Computer Network Security and Maintenance in Cloud Computing Environment

Wenbo Yang[1], Taixiang Guo[2], Peng Wu[3], Ye Zhao[4]

Henan Jinshu Intelligent Technology Co., Ltd. Zhengzhou 450000, Henan

Abstract: ***Although cloud computing technology has brought efficient utilization and flexible configuration of computing resources, the security issues of computer networks in its environment are becoming increasingly prominent. This article deeply analyzes the challenges faced by cloud computing, such as data transmission and storage security risks, insufficient security of cloud service providers, and lack of user security awareness. It proposes comprehensive maintenance strategies including strengthening the security capabilities of cloud service providers, applying data encryption technology, implementing data backup and recovery strategies, strengthening access control and security authentication, and enhancing user security education and training, aiming to build a secure and reliable cloud computing environment.***

Keywords: Cloud computing environment; Computer network; Safety and Maintenance.

1. INTRODUCTION

With the vigorous development of cloud computing technology, it not only provides efficient utilization and flexible allocation of computing resources for enterprises, but also brings new challenges to computer network security. The issues of data transmission and storage, reliability of cloud service providers, and user security awareness and skills in cloud computing environments directly affect the security of data and the continuity of business. Therefore, in-depth exploration of computer network security issues in cloud computing environments and the development of effective maintenance strategies are of great significance for ensuring the stable development of enterprises in the cloud era. Guo (2025) proposed a method for real-time motion recognition by completing Inertial Measurement Unit (IMU) data using Long Short-Term Memory (LSTM) networks [1]. Extending this to robotics, Guo and Tao (2025) conducted modeling and simulation analysis to understand robot-environment interactions [2]. Concurrently, the medical field is leveraging similar data fusion principles, as evidenced by We et al. (2025), who worked towards intelligent monitoring of anesthesia depth through multimodal physiological data [3]. Beyond specific applications, broader societal and systemic factors are also being structurally assessed, such as the influence of family and education on student health behaviors examined by Su et al. (2025) [4], and the optimization of cloud infrastructure reliability via synthetic monitoring researched by Yang (2025) [5]. The modeling of complex user and system behaviors has become increasingly sophisticated. Wang, Dong, and Zhou (2025) applied multimodal temporal modeling and reinforcement learning to analyze and predict user decision-making on short-video platforms [6]. For high-stakes autonomous systems, trust and security are paramount. Tang et al. (2026) developed SVD-BDRL, a blockchain-enhanced framework designed to ensure trustworthy decision-making in autonomous driving [7]. Parallel advances in generative AI are enhancing content creation, with Lu et al. (2025) introducing NeuroDiff3D, a diffusion model optimized for viewpoint-consistent 3D generation [8]. To manage and derive insights from heterogeneous, large-scale data, novel integration frameworks and fusion techniques are critical. Zhang (2025) designed a knowledge graph-enhanced multimodal AI framework specifically for intelligent tax data integration and compliance [9]. Security in distributed networks is addressed by Bi and Su (2025), who proposed a secure access method for education networks based on edge computing [10]. Finally, at the frontier of perception and reconstruction, Xie et al. (2025) developed MARNet, a multi-scale adaptive relational network for robust point cloud completion through cross-modal fusion [11], showcasing the power of integrated sensory data processing.

2. OVERVIEW OF CLOUD COMPUTING

2.1 Definition and Characteristics of Cloud Computing

2.1.1 Concept of Cloud Computing

Cloud computing is an Internet based computing model. It encapsulates computing resources, storage resources and network resources into an independent virtual environment through virtualization technology, and provides

users with on-demand and flexibly configured computing resources and services. This computing model breaks the limitations of fixed allocation and difficult scalability of computing resources in traditional IT architecture, achieving efficient utilization and flexible allocation of computing resources. Users do not need to deploy a large number of hardware devices locally, but only need to connect to the cloud through the Internet to enjoy various computing services, greatly reducing IT costs and improving work efficiency.

2.1.2 Main characteristics of cloud computing

(1) Resource sharing:

One of the biggest features of cloud computing is resource sharing. In the cloud, a large amount of computing resources, storage resources, and network resources are encapsulated into an independent virtual environment, shared by multiple users. This sharing model not only improves resource utilization, but also avoids duplicate construction and resource waste. Users can flexibly allocate resources according to their own needs and achieve on-demand use.

(2) Pay on demand:

Cloud computing adopts a pay as you go billing model, where users only need to pay for the computing resources and services they actually use. This model greatly reduces the initial investment cost of enterprises, allowing them to flexibly adjust IT expenditures according to actual business needs, avoiding the high fixed asset investment in traditional IT architecture.

