Network Security Design for Cloud-Based Systems: A Computer Network Perspective

Yutao Tang

Nanjing Yuma Software Technology Co., Ltd. Jiangsu Nanjing 210000

Abstract: ***With the continuous development of computer networks, cloud computing has emerged as a transformative paradigm. Its distinctive characteristics and substantial advantages have significantly reshaped traditional network application models. At present, as an advanced Internet technology, cloud computing has been widely adopted in daily life, bringing considerable convenience to users. To ensure the secure and effective application of cloud computing, it is essential to prioritize security prevention efforts, enhance security awareness, and optimize protective measures, thereby addressing computer network security challenges within the context of cloud computing development. This paper briefly describes the key characteristics of cloud computing technology, analyzes the existing problems in computer network security within cloud computing environments, and further discusses viable security prevention strategies.***

Keywords: Cloud computing; Computer network Security; Problem analysis.

1. INTRODUCTION

This article mainly focuses on computer network security prevention in cloud computing environment. Based on the collection and organization of literature, the author has conducted a detailed analysis and research on the topic. On the basis of elaborating on relevant theoretical foundations, this article analyzes the problems in computer network security prevention in cloud computing environments, and then proposes optimization measures for computer network security prevention in cloud computing environments. It is hoped that through the research in this article, certain reference and assistance can be provided for the optimization and improvement of computer network security prevention in cloud computing environments. Yang et al. [1] introduced HGMatch, a match-by-hyperedge approach for subgraph matching on hypergraphs, enhancing the efficiency of complex graph analytical queries. Addressing challenges in dynamic data environments, Ukey et al. [2] developed an efficient method for continuous kNN join over dynamic high-dimensional data, providing scalable solutions for real-time similarity search. Within the financial sector, Yang et al. [3] constructed multi-dimensional network credit-related transaction risk maps by integrating graph neural networks, enabling early warning capabilities for financial anomalies. Extending this line of financial security research, Shen et al. [4] applied the Whale Optimization Algorithm to financial payment fraud detection, demonstrating the effectiveness of bio-inspired optimization in identifying fraudulent transactions. In the field of computer vision, Peng et al. [5] exploited aggregation and segregation of representations for domain adaptive human pose estimation, improving model generalization across diverse scenarios. Wu et al. [6] addressed structural health monitoring by developing a small-sample object detection method for surface cracks in concrete structures of high-rise buildings via multi-level transfer learning, tackling the practical challenge of limited training data in critical infrastructure inspection. In photonic device engineering, Tang et al. [7] presented work on the design and optimization of shallow-angle grating couplers for vertical emission from Indium Phosphide devices, contributing to integrated optics development. Sun [8] explored human-computer interaction by proposing adaptive interfaces for personalized user experience using a machine learning approach, enhancing user engagement through intelligent adaptation. Lian and Chen [9] contributed to foundational AI methodologies through research on complex data mining analysis and pattern recognition based on deep learning, advancing capabilities for large-scale knowledge discovery. Zheng and Jiang [10] addressed natural language processing challenges by developing a new methodology for Chinese term extraction from scientific publications, improving precision in domain-specific terminology identification. Complementing earlier work, Wu et al. [11] further validated their small-sample object detection approach for surface cracks in concrete structures of high-rise buildings via multi-level transfer learning. Ding et al. [12] achieved significant progress in unsupervised clothing-changing person re-identification through multi-scale adaptive clustering and local consistency learning, addressing a particularly challenging variant of person retrieval. Finally, in the automotive industry, Ziren [13] conducted dynamic optimization and multi-regional performance validation of automotive sales strategies in the United States, offering empirical insights into region-specific market dynamics.

2. COMPUTER NETWORK SECURITY FEATURES

Cloud computing technology is developed on the basis of electronic communication technology, Internet technology and other technologies. Nowadays, cloud computing has been widely applied in various fields of social life and production in China, promoting the diversified development of computer networks. So, for computer network security issues in cloud computing environments, there are mainly the following characteristics:

(1) Integrity

For computer networks in cloud computing environments, it is not possible to delete or modify data information in the network without user authorization, thus having the advantage of integrity.

(2) High confidentiality

The computer network data information in cloud computing environment has high privacy, and existing data information cannot be shared and disseminated without relevant authorization operations.

(3) Good information auditing quality

For computer network security issues, diverse security risks and hidden dangers often occur. Computer networks can authorize users through cloud computing to help them protect their own data information.

(4) High operability

In the environment of cloud computing, computer networks cannot apply, share, disseminate, and process user data information without user authorization.

