Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1841–1851, DOI 10.12694/scpe.v25i3.2762

# DATABASE ACCESS INFORMATION SECURITY MANAGEMENT SIMULATION UNDER BIG DATA PLATFORM

ZHAOCUI LI *AND DAN WANG †

**Abstract.** When people perform database access information security management, the traditional method cannot accurately verify the identity of the visitor, the credibility of the identity information, and the security management of the access information. With the widespread application of big data technology, the amount of data in databases is rapidly increasing, which brings new challenges to information security management. The main purpose of this study is to explore how to more effectively manage the security of database access information on big data platforms.Therefore, the trusted computing platform is established to implement database access information security management under the data platform. The method determines the user behavior is credible by establishing a behavior chain of behavior based on the user identity and measuring user operation behavior. For the user's private data, the encryption/decryption module is used for security protection, preventing data from being leaked through illegal copying. A trusted metric model based on the USB Key user identity is established and a trusted platform is established. By improving the ELGamal algorithm, the IMC/IMV metrics architecture is utilized to measure platform security attributes. In the first round of anonymous authentication, the identity authentication of the platform is completely completed, and the database access information security management under the big data platform is completed. The simulation results show that in 10 experiments, the transmission time delay of TCP/IP protocol is less than 200ms, and the security of database access information is enhanced after the encryption system is established in the database. This has certain theoretical enlightenment for the improvement of database security and the optimization of information security management.

**Key words:** Big Data, Database, Information Security, Simulation Research

**1. Introduction.** Under the rapid development of computer network technology, various network security incidents continue to occur, seriously affecting the security of user information. Advanced technology has brought convenience to people, and it has also brought various network hazards to them. Code attacks, illegal destruction of systems and data, and illegal information theft are the three most prominent security risks [1]. Traditional network protection methods, such as intrusion detection and virus protection, are implemented in software. Most security methods need to be based on the operating system to operate. Entering the system with a relatively low level of security will not meet the high security requirements of a particular region [2]. Therefore, how to realize security protection from computer architecture and realize the safe and reliable operation of computer system platform has become a core problem to be solved [3].

Trusted computing technology is one of the main technologies to solve computer security problems. By establishing a behavioral trust chain based on user identity, the user behavior is judged to determine whether the user behavior is trustworthy. For the private data of the user, the encryption/decryption module is used for security protection to prevent data from being leaked through illegal copying, and it is proved by experiments. The program can effectively protect the system from the illegal behavior of users and prevent the private data from being illegally stolen [4]. Therefore, to build the security of computer terminals, the basic hardware and software of the terminal must be improved [5]. From the computer terminal core chip, hardware architecture, operating system security protection and other aspects to comprehensively take security measures to ensure that computer terminals are less affected by security issues, which is the basic idea of trusted computing [6]. In summary, trusted computing is used to study the title of database access information security management simulation under the big data platform.Databases have become the main tool for enterprises and organizations to store and process a large amount of information. However, with the expansion of database usage, data

*Department of Senior Technician, Shandong Labor Vocational and Technical College, Jinan, 250022, China (Corresponding author, lee009086@126.com)
†Department of Senior Technician, Shandong Labor Vocational and Technical College, Jinan, 250022, China (wangdan_sdlvtc@163.com)

security and privacy protection issues are becoming increasingly prominent. Therefore, how to implement security protection on computer architecture to ensure the security and privacy of data in databases has become an urgent problem to be solved. This article will introduce a database access information security management solution based on simulation methods on big data platforms, aiming to improve data security and privacy protection levels. Computer architecture is the organizational structure and behavior of a computer system, and its security protection involves various levels such as hardware, operating systems, and application programs.

This article uses real datasets for simulation experiments. This simulation scheme can effectively evaluate the effectiveness of existing security policies and identify potential security risks. This scheme can also be tested and analyzed for different attack scenarios, providing strong support for the formulation of security strategies. In 10 experiments, the transmission delay of TCP/IP protocol was less than 200ms. After establishing an encryption system in the database, the security of database access information was enhanced. This has certain theoretical implications for improving database security and optimizing information security management.

It is mainly divided into three parts: The first part introduces the Trusted Computing Platform, the Trusted Platform Module and the Trusted Metrics Mechanism, and a trusted platform is built for database access information security management. In the second part, a user behavior measurement method based on trusted platform module is proposed. The trusted metric model is constructed based on the trusted platform module and USBKey two-factor authentication mechanism. In the third part, a trusted security terminal management system is established to verify the proposed trusted model.

