Data Security Design in Computer Application Software Development from the Perspective of Information Security Environment

Qiyuan Jie

{jieqiyuan2008@126.com}

College of Computer and Information, Department of Information, Hohai University, Nanjing, 211100, Jiangsu Province, China

Abstract. Information security plays a vital role in computer application software development. With the advent of the digital age, a large amount of sensitive information is stored and transmitted. Ensuring the security of this data is critical for individuals and organizations alike. So this paper studies the security of software development from the perspective of information security. This paper mainly uses the method of comparison and experimental testing to analyze the key points of software development and data security strategies. The experimental results show that in the first data, the recording efficiency of the data computer system for encryption is 1468ms, while that of unencrypted recording is 1368ms, a difference of 100ms. The results of the read-write efficiency test show that the operating efficiency of the encrypted database does not decrease significantly, which meets the efficiency requirements of users in actual projects.

Keywords: Information Security, Application Software, Data Security, Key System

1 Introduction

Information security plays an important role in the development of computer application software. In software development, data security design is an essential link. However, there are many information security environment issues and challenges. One of them is the risk of hacking and data breaches. Hackers try to break into systems and steal sensitive information, which poses a threat to personal privacy and business interests. In addition, software bugs and vulnerabilities, social engineering attacks, etc. can also make data insecure. To deal with these problems, various countermeasures are required to ensure information security.

With the development of network technology, computer application software plays an increasingly important role in people's life. S. Muthulakshmi et al. stated that in the Internet of Things, the traditional solutions for secure information exchange become blurred due to the presence of intruders. Blockchain is the answer to solving problems and mitigating threats by providing a lightweight and secure IoT information model for

ICSETPSD 2023, November 17-18, Coimbatore, India

DOI 10.4108/eai.17-11-2023.2342617

smart applications that considers data security and efficiency [1]. According to M. Jalasri et al., most of the data is collected through IoT devices and needs to be stored in the cloud for further analysis. Intermediary access or attempts by unauthorized users to access sensitive information during data storage can lead to privacy, integrity, and confidentiality issues [2]. S. Aanjanadevi et al. pointed out that since the Internet is widely used to transmit data over the network, security and authenticity have become the main risks. He proposed a biometric security system based on fuzzy extractors and convolutional neural networks [3]. In order to ensure that computer software can meet the needs of users and ensure the safety of user operations, it is particularly prominent to formulate reasonable and effective safety management methods and measures.

This paper first discusses information security and evaluation methods, which explains the importance of data security, and uses defense evaluation related algorithms for analysis. Secondly, the basic theories and methods of application software development are discussed separately, and then the data security strategy is stated from different aspects. Finally, through the data security design experiment, the data security method in this paper is compared and analyzed, and the relevant data results are obtained.

2 Analysis of Data Protection in Information Security and Application Software Development

2.1 Information Security and Assessment Methods

In the development process of computer application software, data security is a very important issue that must be considered. Because if it is not clearly indicated that the information is effectively protected, tampered with or lost, etc., then the user's high-level requirements for system security cannot be met. Information security refers to the security of data when the computer is in use, that is, the network system will not maintain normal operation due to human factors [4-5]. Its security design is to protect computer application software, so as to ensure that user data is not subject to malicious attacks, loss and disclosure [6]. In the traditional sense, due to the openness of the network environment, people have doubts about security. With the development of modern science and technology and the increasing penetration rate of the Internet, more and more enterprises use the network model to achieve their own value maximization goals, so it is necessary to use information technology to solve information security problems.