3. THE CURRENT STATUS OF COMPUTER NETWORK SECURITY IN CLOUD COMPUTING ENVIRONMENT

3.1 Virus and hacker issues

The problem of virus hackers has always been an important issue affecting computer network security. In the cloud computing environment, the targets of hackers and viruses are more clear and the methods are more diverse. Hackers are a major threat to network security in cloud computing environments, and due to the large amount of internal data and complex content, the uncertainty of hacker intrusion gradually increases. Some hackers enter cloud systems to copy and steal information, while others invade cloud systems with the intention of proving their technical strength. However, regardless of the purpose of hackers, the damage to cloud systems and the impact on cloud computing are extremely vicious. Hackers in cloud computing environments must pay attention to the interference and harm of cloud computing. In order to enhance the ability of cloud systems to resist hackers, various network security teams are constantly strengthening the protective measures of security systems. Virus issues are an important factor affecting computer network security and a common problem in cloud computing environments. At present, network viruses in cloud computing environments have undergone significant changes, and traditional infectious disease models such as SIS, SIR, SEIR, etc. have undergone new changes and modifications in cloud computing environments, bringing adverse effects to network security in cloud computing environments. Currently, research on viruses in cloud computing environments is constantly improving. Network security experts will analyze the characteristics of virus transmission and concealment methods in cloud systems, and use corresponding antivirus software and system upgrades to remove viruses.

3.2 Cloud computing security risks

The security risks inherent in cloud computing are a major threat to computer network security. The use of distributed computing has fast data processing and computing speed, but the transmission of data to cloud systems carries significant security risks. With the mastery of cracking keys, it is easy to obtain a large amount of data information. In cloud computing applications, user personal privacy and the uploading and storage of large enterprise commercial data are involved, and these data values are extremely high. Although cloud computing service providers provide information security guarantees for enterprises and individuals, the uncertainty of

internal personnel and the temptation of internal data value increase the risk of data information in the cloud computing environment. In recent years, many cases of data breaches have been malicious incidents caused by internal personnel violating the law. Therefore, in order to strengthen computer network security prevention in cloud computing environments, in addition to preventing external risks, effective and standardized internal key storage should also be adopted.

3.3 Safety technical issues

Security technology has always been the most critical issue in computer network security. With the increasing demand for computer security technology in cloud computing environments, there are more and more problems exposed in terms of security technology. There are many shortcomings in computer security technology in cloud computing environments, especially in terms of ensuring security technology. At present, security protection software and systems related to cloud computing are still in a constantly developing and improving stage. Network security technology in cloud computing environments often corresponds to security threats, and common issues such as privacy theft, resource impersonation, and virus infection in cloud computing environments urgently require reliable security technology to handle. The current information security protection technology still has certain limitations, especially in cloud computing environments where a large amount of data and information are stored. Due to weak security protection technology, it is easy for criminals to steal it. Security protection technology is a technology that needs to be continuously improved to ensure network security in cloud computing environments. At the same time, when users use cloud computing for data computation, the data encryption technology is less rigorous and the key is easily cracked during the data transmission connection process, which is also a common deficiency in current security technology.

4. STRATEGIES FOR STRENGTHENING COMPUTER NETWORK SECURITY PREVENTION IN CLOUD COMPUTING ENVIRONMENT

4.1 Reasonable application of encryption technology

It is very important to enhance the security of information data and protect the legitimate rights and interests of users. In the process of improving security and confidentiality, the most common and highly operational method is to use encryption technology. When using this technology, data is generally transmitted securely in cloud management and cloud storage servers. The most commonly used encryption technology today is the RSA asymmetric encryption algorithm, which directly transfers asymmetric data between the server and the user using the keys present in the user. In general, the DES symmetric encryption algorithm is used for data transmission. In real life, when users want to store data, the data will enter the corresponding database, and then be encrypted by the user's encryption technology. In the virtual network environment, diversified authentication modes are used to verify the user's identity. Then, cloud computing security systems can enhance the confidentiality of the security system while ensuring information security.

4.2. Enhance the awareness of client security precautions

In the context of cloud computing, users' awareness of security precautions cannot be ignored, and it is necessary to continuously enhance and educate users' awareness of precautions. Firstly, ensuring the personal identity authentication of users, including real name authentication and SMS authentication, can effectively prevent the intrusion of unidentified individuals, criminals, and hackers. This can achieve strict supervision of unauthorized users and centralized control of negative impacts. Secondly, users should learn to have basic knowledge of network security and good computer operation habits, and avoid setting data information and corresponding storage passwords on public computers. Regular security checks, virus scanning, vulnerability fixing, and patch installation should be conducted on computers to prevent illegal intrusion by clients. Enterprise users should develop unique security measures based on their own characteristics. For example, companies providing services for cloud platforms can effectively improve the protection level of their computer systems through filtering and prevention measures. Common methods include using open-source encryption software TrueCrypt to encrypt disks, RSA and DES to encrypt user information, adding Websense to intercept malicious code, using Vontu to protect confidential software, using Vericept tool to monitor data transmission in personal user computers, promptly identifying security risks, filtering and intercepting malicious information, and ensuring data security.

4.3 Data Backup and Restoration

To ensure the security of computer networks in cloud computing environments, it is necessary to perform necessary data backup and restoration to avoid serious losses to users caused by data damage and loss. During the user operation process, it is easy to encounter operational errors and virus attacks, and data backup and restoration measures need to be taken to ensure data integrity. In the context of cloud computing, the storage of information data is carried out in a discrete manner, which enables rapid data restoration. Therefore, regularly backing up data can ensure data security. In case of data damage or loss, it can also be restored and recovered to avoid user losses.