**2. Background of the Study.** With the continuous innovation and development of modern information technology, the most commonly used and widely used in people's life is information. The management of database access information security under the big data platform has attracted the attention of many scholars. Alkida B et al. pointed out that computer operating systems and network platform systems constitute an information database and form a network information platform system [7].

Ramos G et al. mentioned that access control was an important mechanism to ensure that the database system was not invaded and information was protected. And various access control mechanism methods were proposed by them, such as autonomous access control, mandatory access control, etc. [8]. Christodoulou N A et al. proposed autonomous access control method based on the attributes of user access data information. The object access rights are defined by the different attributes of the subject and the subject, and the research proves that the control method is autonomous control [9]. Chuan-Yu L V et al. proposed a database access information security management method under the big data platform. The attribute-based multi-authorization encryption system was constructed to reduce the number of matching operations and improve the efficiency of password utilization. The results show that the encryption of the database enhances the security of database access information and realizes the security management of database access information under the big data platform [10]. Aulkemeier F and others believed that while using computers, a large amount of data information was be generated. At this time, computer database technology should be used to efficiently accomplish the task of information security management. The results show that this can improve the accuracy and reliability of data information transmission [11]. Konstantelos I and others analyzed the security risks and management status of hospital information systems, proposing effective measures to achieve the security of hospital information databases, which is of great significance to ensure the stable, efficient and safe operation of hospital information systems [12]. Zhang F et al. established a real-time monitoring system based on WEB query server, which realizes the real-time monitoring and management functions of online query users, thus improving the security of back-end database information [13]. Example F used the reference table of the network asset refinement table, threat list, and network security threat risk factor matrix for bank security risk, information assets, network security management, and secure time management to analyze the threats and vulnerability of bank through qualitative and quantitative risk analysis, which is of universal significance for the study of bank information security [14]. Hirose K et al. explored its application by analyzing the security access and backup management technology of Oracle database, providing enterprises with more comprehensive and accurate ideas to ensure the system is reliable and secure [15].

According to the above research by China and other foreign scholars, the level of confidentiality of information involved in each level of database access security management is different, and the requirements for

users to view content are also different. If confidential information is disclosed, it will have unpredictable consequences. Therefore, ensuring the reliability and completeness of data information in the database is an important topic in the field of information security. The database access information security management under the big data platform can solve the above problems and ensure the information security in the database, which has important practical significance.

## 3. Application of Trusted Computing in Database Access Information Security Management.

**3.1. Trusted platform construction based on database access information security management.** The trusted computing platform is computer hardware and software integrated entity constructed by a hardware security chip and its supporting software plus some functional components, and provides trusted computing services externally. TCG believes that starting from an initial "trust root", in every state transition of the trusted computing platform, this trust state can remain unchanged through delivery [16,17]. Then the trusted computing environment will not be destroyed, and the trusted state will remain. The trusted operation of the trusted platform will not cause damage to the platform, so the trusted state of the trusted platform will be maintained. This mechanism is called the trust delivery mechanism. The trusted platform for both local users and remote users is always a trusted platform. In order to convince users that the platform is trustworthy, it is often to let users believe that a trusted password security module has been configured in the computing platform, and a series of user-selected security protection software is correctly installed and correctly operated in the system, so that a trust relationship between the user and the computing platform can be established.

The Trusted Computing Platform architecture consists of three parts, TPM, TSS, and user programs. TPM has its core part to serve the upper layer applications. The main process of the metric is as follows: establish metrics and rules, implement metrics on metrics, collect metrics and process them to generate metric sets, and compare the generated metrics set with the expected metrics given by the producer or trusted set [18,19]. Finally, the measurement results are obtained. Trusted measurement technology mainly includes three main parts: trusted metrics, trusted storage and trusted remote reporting. The trusted computer uses the trusted computing metric technology to measure whether a certain program running by the verification system is secure and reliable, and ensures the trusted state of the trusted platform. In the research field of trusted computing, trusted metric technology can be divided into multiple types due to different measurement time or measurement objects. For example, according to different measurement time, it can be divided into static measurement and dynamic measurement [20]. A static metric is a measure that is measured only once when the object is being measured. A dynamic metric is a measure of the behavior of a metric object or the behavior of an object's behavior during object execution. According to different measurement objects, it can be divided into platform-based integrity metrics, platform-based attribute metrics, and semantic-based metrics.Platform integrity metrics, platform based attribute metrics, and semantic based metrics are all used to evaluate the integrity of information or data, but the differences between them are mainly reflected in the application scenarios and methods. Platform integrity measurement is mainly used to evaluate the integrity of a platform. Platform based attribute measurement mainly evaluates the reliability, stability, and security of a platform based on its attributes. Semantic based measurement mainly evaluates the integrity of data based on its semantic content. It focuses on whether the data expresses its semantic meaning truthfully, accurately, and completely, such as whether the text data expresses the correct meaning, and whether the image data is clear and complete.