The status of the defender's loss of detection will cause the cloud computing system to be unable to respond to the malicious attacker's attack behavior. Although it will not bring resource overheads such as punishing malicious attackers and restoring damaged files, it will not be able to avoid system damage caused by malicious attacks [7-8]. This paper defines the payoff functions of the malicious attacker and the defender in the computer risk assessment game model as:

$$P_A = Y_A - Z_A \tag{1}$$

$$P_D = Y_D - Z_D \tag{2}$$

Among them, Y_A and Y_D denote the benefits of malicious attackers and cloud computing defenders, respectively. The damage function of the system is:

$$L_{Damage} = GL_i \times (L_d \times W_d + L_J \times W_J + L_X \times W_X + L_S \times W_S + L_{Xv} \times W_{Xv}) \tag{3}$$

Among them, GL_i represents the degree of harm inherent in a certain type of attack itself. In addition, J stands for integrity, d stands for confidentiality, X stands for availability, and S stands for trustworthiness. This paper uses Hadoop to build a cloud computing environment, and combines Nusses and Snort two application software to scan the entire cloud computing environment for vulnerabilities and risk threats. Combined with expert scoring, the identification of information vulnerability is evaluated from five aspects: confidentiality, integrity, usability, credibility, and auditability. By dividing the risk value, the range of risk value corresponding to each security level is obtained, as shown in Table 1:

Table 1. Range of Risk Values for Each Safety Level

Grade	Range
Very low	<=3
Low	3~6
Middle	6~9
High	9~12
Very high	>=12

Information sharing in the network environment is a substitute for traditional information collection, analysis and sharing, not a supplement. If the internal information integration ability is not guided by regulations, it may lead to a large number of information risks. Especially in the network commercial environment, artificial intelligence technology has a strong ability to aggregate and process data information, which may threaten the independent decision-making power of user information. It is difficult for information subjects to find out that their rights have been violated in the first place. It is difficult to determine the subject of infringement, and it is even more difficult to pursue responsibility.

2.2 Computer Application Software Development

Computer application software development is the process of designing, writing, testing and maintaining software applications for computer equipment using appropriate programming languages, tools and techniques. Its development process is shown in Figure 1.

In the initial stages of software development, it is necessary to analyze customer, user and market needs in order to clarify the goals, functions and performance of the software application. Requirements analysis is the cornerstone of the entire development process, ensuring that the software project in this paper meets the actual needs of users. Designing software architecture and framework based on requirements analysis includes selecting technology stack, determining module structure and creating interface specification. Good design improves software maintainability, scalability, and performance. The programming phase is a core part of the software development process. According to the design scheme, programming languages and corresponding tools are used to realize the software functions. During this process, it is necessary to follow programming standards and best practices to ensure the quality and readability of the software code. Software testing aims to detect and correct errors and vulnerabilities in software, and to verify whether the software meets requirements and is efficient and usable. After testing, deploying the software to the target environment, such as a server, client, or mobile device. The deployment process may require configuring databases, network settings, and security options. Software development does not end at the deployment phase. After the software is debugged, it must be monitored, maintained and optimized to ensure the stable and efficient operation of the software system. Version management and updates are necessary to continuously adapt software to changing user and market needs. This includes fixing bugs, adding new features, improving performance and adapting to new technologies.

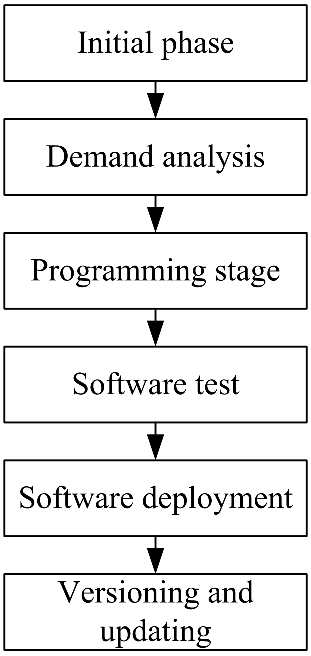

Fig.1 Computer application software development process

Developing software is a complex project involving multiple phases and interdisciplinary knowledge. This requires basic knowledge of programming languages, algorithms, data structures, operating systems, and the ability to solve practical problems. Additionally, good teamwork, communication skills, and time management skills are also essential for software development. Appropriate countermeasures and technical means can effectively guarantee data security and protect the interests of individuals and organizations. At the same time, data security analysis helps to identify potential security issues and take appropriate preventive measures. Information security plays a vital role in the development of computer application software.