(3) Elastic expansion and contraction:

Another important feature of cloud computing is its elastic scalability. With the development of business, users' demands for computing resources will constantly change. Cloud computing platforms can automatically adjust the scale of computing resources according to users' actual needs, achieving elastic scaling of resources. This ability enables enterprises to easily cope with the challenges of peak business periods, ensuring business continuity and stability.

(4) High availability:

Cloud computing platforms ensure the security of user data and the availability of services through distributed deployment, data redundancy, and disaster recovery backup technologies. Even if a node or region fails, it can quickly switch to other nodes or regions to ensure the continuous operation of the service.

2.2 Cloud Computing Application Fields

2.2.1 Application examples of cloud computing in enterprise informatization, e-commerce, big data processing and other fields

(1) Enterprise Informatization:

Cloud computing is widely used in the field of enterprise informatization. Many enterprises choose to migrate their core systems such as ERP and CRM to the cloud, achieving centralized management and efficient utilization of resources through cloud computing platforms. In addition, cloud computing provides convenient collaborative office tools for enterprises, such as online meetings, document sharing, etc., which improves employee work efficiency and enterprise competitiveness.

(2) E-commerce:

In the field of e-commerce, cloud computing provides strong support for e-commerce platforms. Through cloud computing platforms, e-commerce platforms can easily meet the needs of large-scale concurrent access and high data processing, ensuring smooth transactions. At the same time, cloud computing also provides intelligent data analysis services for e-commerce enterprises, helping them to deeply explore user behavior data, optimize marketing strategies, and enhance user experience.

(3) Big data processing:

Big data processing is another important application area of cloud computing. Cloud computing platforms provide powerful data storage and computing capabilities, enabling enterprises to easily handle massive amounts of data. Through cloud computing platforms, enterprises can conduct complex data analysis and mining work, discover potential market opportunities and business value. In addition, cloud computing provides convenient data visualization tools for enterprises, helping them transform complex data into intuitive and understandable charts and reports.

2.2.2 Convenience and benefits brought by cloud computing technology

The introduction of cloud computing technology has brought many conveniences and benefits to enterprises. Firstly, cloud computing reduces the IT costs of enterprises, allowing them to invest more funds into their core businesses. Secondly, cloud computing has improved the work efficiency and competitiveness of enterprises, by providing convenient collaborative office tools and intelligent data analysis services, helping enterprises achieve optimization of business processes and intelligent decision-making. Finally, cloud computing also enhances the service quality and user experience of enterprises by providing high availability and scalable service guarantees, ensuring that users can enjoy efficient and stable services anytime and anywhere.

3. CHALLENGES FACED BY COMPUTER NETWORK SECURITY IN CLOUD COMPUTING ENVIRONMENT

3.1 Data transmission and storage security risks

3.1.1 Security Threat Analysis

In the vast blue ocean of cloud computing, the transmission and storage of user data are like two oars sailing, driving the operation of services, but also exposed to wind and rain. During data transmission, data is like sailing in open waters, facing various threats. Hackers use complex and varied attack methods, such as phishing, data eavesdropping, man in the middle attacks, etc., to attempt to intercept or tamper with transmitted data. At the same time, malicious software is like a reef in the ocean, lurking everywhere on the network, waiting for the opportunity to infect user devices or cloud service systems, and then steal or destroy data. The data storage process is also full of challenges. Although cloud service providers' data centers have advanced protection technologies, they may also be exposed to risks due to system vulnerabilities, configuration errors, or human negligence. Unencrypted or improperly encrypted sensitive data is like an unlocked treasure chest, easily accessible to criminals. In addition, permission management for data storage is also a major challenge. If permission settings are unreasonable or supervision is inadequate, it will directly lead to illegal access or abuse of data.

3.1.2 Severity of Data Leakage and Illegal Access

The severity of data breaches and illegal access is like a tsunami, which can cause incalculable losses to individuals, businesses, and countries. The leakage of personal data may lead to consequences such as identity theft, property damage, and reputation damage, seriously affecting an individual's quality of life and social trust. The leakage of enterprise data may involve sensitive information such as trade secrets and customer data, leading to a decline in competitiveness, severe economic losses, and even legal disputes and trust crises. More seriously, when government or critical infrastructure data is illegally accessed or tampered with, it may pose significant issues to national security and social stability.

3.2 Security Issues of Cloud Service Providers

As the cornerstone of cloud computing, cloud service providers' security protection capabilities and policy execution are crucial. However, in reality, some cloud service providers have shortcomings in terms of security.

Firstly, the insufficient security protection capability may result in its inability to effectively resist external attacks, such as failure to update security patches in a timely manner, lack of advanced threat detection capabilities, etc.