For data integrity metrics, the TPM provides a hash function and a grouping key for calculating the digest value, while also providing a secure storage unit platform configuration register (PCR, Platform Configuration Register) for storing and updating the metric results. When the platform collects the expected value of the object, the expected value of the collected metric object is stored in the platform configuration register, so that the PCR and the hash function interface provided by the TPM can extend the trust chain established by the trusted root. The hash function provided by the TPM is combined with the platform register PCR to update the PCR value as shown in equation 3.1:

$$PCR[i] = SHA - 1(PCR[i]|new\_Value \tag{3.1}$$

Use a hash function, such as SHA-256 (secure hash algorithm 256 bits), to hash the old PCR value as input. This will generate a new hash value. Add new data to the old PCR values after hashing. This may

involve performing bitwise AND operations, bitwise OR operations, addition operations, or other forms of combination between new and old data. Hash the results after adding new data again. This will generate a new PCR value. The old PCR value and the added new data are hashed in the (1) manner to obtain a new PCR value, so that the PCR value generated by the update is related to the old value and the order of the newly added data, and the old value of the SHA-1 algorithm is performed. The sequence of PCR and new data is not interchangeable. That is, the update PCR is not possible if the value of the old value PCR is not based. Integrity metrics and integrity verification are the basic functions of trusted metrics. The metric first measures the operational state of the system in real time and provides a metric reference. A trusted report is a metric that a trusted platform generates to measure different components when creating a trusted environment. It is not only needed to measure its own components, but also to provide external trusted reporting information when it proves that its platform is trusted. Therefore, the trusted report trust root and trusted report are the core of the trusted platform integrity measurement model, and are the necessary conditions for mutual authentication and measurement between the requester and the authenticator.

**3.2. Trustworthy Metric Model Based on USBKey User Identity.** In a computer system, user behavior is generally defined as the user's access or operation of system resources after authentication, including the behavior of the process as the principal. Therefore, the user identity is determined by combining the USBKey and the TPM for different users, and the different users are measured according to the basis. At present, the security operating system mainly starts from the three aspects of authentication, authorization and auditing, and designs three levels of different users (administrators, ordinary users, audit users), and sets different permissions for level 3 users [21,22]. By binding different security policies through trusted mechanisms, users' access to system resources and trusted use are controlled. The administrator has the highest level of access control permission of the system. The ordinary user can only perform customized operations on the system (such as adding/decrypting based on user roles). The audit user can only view the audit log. The root password is reset to the default password after initialization. Before using the key, the root password needs to be used for authentication, and the authentication is passed to authorize the use of the key. Therefore, in order to prevent malicious access by other programs, it is only necessary to modify the root password to a system-specific password. Therefore, the authentication of the user identity uses the USBKey two-factor authentication mechanism to authenticate the user identity based on whether the USBKey is connected to the operating system, which effectively improves the security of the information stored in the USBKey, and the USBKey user authentication information and TPM certification and authorization are combined to achieve trusted authorization for different users [23,24]. The USBKey is used to store the unique identifier UUID of the key stored in the TPM, and the UUID can be used to use the TPM key. The USBKey is held by the user. Before using the USBKey, the user needs to input the password of the USBKey and verify its integrity. After passing the algorithm, the TPM key is used.

When the user logs in to the system with the correct USBKey, the decryption key is obtained through the TPM. The user database is decrypted by the TPM, and the user identity information is provided for the behavior measurement module. The behavior measurement model measures the user behavior according to the user identity and the specified identity access policy. For the entire measurement system, a key part of the system is dynamically loadable user identity-based transparent encryption/decryption and user behavior metrics.