4.4 Building a Security Protection System

In order to improve and optimize the management mode of computer network security, relevant personnel can actively build a computer network security protection system, including two modules: workstation protection and server protection. Workstation protection belongs to the lowest level of computer network security protection system and is the last security defense measure. Server protection should not only have the ability to monitor viruses, but also include automatic virus code updates, alarm functions, and remote installation functions. The majority of users have a high frequency of email and web browsing, leading to an increasing number of virus intrusion paths. The security of user data information can be ensured by setting new levels. For users' network data information resources, once a security incident occurs, it will result in significant losses. Therefore, users can ensure their data security by regularly backing up data information within the computer network, such as backing up system logs and server data. Once an accident occurs in the computer network, user data information can be restored in a timely manner. Users can reduce the adverse effects of computer network security incidents by purchasing professional network backup software.

4.5 Implement centralized management of information data

Establish a security model for cloud computing, integrate computer information and data resources, and conduct comprehensive management. Pay attention to the control of boundary information data, implement dynamic resource management, and analyze and study it to develop more logical processes for the construction of information data, promote the development of physical structures, ensure system security in the field of physical boundary security, and better ensure the traffic and confidence security of corresponding operations in cloud computing environments. In this process, a two-level personnel responsibility system is implemented for data management. Ordinary operation and maintenance personnel are only responsible for the daily maintenance and operation of the server, while core personnel have stricter operation and maintenance process constraints to control their tampering, deletion, and use of user data information, greatly enhancing the security of the computer network and ensuring the security and confidentiality of data.

5. CONCLUSION

To sum up, with the rise and development of the Internet, human beings have entered the era of information technology, and cloud computing technology is also developing and improving. This technology has contributed to the development of society, which has made people's lives more convenient. However, cloud computing can also be called a double-edged sword. This technology can provide convenience for people's work and learning, but there are also some network security issues. To address these issues, we can strengthen the research and application of security technology, enhance customer awareness of security prevention, implement centralized management of information data, and accelerate the improvement of relevant laws and measures to effectively ensure computer network security in the cloud computing environment.

REFERENCES

[1] Yang, Z., Zhang, W., Lin, X., Zhang, Y., & Li, S. (2023, April). HGMatch: A Match-by-Hyperedge Approach for Subgraph Matching on Hypergraphs. In 2023 IEEE 39th International Conference on Data Engineering (ICDE) (pp. 2063-2076). IEEE.

[2] Ukey, N., Zhang, G., Yang, Z., Li, B., Li, W., & Zhang, W. (2023). Efficient continuous kNN join over dynamic high-dimensional data. World Wide Web, 26(6), 3759-3794.

[3] Yang, X., Zheng, X., & Lu, Q. (2025, October). Construction and early warning of multi-dimensional network credit-related transaction risk maps by integrating graph neural network (GNN). In Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science (pp. 919-923).

[4] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.
[5] Peng, Qucheng, Ce Zheng, Zhengming Ding, Pu Wang, and Chen Chen. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." In 2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG), pp. 1-10. IEEE, 2025.
[6] Wu, J., Luo, L., & Liao, N. (2025). Small-Sample Object Detection of Surface Cracks in Concrete Structures of High-Rise Buildings via Multi-Level Transfer Learning. Innovation & Technology Advances, 3(2), 57–72. https://doi.org/10.61187/ita.v3i2.262
[7] Tang, Yingheng, et al. "Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices." (2020).
[8] Sun, L. (2025, November). Adaptive Interfaces for Personalized User Experience: A Machine Learning Approach. In Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development (pp. 457-462).
[9] Lian, J., & Chen, T. (2024). Research on Complex Data Mining Analysis and Pattern Recognition Based on Deep Learning. Journal of Computing and Electronic Information Management, 12(3), 37-41.
[10] Zheng, H., & Jiang, T. (2025). A New Methodology for Chinese Term Extraction from Scientific Publications. Innovation & Technology Advances, 3(2), 19–45. https://doi.org/10.61187/ita.v3i2.222
[11] Wu, J., Luo, L., & Liao, N. (2025). Small-Sample Object Detection of Surface Cracks in Concrete Structures of High-Rise Buildings via Multi-Level Transfer Learning. Innovation & Technology Advances, 3(2), 57–72. https://doi.org/10.61187/ita.v3i2.262
[12] Y. Ding, Z. Ye, I. Xu, S. Lyu and L. Zhang, "Multi-Scale Adaptive Clustering and Local Consistency Learning for Unsupervised Clothing-Changing Person Re-Identification," in IEEE Transactions on Information Forensics and Security, vol. 21, pp. 2889-2904, 2026, doi: 10.1109/TIFS.2026.3671089.
[13] Ziren, Z. (2026). Dynamic Optimization and Multi-Regional Performance Validation of Automotive Sales Strategies in the United States. Academic Journal of Natural Science, 3(1), 1-7.