Secondly, lax implementation of security policies may also bring risks, such as chaotic permission management, insufficient log auditing, and inadequate emergency response mechanisms. These shortcomings not only threaten the security of user data, but may also damage the reputation and market share of cloud service providers.

3.3 Insufficient user security awareness and skills

In the wave of cloud computing, users are both beneficiaries and participants. However, many users neglect their security responsibilities when using cloud computing services. Users with weak security awareness may randomly click on links of unknown origin, download unverified attachments, use weak passwords, etc., all of which provide opportunities for hackers to take advantage of. Meanwhile, users with insufficient skills may not be able to correctly configure the security settings of cloud services and identify potential security risks, thereby increasing the risk of data breaches and unauthorized access. Therefore, improving users' security awareness and skill level is one of the important measures to ensure the security of cloud computing environments.

4. NETWORK SECURITY MAINTENANCE STRATEGIES IN CLOUD COMPUTING ENVIRONMENTS

4.1 Strengthen the security capabilities of cloud service providers

4.1.1 Encourage cloud service providers to strengthen their security system construction

As the cornerstone of cloud computing services, the security capabilities of cloud service providers directly affect the security of user data. Therefore, encouraging cloud service providers to strengthen their security system construction is the top priority. This includes but is not limited to establishing strict security policies and processes, forming professional security teams, introducing advanced security technologies and management tools, etc. By building a comprehensive and in-depth security system, cloud service providers can effectively resist external attacks, ensuring the confidentiality, integrity, and availability of user data. In practical implementation, cloud service providers can refer to international security standards such as ISO27001, SOC2, etc. to build and improve their own security systems. At the same time, we should actively participate in security exchanges and cooperation within the industry, and continuously improve our own security protection capabilities.

4.1.2 Require cloud service providers to conduct regular security audits and vulnerability scans

Security auditing and vulnerability scanning are important means of discovering and fixing security vulnerabilities. Cloud service providers should regularly conduct comprehensive security audits and vulnerability scans to ensure timely detection and repair of security vulnerabilities and weaknesses in the system. In addition, cloud service providers should establish a rapid response mechanism to quickly take measures to address and repair security issues discovered. To ensure the effectiveness of security audits and vulnerability scans, cloud service providers can invite third-party professional organizations to conduct independent security assessments. These institutions usually have rich experience in security assessment and professional technical strength, which can objectively evaluate the security level of cloud service providers and provide improvement suggestions.

4.2 Adopting data encryption technology

4.2.1 Basic Principles of Data Encryption Technology and Its Application in Cloud Computing Environment

Data encryption technology is a technical means of converting plaintext into ciphertext through specific algorithms to protect data confidentiality. The application of data encryption technology is particularly critical in cloud computing environments. By encrypting user data and uploading it to the cloud for storage or transmission, it can effectively prevent data from being intercepted during transmission or illegally accessed during storage. Common data encryption techniques include symmetric encryption and asymmetric encryption. Symmetric encryption algorithm uses the same key for encryption and decryption operations, which has high encryption efficiency and low computational cost; Asymmetric encryption algorithms use a pair of public and private keys for encryption and decryption operations, which have higher security and flexibility. In cloud computing environments, appropriate data encryption techniques can be selected based on specific application scenarios and requirements to achieve data protection [3].

4.2.2 The Importance of Using Encryption Techniques in Data Transmission and Storage Processes

In the cloud computing environment, user data faces many security risks during transmission and storage. Therefore, the use of encryption technology in data transmission and storage processes is particularly important. By using encryption technology, it is possible to ensure that data is not intercepted or tampered with during transmission, while also effectively preventing unauthorized access and data leakage risks during storage. To ensure the security of data transmission and storage, cloud service providers should provide end-to-end data encryption services. This includes using encryption protocols such as SSL/TLS to encrypt data during transmission, as well as using transparent data encryption (TDE) or other advanced encryption techniques during data storage to ensure the security of data on cloud storage media. In addition, cloud service providers should also provide Key Management Services (KMS), allowing users to have full control over their encryption keys. This means that users can store their keys in their own systems and only send encrypted data to the cloud for processing or analysis when necessary, ensuring that even the cloud service provider itself cannot decrypt user data, further enhancing data security.

4.3 Implement data backup and recovery strategies

4.3.1 Develop a comprehensive data backup and recovery plan

Data backup and recovery are important measures to ensure business continuity and data reliability. In the cloud computing environment, due to the centralized storage of data on cloud servers, once data loss or damage occurs, it will cause significant losses to the enterprise. Therefore, it is crucial to develop a comprehensive data backup and recovery plan. The plan should specify key elements such as backup frequency, scope, selection of backup media, and recovery strategies and processes. At the same time, it is necessary to consider the accessibility, recoverability, and verifiability of backup data to ensure that data can be quickly restored when needed.