**3.3. Platform Authenticity Verification Based on User Behavior Trusted Metric Design.** When the user logs in to the system, after the encryption/decryption attribute is set to the system resource, the system uses the key in the USBKey to dynamically add/decrypt the specified file resource of the system. The results generated by the system trusted process and user system resource configuration are stored in two special files and protected by an access control mechanism. These two special files are the system trusted process list and the user system resource configuration table, which are the basis of user behavior metrics. After the security kernel module is initialized, the system executable program is dynamically loaded, and the trusted process information is measured, the trusted process is loaded, the security configuration policy information of the user is obtained by acquiring the TPM encryption/decryption database, and a resource configuration file is read to establish a System resource controlled information chain. When the user configures the encryption/decryption attribute on the system resource, when the file is read, it first searches for the executable file in the controlled

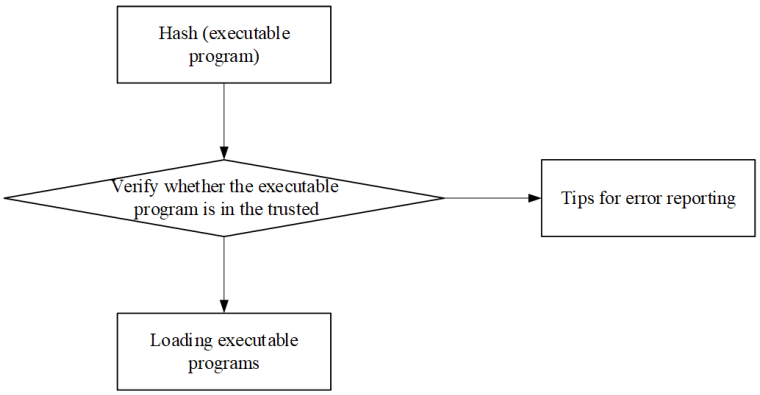


Fig. 3.1: Executable program loading process

file list. If it belongs, the key is obtained by the TPM and the file is decrypted. To protect the security of individual special files, the user identity information is associated with the process information, and the access control policy is performed with the process information. For the system resources, the user can be specified and the specified process can be operated.

When the system logs in, the user's identity role and the information chain based on the user role are established. When a specified user modifies or accesses the specified resource information, it can only be performed by the specified process. The credibility of the user's identity authentication has been described above. The trustworthiness of the process is mainly determined by checking whether the binary code of the executable program is complete, and ensuring that the application executable program is complete and has not been tampered with.

In order to ensure the integrity of the executable program, the "system program whitelist" design is adopted. The system establishes and maintains a trusted list of executable programs. The list stores the path and hash value of the executable program code in the system. When an executable program is started, the TPM hash function is used to calculate the Hash value of the executable program. It is then compared to the stored hash values in the trusted list. If the program path exists in the trusted list and the pre-stored hash value matches the actual metric hash value, the program is allowed to run. If the executable program is not in the list or the pre-stored value does not match the actual value, the operation is prohibited. Since the trusted list is also damaged, in order to ensure that the trusted list is not modified by the illegal program, the access restriction is restricted by the control. Only the specified user can accept the operation request by using the specified program in the specified format. The loading process of its executable program is shown in Figure 3.1.The hash values stored in the trust list are typically used to verify the integrity and trustworthiness of data. By comparing the data with the hash values in the trust list, it can be determined whether the data has been tampered with or damaged. If the data matches the hash value in the trust list, it means that the integrity of the data has been verified, as the hash value is generated by converting the data into a fixed length string. If the data does not match the hash value in the trust list, it indicates that the data may have been tampered with or damaged, and corresponding measures should be taken, such as re obtaining the data or further processing.