This must be designed from an overall system security perspective and ensure that security requirements are fully considered when designing and implementing the system. Software design and architecture based on security best practices implement appropriate authorization and access control mechanisms, as well as effective authentication and authorization mechanisms [9-10]. Sensitive data must be encrypted, stored, transmitted and processed using appropriate encryption algorithms and protocols to ensure that data is not easily stolen, altered or disclosed during storage and transmission. Threat modeling and security analysis are critical steps in the development process. Security threats in the system should be deeply analyzed and appropriate security policies and safeguards should be developed. This includes identifying potential vulnerabilities and making corrections through methods such as vulnerability analysis and security testing [11-12]. In addition, the development and training of security awareness should be emphasized. Through regular security training, developers' awareness and understanding of security issues can be improved, the operational behavior in the development process can be standardized, and the quality and design level of software security can be improved. Vulnerabilities and software errors are one of the biggest threats in information systems. Quickly fixing and update security holes and bugs in software to keep it safe and stable. Computer application software in certain fields and industries may require safety certification and conformity assessment. Complying with applicable security standards and norms to ensure software complies with applicable regulations and industry requirements. Response and elimination are important steps in security incident and incident management. Formulating a clear response and disposal plan, and take appropriate emergency measures in a timely manner to minimize losses in the event of a security incident. Information security design is a comprehensive task that requires comprehensive thinking from multiple perspectives. Only by enhancing the security awareness of the software development team, constantly updating the software security mechanism, and strictly adhering to the security standards and norms of design and development, can we provide safer and more reliable computer application software.

2.3 Data Security Policy

Encryption is an important method to protect sensitive data [13-14]. When developing application software, encryption algorithms should be considered to encrypt data storage and transmission to ensure that data is not easily stolen or manipulated during storage and transmission. At the same time, keys must be properly managed to avoid key leakage. Access control is an important measure to prevent unauthorized access. Reasonable access control policies may restrict access to sensitive data, including permission levels and role settings [15-16]. Only authorized users can access the corresponding data, thus effectively protecting data security. When developing software, it is important to consider using secure authentication and authorization mechanisms to verify and authorize user identities. This ensures that only legitimate users can access sensitive data while protecting against malicious actions by illegitimate users. Data backup and recovery is an important method of dealing with accidental data loss or catastrophic crashes and ensuring rapid recovery in the event of data loss or corruption. Software development should consider establishing a regular data backup mechanism and ensure timely recovery of backed up data. Detecting and track security events in the system in a timely manner by recording logs and performing audits. Security auditing and monitoring systems help to quickly identify potential security risks [17-18]. Also, regular vulnerability analysis and remediation is critical. During the software development process, attention should be paid to recording the log information of key operations, abnormal events, and security events, and ensuring the safety of traceability analysis and investigation protocols when necessary. When developing software, this paper should consider introducing an exception handling mechanism to detect and handle exceptions in software operations in a timely manner to avoid system crashes caused by data leakage or exceptions. At the same time, security assessment and vulnerability analysis should be conducted regularly to quickly correct and update security vulnerabilities in software [19-20]. During software development, it is very important to maintain security awareness and knowledge. Regular training on the latest security threats and protections is required to increase the importance of data security design. In computer application software development, performing data security analysis is an important step in ensuring data security. This helps to avoid and resolve potential issues in advance and ensures the security of application data.