4.3.2 Emphasize the diversity and remote nature of data backup

In order to improve the reliability and security of data, emphasis should be placed on the diversity and remote nature of data backup. Diversity means using multiple different backup methods and media to store backup data, in order to reduce the risk of single point of failure. For example, backup data can be stored on various media such as local disks, tape libraries, cloud storage, etc. to ensure data redundancy and recoverability. Remote location refers to storing backup data in a geographical location far from the original data center to cope with the impact of natural disasters, human destruction, and other emergencies. By backing up remotely, it is possible to ensure that backup data remains available in the event of a disaster, thereby ensuring business continuity.

4.4 Strengthen user security education and training

4.4.1 Enhance users' security awareness

Users are the first line of defense for network security. Improving users' security awareness is one of the important means to prevent network security risks. Cloud service providers and user organizations should regularly conduct network security education activities to popularize key information such as network security knowledge, network fraud methods, and prevention measures to users. By educating users to identify common security risks such as phishing emails and malicious software, and teaching them how to take corresponding preventive measures, the risk of users being attacked can be reduced.

4.4.2 Train users on the correct use of cloud computing services

In addition to raising users' awareness of security, it is also necessary to train them on the proper use of cloud computing services. Due to the complexity and diversity of cloud computing services, users may encounter various security issues during their use. Therefore, cloud service providers and user organizations should provide detailed operation guidelines and training courses to help users understand the functions and features of cloud computing services, master the correct usage methods and security operation norms. By training users on the proper use of cloud computing services, it is possible to avoid security issues caused by improper operations and improve the security of the entire cloud environment.

5. CONCLUSION

In summary, computer network security and maintenance in cloud computing environments is a complex and systematic project that requires joint efforts from cloud service providers, enterprises, and users. By strengthening the research and application of security technology, enhancing security management and institutional construction, and improving user security awareness and skills, we can effectively address the security risks brought by cloud computing and build a secure, reliable, and efficient cloud computing ecosystem. In the future, with the continuous advancement of technology and the deepening of applications, cloud computing network security will face more new challenges. We need to remain vigilant, continue to innovate, and safeguard the healthy development of cloud computing.

REFERENCES

[1] Guo, Y. (2025, May). IMUs Based Real-Time Data Completion for Motion Recognition With LSTM. In Forum on Research and Innovation Management (Vol. 3, No. 6).
[2] Guo, Y., & Tao, D. (2025). Modeling and Simulation Analysis of Robot Environmental Interaction. Artificial Intelligence Technology Research, 2(8).
[3] We, X., Lin, S., Pruś, K., Zhu, X., Jia, X., & Du, R. (2025). Towards Intelligent Monitoring of Anesthesia Depth by Leveraging Multimodal Physiological Data. International Journal of Advance in Clinical Science Research, 4, 26–37. Retrieved from https://www.h-tsp.com/index.php/ijacsr/article/view/158
[4] Su, Z., Yang, D., Wang, C., Xiao, Z., & Cai, S. (2025). Structural assessment of family and educational influences on student health behaviours: Insights from a public health perspective. Plos one, 20(9), e0333086.
[5] Yang, Y. (2025). Research on Site Reliability Optimization Technology Based on Synthetic Monitoring in Cloud Environments.
[6] Wang, J., Dong, J., & Zhou, L. (2025). Research on Short-Video Platform User Decision-Making via Multimodal Temporal Modeling and Reinforcement Learning: Deep Learning for User Decision Behavior. Journal of Organizational and End User Computing (JOEUC), 37(1), 1-24.
[7] Tang, Z., Feng, Y., Zhang, J., & Wang, Z. (2026). SVD-BDRL: A trustworthy autonomous driving decision framework based on sparse voxels and blockchain enhancement. Alexandria Engineering Journal, 134, 433-446.
[8] Lu, K., Sui, Q., Chen, X., & Wang, Z. (2025). NeuroDiff3D: a 3D generation method optimizing viewpoint consistency through diffusion modeling. Scientific Reports, 15(1), 41084.
[9] Zhang, T. (2025). A Knowledge Graph-Enhanced Multimodal AI Framework for Intelligent Tax Data Integration and Compliance Enhancement. Frontiers in Business and Finance, 2(02), 247-261.
[10] Bi, Y., & Su, T. (2025). A secure access method in English education network based on edge computing. Alexandria Engineering Journal, 128, 1125-1133.
[11] Xie, J., Zhang, L., Cheng, L., Yao, J., Qian, P., Zhu, B., & Liu, G. (2025). MARNet: Multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion. Information Fusion, 103505.