In trusted computing, an important aspect of inter-platform security authentication is identity authentication between platforms. Trusted authentication between platforms can only be completed on the basis of proving the identity of the platform. The authentication of the platform identity is based on the identity authentication of the TPM. The verification of the platform authenticity is the verification of the platform identity, mainly to verify whether the platform at both ends of the communication is a real trusted platform. In trusted computing, each TPM has a unique endorsement key (EK), and each endorsement key uniquely represents a TPM. In order to prevent the identity of the endorsement key leakage platform, the TCG specification uses the ATM (attestation identity key) generated by the TPM first to replace the endorsement key to prove that

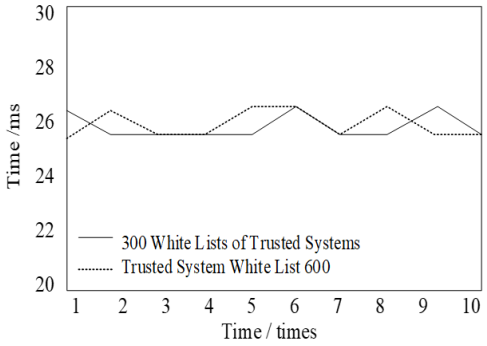


Fig. 4.1: Time comparison of system running program

it has a real trusted platform.

**4. Experimental Design and Analysis.**

**4.1. Experimental environment.** In view of the above scheme, the whole system is realized in this paper. The implementation environment is a domestic machine based on the trusted platform module. The experimental environment is configured as: operating system: the winning standard 32-bit operating system. Processor chip: Godson 3A, clocked at 1GHz. Memory and hard disk capacity: 2G memory, 500G hard disk. Develop IDE: QtCreator, NetBeans. Development language: QT, LinuxC. In the experimental environment, the software used for the trusted platform module of Chinese made machines is Kirin V3.0. For the developed system, in order to ensure the availability of the system without affecting the operation and user experience of the operating system, the performance of the developed software system is tested. The test terminal environment is configured as follows: the operating system is a winning 32-bit operating system of Kirin, the processor chip uses Godson 3A, the main frequency is 1 GHz, the memory is 2G, and the hard disk is 500G.

The experimental terminal is configured as follows: The processor chip adopts Godson 3A, the main frequency is 1 GHz, the memory is 2G, and the hard disk 500G compares the user login consumption time, and performs 10 tests. It takes an average of 16 seconds to log in to the system desktop using this system, and it takes an average of 16 seconds to log in with a trusted system without user authentication. Analysis Because the USBKey two-factor authentication replaces the original system user password authentication during the system login process, although the USBKey communication and the TPM communication consume time compared to the original system authentication, the time consumption can be neglected.

**4.2. Model Performance Analysis.** This method is implemented in the system of winning the standard Qilin + Godson 3A. The system performance is mainly analyzed from the following two aspects. The first is the user identity authentication measurement time, the second is the system whitelist query and measurement time, and the third is the file encryption/decryption time. For the system whitelist metrics, the following tests were made respectively, when the system whitelist was 300 and when the system whitelist was 600. A 1M size executable program is queried and the digest value is calculated and tested 10 times. The required time comparison is shown in Figure 4.1.

According to the experimental data, when the system trusted whitelist is basically the same in the query and measurement time required for 300 and 500. Therefore, it can be known that the query time in the whitelist is relatively short, mainly because the executable program summary is worth calculating. System whitelist queries and metrics have little impact on user experience and system performance at the ms level, and are within acceptable limits. For the time consumption of file transparent encryption/decryption, 10 groups of experiments are designed to consume time for reading and writing operations on 1M files and 2M files respectively. The time required to read and write 1M files and 2M files is shown in Figure 4.2.

The time to write the 1M file and the 2M file separately is as shown in Fig. 4.3.