3 Data Security Design Experiment

3.1 Transmission and Storage Encryption

Data encryption technology is an important requirement to ensure network security, especially in cloud computing services with very high data volumes. Due to the rapid development of information technology and the growing demand for data encryption, data encryption has also attracted the attention of industry experts. Encryption technology is mainly divided into symmetric key algorithm and asymmetric key algorithm. Digital envelope technology is an encryption technology that combines asymmetric encryption and symmetric encryption. By using digital envelope technology, it overcomes the difficulty of key distribution in private key encryption and the problem of long encryption time in public key encryption. The traditional DES (data encryption standard) encryption algorithm is a symmetric encryption algorithm. The algorithm can provide high-quality data protection and protect data from theft and malicious attacks. In order to improve the security of the algorithm, various improved algorithms have been proposed, mainly for increasing the key size, such as the triple DES algorithm. The triple DES algorithm effectively improves the security of the algorithm, but the time is doubled, which greatly reduces the execution efficiency. A simple DES key expansion method extends the effective bit length of the algorithm key from one bit to another without reducing the encryption effect of the algorithm, but only increases the time to generate part of the key. The test results of plaintext "avalanche phenomenon" and key replacement are shown in Figure 2.

The improved DES algorithm has an encryption effect similar to that of the traditional encryption algorithm. When using the traditional DES encryption algorithm, short keys are vulnerable to brute-force exhaustion attacks under current high-speed computing conditions. Therefore, the use of the improved algorithm proposed here not only meets the speed requirements that the asymmetric encryption algorithm cannot achieve, but also makes up for the disadvantages of the traditional algorithm that are vulnerable to attacks, and has good encryption results.

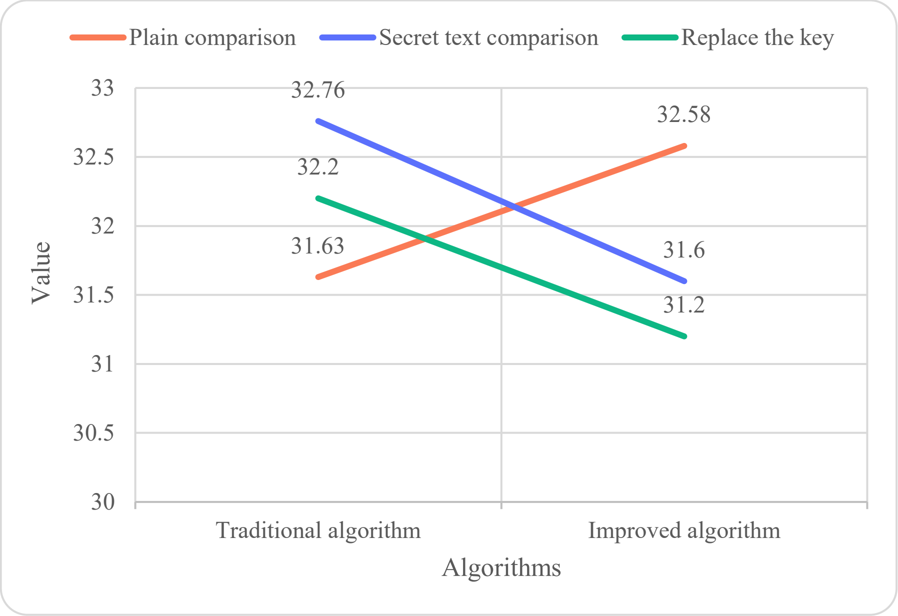

Fig.2 Clear text of the "avalanche phenomenon" and the test results of the key replacement

3.2 Database Security Measures and Test Environment Construction

Recorded information stored in a database system is sometimes not what some users expect, and it is expected that the information in the database can be retrieved correctly in the event of a software or hardware error in the database management system. The security of database systems is closely related to the security of computer systems, where security measures are usually defined by a layered approach. The first step is to check the legitimacy of the identity of the user entering the computer system. Users accessing computer systems must be authenticated users. For authorized users entering the system, the database management system must also enforce access control to allow users with appropriate access rights to access the corresponding data. For information stored in a database, the confidentiality of the information can be ensured by storing encrypted text.

In the actual build test environment, it is divided into two parts: the host and the target device. The host operating system is the Windows operating system on which the Tornado 2.2 integrated development environment runs. The operating system of the target device is Works 5.6 running on a virtual machine. The implementation of the encryption function assumes that the external interface of the database is not modified as much as possible, and the implementation of the encryption function is transparent to the user. When testing the encryption performance of the embedded database, the original database is set as an empty database, and the data is written to the database for five consecutive times, each writing 100,000 records. When a record is written, the corresponding fields that require encryption are encrypted and stored in the database.

