (2021). Secure Ring Signature based privacy preserving of Public Auditing mechanism for outsourced data in cloud computing paradigm. *Journal of Physics: Conference Series*, *1916*(1), 012079. doi:10.1088/1742-6596/1916/1/012079

Stodt, J., Schönle, D., Reich, C., Ghovanlooy Ghajar, F., Welte, D., & Sikora, A. (2021). Security audit of a blockchain-based industrial application platform. *Algorithms*, *14*(4), 121. doi:10.3390/a14040121

Stoel, M. D., & Havelka, D. (2021). Information technology audit quality: An investigation of the impact of individual and organizational factors. *Journal of Information Systems*, *35*(1), 135–154. doi:10.2308/isys-18-043

Tian, J. F., & Wang, H. N. (2020). An efficient and secure data auditing scheme based on fog-to-cloud computing for Internet of things scenarios. *International Journal of Distributed Sensor Networks*, *16*(5), 1550147720916623. doi:10.1177/1550147720916623

Tolba, A., & Al-Makhadmeh, Z. (2021). Predictive data analysis approach for securing medical data in smart grid healthcare systems. *Future Generation Computer Systems*, *117*, 87–96. doi:10.1016/j.future.2020.11.008

Vengadapurvaja, A. M., Nisha, G., Aarthy, R., & Sasikaladevi, N. (2017). An efficient homomorphic medical image encryption algorithm for cloud storage security. *Procedia Computer Science*, *115*, 643–650. doi:10.1016/j.procs.2017.09.150

Vladyko, A., Spirkina, A., & Elagin, V. (2021). Towards Practical Applications in Modeling Blockchain System. *Future Internet*, *13*(5), 125. doi:10.3390/fi13050125

von Sanden, N., & Neideck, G. (2021). Learnings from the development of Public Sector Multi-source Enduring Linked Data Assets. *The Australian Journal of Social Issues*, *56*(2), 288–300. doi:10.1002/ajs4.157

Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Haihua, L. (2020). Identity Authentication Security Management in Mobile Payment Systems. *Journal of Global Information Management*, *28*(1), 189–203. doi:10.4018/JGIM.2020010110

Wu, Z., Zang, C., Wu, C., Deng, Z., Shao, X., & Liu, W. (2022). Improving Customer Value Index and Consumption Forecasts Using a Weighted RFM Model and Machine Learning Algorithms. *Journal of Global Information Management*, *30*(3), 1–23. doi:10.4018/JGIM.20220701.oa1

Xu, C., Lin, M., Cheng, J., Zhao, Y., & Zuo, C. (2021). IoT Services: Realizing Private Real-Time Detection via Authenticated Conjunctive Searchable Encryption. *Journal of Cybersecurity*, *3*(1), 55.

Yan, C., Li, B., Vorobeychik, Y., Laszka, A., Fabbri, D., & Malin, B. (2019). Database audit workload prioritization via game theory. *ACM Transactions on Privacy and Security*, *22*(3), 1–21. doi:10.1145/3323924

Yao, S., Jing, P., Li, P., & Chen, J. (2022). A multi-dimension traceable privacy-preserving prevention and control scheme of the COVID-19 epidemic based on blockchain. *Connection Science*, *34*(1), 1654–1677. doi:10.1080/09540091.2022.2077912

Yu, C., Li, Z., Yang, D., & Liu, H. (2022). A fast robotic arm gravity compensation updating approach for industrial application using sparse selection and reconstruction. *Robotics and Autonomous Systems*, *149*, 103971. doi:10.1016/j.robot.2021.103971

Zhang, A., Bao, M., Xu, X., Zhang, L., & Cui, Y. (2021A). The Effect of Dual-Level Transformational Leadership on New Firm Performance: The Mediated Role of Entrepreneurial Bricolage. *Journal of Global Information Management*, *29*(6), 1–18. doi:10.4018/JGIM.294577

Zhang, A., Chen, Y., Xu, X., Gao, Y., & Zhang, L. (2021B). Impacts of Resource Alertness and Change Leadership Style on Financial Performance: An Empirical Study. *Journal of Global Information Management*, *29*(2), 45–60. doi:10.4018/JGIM.2021030103

Zhang, H., Fan, L., Chen, M., & Qiu, C. (2022). The Impact of SIPOC on Process Reengineering and Sustainability of Enterprise Procurement Management in E-Commerce Environments Using Deep Learning. *Journal of Organizational and End User Computing*, *34*(8), 1–17. Advance online publication. doi:10.4018/JOEUC.306270