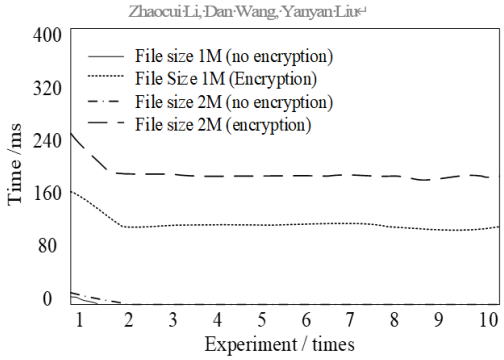


Fig. 4.2: Comparisons of the time required to read files

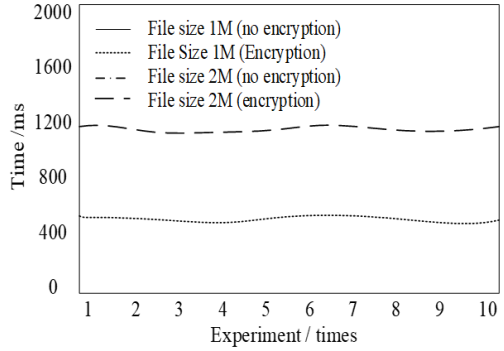


Fig. 4.3: Time required for file writing

Combined with the data of the file reading and writing experiment, it can be known that during the read operation, due to the caching mechanism of the system, the first reading time is greater than the time required to read the file later, the reading and writing time is compared, and the writing operation time is significantly larger than the reading operation time. This is because file writes require lock protection to prevent data consistency from being compromised. Comprehensive experimental data when the transparent addition and decryption functions are added, the file read and write operations take time to increase, but the increase time is still within the acceptable range of the user.

**4.3. Platform performance test and result analysis.** Three calculator programs are added to the dynamic measurement system for testing. Compared with the dynamic measurement system metric program, the CPU resource consumption and memory resource consumption are shown in Figures 4.4 and 4.5.

From the comparison experiments of Figs. 4.4 and 4.5, the CPU consumption rate of the enabled measurement system is 15% higher than that of the non-enabled measurement system. In terms of memory space usage, enabling metrics is about 8% more than enabling metrics. Since system consumption is related to the metrics process, it can be seen that there are certain effects on system performance when measuring three calculator processes. But, in order to ensure high reliability, the consumption of system resources is acceptable. The test terminal environment configuration of this paper is as follows: The processor chip adopts Godson 3A, the main frequency is 1GHz, the memory is 2G, and the hard disk is 500G. In order to test the performance of the ETAAP protocol, an experimental comparison is made with the protocol (TCP/IP) not used. The experiment is carried out 10 times. The 200KB data test is transmitted under two trusted computing platforms to check the comparison between the system CPU usage and the system memory usage during the transmission process.

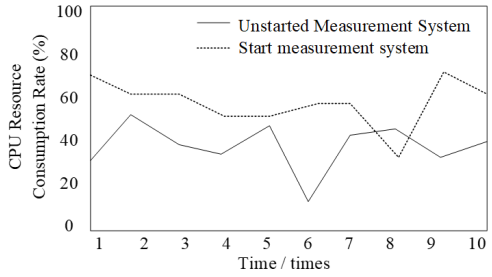


Fig. 4.4: CPU resource consumption ratio comparison

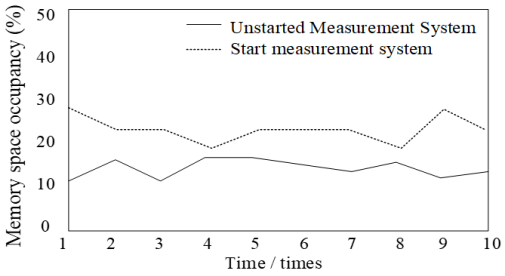


Fig. 4.5: Comparisons of memory occupancy

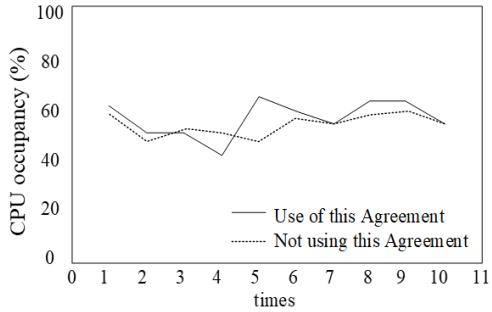


Fig. 4.6: CPU resource consumption

The experimental results are shown in Figure 4.6 and Figure 4.7.

It can be seen from the comparison between Fig. 4.6 and Fig. 4.7 that the CPU usage and memory usage of this protocol are basically different from those of the unused protocol. In response to the data delay caused by the adoption of this protocol, 200KB and 400KB files are tested and sent in the experimental environment, and 10 experiments are performed. The experimental results are shown in Figure 4.8 and Figure 4.9.