3.3 Test Results

As shown in Figure 3, in the write efficiency test, the encrypted write record efficiency value is always greater than the unencrypted write record efficiency value. In the fifth data, the recording efficiency of the system for encryption is 1317ms, while that for unencrypted recording is 1185ms, a difference of 132ms.

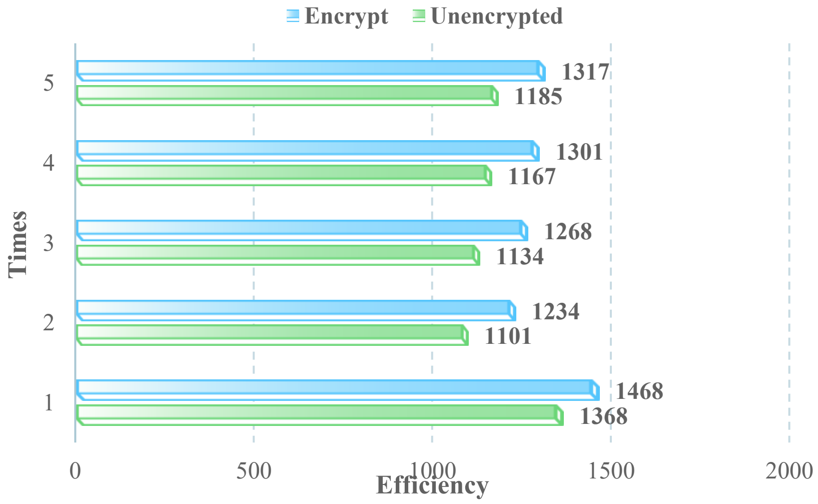

Fig.3 Writing efficiency test results

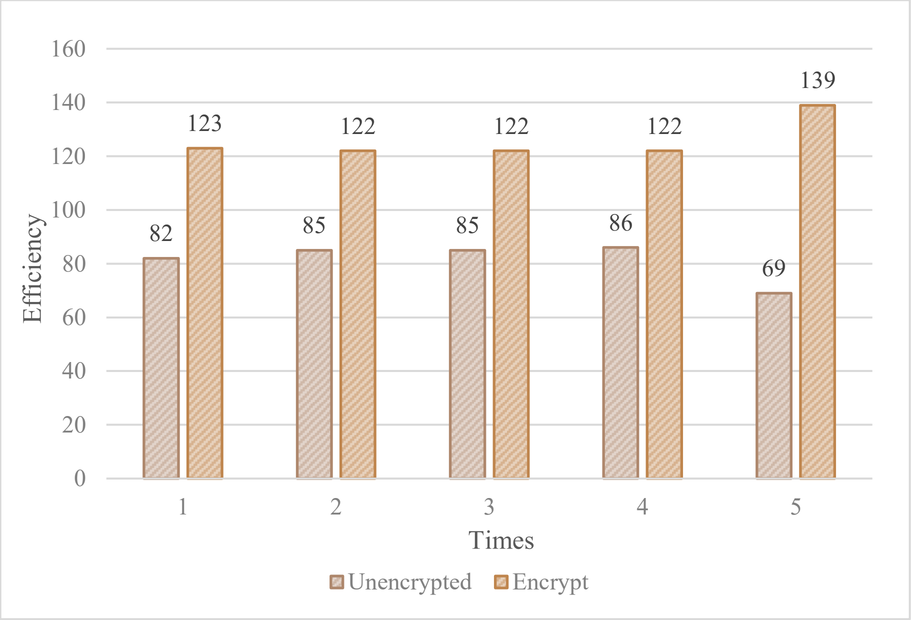

Fig.4 Reading efficiency test results

As shown in Figure 4, in the read efficiency test, the encrypted read record efficiency value is always greater than the unencrypted read record efficiency value. In the first data, the system's read record efficiency for encryption is 123ms, while that for unencrypted records is 82ms, a difference of 41ms. In the fifth data, the recording efficiency of the system for encryption is 139ms, while that for unencrypted recording is 69ms, a difference of 70ms. The encryption read record efficiency of the first four times is consistent.

Testing the encryption capabilities of the embedded database can determine the encryption information for encrypted database storage fields. If the database key is entered correctly, the database data can be read correctly. However, if the key is entered incorrectly, the database information cannot be accessed, thus effectively preventing illegal user access. At the same time, in order to ensure the security of encrypted dictionary files, a hierarchical key management system is introduced.

4 Discussion

In computer application software development, data security is a problem that cannot be ignored. Data security not only means that there will be no errors and damages when the system is running, and there will be no failures in the use process, but it also includes the protection of database information. Some important files should be backed up regularly. In the process of computer application software development, it is necessary to fully consider the possible security risks of the software itself, such as hacker attacks, Trojan horse viruses, and illegal access. These threats can result in the interception and destruction of information resources. Therefore, certain measures need to be taken to prevent such risk events from happening. Only by ensuring that the system has high reliability and stable performance can the information security of the entire system be guaranteed.

In terms of the security performance of computer application software, it mainly refers to encrypting and protecting data. Information security is achieved through methods such as cryptography and network protocols, and a complete and effective encryption system is established to ensure its security and stability. A variety of data management methods can also be used to implement confidentiality control and recovery functions to ensure its effectiveness and improve the security performance of computer application software. Strengthening firewall technical precautions to prevent illegal access through encryption. Setting up sensitive files specially used to protect against viruses, hacker attacks, etc., regularly check and update important application software to ensure its security. At the same time, it is also necessary to strengthen data management and maintenance to ensure that computer application software can run safely.

5 Conclusion

In the development of computer application software, data security is a core issue and also a difficult point. This paper mainly studies the data protection of computer application program design under the information security environment. To ensure data security, access control needs to be strengthened, and only authorized users are allowed to access sensitive data. Encryption technology is also an important means to protect data security. For important sensitive information, strong encryption algorithms should be used for encrypted storage and transmission. In addition, sound security training and awareness raising are also important factors in preventing social engineering attacks. By taking appropriate measures to ensure the confidentiality, integrity and availability of data during storage, transmission and processing.

References

[1] S. Muthulakshmi, A. Kannammal: Security Enhancements Based on Optimal Lightweight Blockchain Model for Data Sharing in Wireless IoT Networks. Ad Hoc Sens. Wirel. Networks 55(3-4): 233-256 (2023)

[2] M. Jalasri, L. Lakshmanan: Managing data security in fog computing in IoT devices using noise framework encryption with power probabilistic clustering algorithm. Clust. Comput. 26(1): 823-836 (2023)

[3] S. Aanjanadevi, S. Aanjankumar, K. R. Ramela, V. Palanisamy: Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics. Comput. Syst. Sci. Eng. 45(3): 2351-2362 (2023)

[4] Volodymyr I. Rozvadovsky, Liubomyr V. Zinych, Andriy A. Albu: Post-Soviet Estonia's information safety: lessons for Ukraine. Int. J. Electron. Secur. Digit. Forensics 13(1): 53-63 (2021)

[5] Khadija Ashraf, Vignesh Varadarajan, Md. Rashed Rahman, Ryan Walden, Ashwin Ashok: See-Through a Vehicle: Augmenting Road Safety Information Using Visual Perception and Camera Communication in Vehicles. IEEE Trans. Veh. Technol. 70(4): 3071-3086 (2021)

[6] Xiaofeng Qi, Tiejun Cui, Liangshan Shao, Yuyan Xing: Research on intelligent

classification of multi-attribute safety information and determination of operating environment. J. Ambient Intell. Humaniz. Comput. 11(9): 3509-3520 (2020)