From the comparison implementation of Figs. 4.8 and 4.9, it can be seen that when transmitting the same size data file, the transmission time delay of adopting the end-to-end trusted anonymous authentication protocol and directly adopting the TCP/IP protocol is within 200ms. The delay of time mainly occurs in the verification phase of the identity authentication and extended system security attributes, and will not affect the system performance in the future data transmission. From the analysis of the experimental results, it can be seen that the impact of this protocol on the performance of the system is acceptable.In today's information age, computer terminals play an important role in various industries and fields. However, with the improvement

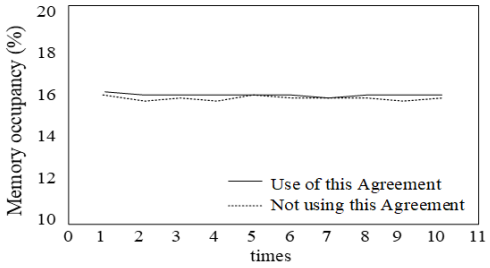


Fig. 4.7: Memory resource consumption

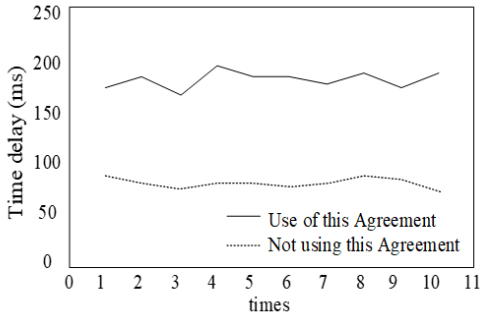


Fig. 4.8: Time Delay Contrast Diagram for Transferring 200KB Files

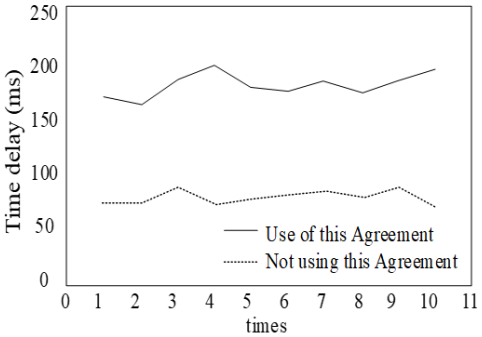


Fig. 4.9: Time Delay Contrast Diagram for Transferring 400KB Files

of its popularity, the security issues of computer terminals are becoming increasingly prominent. For critical or sensitive computer terminals, hardware level security measures such as security chips and trusted execution environments can be adopted to prevent physical attacks and illegal access. Timely update and upgrade the hardware components of computer terminals, such as CPU, memory, hard disk, etc., to improve the system's processing power and operational efficiency, while also reducing security vulnerabilities. For computer terminals involving sensitive information, measures such as encrypted storage and encrypted transmission can be adopted to ensure data security.

**5. Conclusions.** The research background and theoretical knowledge of trusted computing are introduced, and the platform structure, basic composition and functional mechanism of trusted computing are analyzed.

The basic components include a trusted platform module and a software protocol stack, which introduces the password support platform for trusted computing and the security function and password mechanism for password support. Based on the service provided by the trusted computing platform, the internal user behavior measurement model of the main text platform is studied. A USB Key user identity measurement model is proposed. In this model, based on the mutual authentication of USBKey and Trusted Platform Module, user identity based authentication and authorization are implemented. User identity based behavioral trust chain and data security encryption/decryption functions are established. Experimental analysis shows that the proposed method implements user behavior metrics and data security guarantee based on user identity grading. For the problem of security authentication between platforms, based on trusted computing, the zero-knowledge authentication protocol is used to complete the mutual authentication of the inter-platform identity, which further improves the security performance of the platform. Under this premise, mutual authentication is performed between the integrity of the platform and the security attributes of the platform to ensure that the security of the platform conforms to the access policy while the identity of the platform is correct. However, there are still deficiencies. In future research, it is necessary to further improve the applicability of the system and develop a security system in different environments.The simulation of database access information security management under big data platforms relies on a large amount of data for simulation and training. However, these data may have quality issues, such as incomplete or inconsistent data, which can have a negative impact on simulation results. Therefore, it is necessary to strengthen the evaluation and cleaning of data quality to ensure the accuracy of simulation. In the future, it is necessary to use artificial intelligence technology to intelligently upgrade simulation systems, such as adaptive optimization and automatic decision-making, in order to improve the efficiency and accuracy of simulation.

## REFERENCES


[1] Chehri, A., Fofana, I., Yang, X., *Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. Sustainability, 13(6): 3196, 2021.*

[2] Awaysheh, F. M., Aladwan, M. N., Alazab, M., *Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6):3676-3693, 2021.*

[3] Smys, D. S., Wang, D. H., Basar, D. A., *5G network simulation in smart cities using neural network algorithm. Journal of Artificial Intelligence and capsule networks, 3(1): 43-52, 2021.*

[4] Gong, Y., Liao, J., *Blockchain technology and simulation case analysis to construct a big data platform for urban intelligent transportation. Journal of Highway and Transportation Research and Development (English Edition), 13(4): 77-87, 2019.*

[5] Zhou, Z., Wang, M., Huang, J., *Blockchain in big data security for intelligent transportation with 6G. IEEE Transactions on Intelligent Transportation Systems, 23(7): 9736-9746, 2021.*

[6] Gladun, A. Y., Khala, K. A., *Ontology-based semantic similarity to metadata analysis in the information security domain. Problems in Programming, (2): 34-41, 2021.*

[7] Garg, S., Singh, A., Kaur, K., et al. *Edge computing-based security framework for big data analytics in VANETs. IEEE Network, 33(2): 72-81, 2019.*

[8] Wandji, P. Y. B., Charrier, C., Di, M. J.,*Deep features fusion for user authentication based on human activity. IET Biometrics, 12(4): 222-234, 2023.*

[9] Liu, X., Ding, N., Shi, J., *An Identity Recognition Model Based on RF-RFE: Utilizing Eye-Movement Data. Behavioral Sciences, 13(8): 620, 2023.*

[10] Stergiadis, C., Kostaridou, V. D., Veloudis, S., *A Personalized User Authentication System Based on EEG Signals. Sensors, 22(18): 6929, 2022.*

[11] Son. S., Park, Y., Park. Y., *A secure, lightweight, and anonymous user authentication protocol for IoT environments. Sustainability, 13(16): 9241, 2021.*

[12] Konstantelos, I., Jamgotchian, G., Tindemans, S., *Implementation of a Massively Parallel Dynamic Security Assessment Platform for Large-Scale Grids. IEEE Transactions on Smart Grid, PP(99): 1-1, 2016.*

[13] Sun, J., Khan, F., Li, J., *Mutual authentication scheme for the device-to-server communication in the Internet of medical things. IEEE Internet of Things Journal, 8(21): 15663-15671, 2021.*

[14] Janjanam, L., Saha, S. K., Kar, R., *Optimal Design of Hammerstein Cubic Spline Filter for Nonlinear System Modeling Based on Snake Optimizer. IEEE Transactions on Industrial Electronics, 70(8): 8457-8467, 2022..*

[15] Hirose, K., Kim, S., Kano, Y., et al. *Full information maximum likelihood estimation in factor analysis with a large number of missing values. Journal of Statistical Computation & Simulation, 86(1): 91-104, 2016.*

[16] Liang, J., Zhang, M., Leung, V. C. M., *A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud. IEEE Internet of Things Journal, 7(6): 5481-5490, 2020.*

[17] Teisserenc, B., Sepasgozar, S., *Adoption of blockchain technology through digital twins in the construction industry 4.0: A PESTELS approach. Buildings, 11(12): 670, 2021.*

[18] Kiu, M. S., Chia, F. C., Wong, P. F., *Exploring the potentials of blockchain application in construction industry: a systematic review. International journal of construction management, 22(15): 2931-2940, 2022.*
[19] Sukhija, N., Bautista, E., *Towards a framework for monitoring and analyzing high performance computing environments using kubernetes and prometheus, 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 257-262, 2019.*
[20] Liu, Z., Chi, Z., Osmani, M., et al. *Blockchain and building information management (BIM) for sustainable building development within the context of smart cities. Sustainability, 13(4): 2090, 2021.*
[21] Rahman, A., Nasir, M. K., Rahman, Z., *Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management. IEEE Access, 8: 140008-140018, 2020.*
[22] Li, W., Wu, J., Cao, J., *Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. Journal of Cloud Computing, 10(1): 1-34, 2021.*
[23] Zhong, B., Wu, H., Ding, L., et al. *Hyperledger fabric-based consortium blockchain for construction quality information management. Frontiers of engineering management, 7(4): 512-527, 2020.*
[24] Thapa, C., Camtepe, S., *Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 129: 104130, 2021.*

*Edited by:* Zhigao Zheng
*Special issue on:* Graph Powered Big Aerospace Data Processing
*Received:* Oct 30, 2023
*Accepted:* Nov 24, 2023