[7] S. Prince Chelladurai, T. Rajagopalan: Intelligent Digital Envelope for Distributed Cloud-Based Big Data Security. Comput. Syst. Sci. Eng. 46(1): 951-960 (2023)

[8] Shiny Mukkath I., Nirmala Devi M.: PUF based on chip comparison technique for trustworthy scan design data security against side channel attack. Int. J. Cloud Comput. 12(2/3/4): 201-223 (2023)

[9] Hamza Rafik, Abderrahim Maizate, Abdelaziz Ettaoufik: Data Security Mechanisms, Approaches, and Challenges for e-Health Smart Systems. Int. J. Online Biomed. Eng. 19(2): 42-66 (2023)

[10] Ankush Balaram Pawar, Shashikant U. Ghumbre, Rashmi M. Jogdand: Privacy preserving model-based authentication and data security in cloud computing. Int. J. Pervasive Comput. Commun. 19(2): 173-190 (2023)

[11] Mustafa Qahtan Alsudani, Mustafa Musa Jaber, Rami Qays Malik, Sura Khalil Abd, Mohammed Hasan Ali, Ahmed Alkhayyat, G. A. Khalaf: Blockchain-Based E-Medical Record and Data Security Service Management Based on IoMT Resource. Int. J. Pattern Recognit. Artif. Intell. 37(6): 2357001:1-2357001:24 (2023)

[12] M. I. Mary Metilda, D. Lalitha, S. Vaithyasubramanian: Data security-web login authentication process using password generating tile array token interval timed coloured Petri nets. Int. J. Wirel. Mob. Comput. 24(2): 134-143 (2023)

[13] Balamurugan Perumal, Arulkumaran Ganeshan, Santhosh Jayagopalan, K. S. Preetha, Ramasamy Selamban, Dinesh Elangovan, Sumathy Balasubramani: Real time multi view image based FPC plant management with SS data security and low rate attack detection for efficient smart agriculture in WSN. J. Intell. Fuzzy Syst. 44(1): 91-100 (2023)

[14] Dulal Kumbhakar, Kanchan Sanyal, Sunil Karforma: An optimal and efficient data security technique through crypto-stegano for E-commerce. Multim. Tools Appl. 82(14): 21005-21018 (2023)

[15] Tina Marjanov, Maria Konstantinou, Magdalena Józwiak, Dayana Spagnuelo: Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR. Proc. Priv. Enhancing Technol. 2023(3): 405-417 (2023)

[16] Parsa Sarosh, Shabir Ahmad Parah, Bilal Ahmad Malik, Mohammad Hijji, Khan Muhammad: Real-Time Medical Data Security Solution for Smart Healthcare. IEEE Trans. Ind. Informatics 19(7): 8137-8147 (2023)

[17] Venkatachalam Balamurugan, Ramamoorthy Karthikeyan, B. Sundaravadivazhagan, Robin Cyriac: Enhanced Elman spike neural network based fractional order discrete Tchebyshev encryption fostered big data analytical method for enhancing cloud data security. Wirel. Networks 29(2): 523-537 (2023)

[18] Paramita Chatterjee, Rajesh Bose, Subhasish Banerjee, Sandip Roy: Enhancing Data Security of Cloud Based LMS. Wirel. Pers. Commun. 130(2): 1123-1139 (2023)

[19] Chippada Nagamani, Suneetha Chittineni: Network database security with intellectual access supervision using outlier detection techniques. Int. J. Adv. Intell. Paradigms 22(3/4): 348-361 (2022)

[20] Luis Alberto Núñez Lira, Kukati Aruna Kumari, Ramakrishnan Raman, Ardhariksa Zukhruf Kurniullah, Santiago Aquiles Gallarday Morales, Tula Del Carmen Espinoza Cordero: Data Security Enhancement in 4G Vehicular Networks Based on Reinforcement Learning for Satellite Edge Computing. Int. J. Commun. Networks Inf. Secur. 14(3): 59-72 (2022)