Exploration of Security Vulnerability Mining and Protection Technologies for Cloud Computing Platforms

Guo Qingtao[1], Zhang Juyi[2]

Hebei Fangwei Network Technology Co., Ltd. Shijiazhuang, Hebei 050000

Abstract: ***Cloud computing platforms are a crucial part of modern information technology, and the security of cloud computing platforms is increasingly receiving widespread attention. The article aims to explore security vulnerability mining and protection technologies for cloud computing platforms, in order to promote their safe and stable operation. Firstly, research and summarize the basic concepts of cloud computing platforms, security challenges, and security vulnerability classification, and propose relevant security protection strategies. Then, a deep analysis of the significance of security vulnerability mining is conducted, introducing the methods and tools of vulnerability mining, discussing the process and practices of vulnerability mining, and providing countermeasures for the challenges faced in the mining process. In addition, the paper systematically discusses the key technologies, implementation strategies, and effectiveness evaluation methods for cloud computing platform security protection. The conclusion drawn from this study is that strengthening the mining and protection of security vulnerabilities in cloud computing platforms is the key to ensuring the safe and smooth operation of the platform, and can also provide useful references for research and practice in related fields.***

Keywords: Cloud computing platform; Security vulnerabilities; Vulnerability mining; Security protection; Technical exploration.

1. INTRODUCTION

Cloud computing is an important branch of modern information technology, and its advantages in data storage, processing, and analysis are gradually becoming a key driving force in the process of social and economic development. However, while cloud computing services are widely used, their security issues are increasingly becoming a hot topic of research in the industry. The mining and protection technology of security vulnerabilities in cloud computing platforms not only concerns data security and privacy protection issues, but also ensures the sustainable development of cloud computing services. At present, although some progress has been made in the research of cloud computing platform security, there are still many shortcomings and research gaps in the identification, evaluation, and protection strategies of security vulnerabilities.

To solve the problem of security vulnerability mining and protection technology in cloud computing platforms, machine learning and artificial intelligence are proposed. By establishing a security vulnerability feature library and using machine learning algorithms for cloud computing platform behavior analysis and modeling, potential security vulnerabilities can be quickly discovered and alerted. At the same time, combining artificial intelligence technology to evaluate the impact range and degree of harm of security vulnerabilities, and providing decision support for the formulation of relevant protection strategies. In addition, this study also delved into various security measures for cloud computing platforms, such as access control, data encryption, and intrusion detection, with the aim of establishing a comprehensive security protection system.

2. OVERVIEW OF CLOUD COMPUTING PLATFORM SECURITY

Recent research has demonstrated significant advancements in modeling robot-environment interactions [1] and in developing intelligent monitoring systems using multimodal physiological data [2]. Concurrently, studies have applied computational analysis from a public health perspective to understand influential factors on student behavior [3], while other work focuses on optimizing the reliability of cloud infrastructure through synthetic monitoring [4]. The pursuit of trustworthy autonomous systems is evident in the development of blockchain-enhanced decision frameworks for self-driving cars [5]. In the realm of industrial maintenance, highly reliable fault diagnosis models utilizing densely connected convolutional networks and transfer learning have been proposed [6]. The impact of digital transformation is being examined across various sectors, including the evolutionary logic of marketing strategies in real estate [7]. The application of artificial intelligence continues to

diversify, with innovations in medical consultation through advanced identification models [8], optimization of parallelism methods for large language model-based recommendation systems [9], and AI-driven sales forecasting in the gaming industry [10]. Algorithmic optimization remains a key research area, spanning from SEO strategies using graph algorithms for website structure [11] to text-to-3D modeling for accelerating urban architectural planning [12]. Furthermore, specialized intelligent systems are being developed for personalized medical plan generation [13] and for cross-media data fusion and analytics [14]. Foundational computer vision research on object referring with integrated gaze estimation [15] supports these advanced applications. Finally, research into dynamic resource adaptation, such as optimizing the supply and demand of emergency materials using clustering techniques, highlights the role of AI in logistics and crisis management [16].

2.1 Basic Concepts of Cloud Computing Platforms

In the cloud computing platform, relying on the Internet, it provides on-demand computing resources and services, with the basic characteristics of resource virtualization, business scalability, access universality, management centralization, etc. Cloud computing platforms use virtualization technology to abstract physical resources into dynamically distributable virtual resources, allowing users to obtain the computing power, storage space, and application programs they need at any time according to their actual needs. At the same time, the cloud computing platform is a distributed architecture with strong computing and storage capabilities, which can support large-scale user access and data processing. In addition, cloud computing platforms adopt a centralized management approach to uniformly schedule and optimize resource configuration, thereby improving resource utilization and service quality. However, the openness and complexity of cloud computing platforms have also raised many security risks and challenges, which requires us to conduct in-depth research and exploration on relevant security protection technologies and strategies.

2.2 Security Challenges of Cloud Computing Platforms

The new computing model of cloud computing has core advantages such as flexible resource allocation, service scalability, and cost-effectiveness [1]. However, while cloud computing platforms are widely used, security issues have gradually become a bottleneck hindering their development. Cloud computing platforms face the following major security challenges:

2.2.1 Data Security

Cloud computing platforms need to process and store massive amounts of user data, which may contain sensitive information. Data leakage, data tampering, and data abuse seriously affect users' trust in cloud computing platforms. In addition, ownership and control of data is also an important issue that cloud computing platforms urgently need to address;

2.2.2 Network Security Issues

Cloud computing platforms generally use virtualization technology for resource sharing and separation. However, virtualization technology itself has security vulnerabilities, such as virtual machine escape attacks and information leakage between virtual machines. In addition, the network architecture of cloud computing platforms is relatively complex, and network attack methods are constantly being updated, which poses significant challenges to network security;

2.2.3 Identity authentication and access control

Cloud computing platforms require user authentication to provide corresponding services based on their identity and permissions. However, the identity authentication mechanism can also have vulnerabilities, such as password cracking and session hijacking. Access control policies also face challenges in the design and implementation process, and must balance security and usability; Fourthly, in terms of laws, regulations, and standards. The rapid development of cloud computing platforms poses challenges to current laws, regulations, and standards. How to establish reasonable regulations and standards from the perspective of protecting user privacy, data security, and intellectual property is a challenge that cloud computing platforms need to face.

2.3 Classification of Security Vulnerabilities in Cloud Computing Platforms

Cloud computing platform security vulnerabilities can be classified according to their sources and scope of impact. Here are some commonly used classification methods:

2.3.1 Security vulnerabilities can be classified into internal vulnerabilities and external vulnerabilities based on their sources

Internal vulnerabilities are generally caused by design flaws, incorrect configuration, or chaotic management of cloud computing platforms, such as virtualization vulnerabilities, incorrect permission allocation, and so on. External security vulnerabilities are usually exploited by external attackers who exploit weak links in cloud computing platforms, such as network attacks or malicious software, to carry out attacks.

2.3.2 Security vulnerabilities can be divided into local vulnerabilities and global vulnerabilities based on their impact scope

Local vulnerabilities generally only affect a certain part or service in the cloud computing platform, such as individual virtual machines or a specific application. Global security vulnerabilities may have an impact on the entire cloud computing platform, including but not limited to deficiencies in network architecture and vulnerabilities in authentication systems;
2.3.3 Security vulnerabilities can be classified into software vulnerabilities, hardware vulnerabilities, and human made vulnerabilities based on their types

Software vulnerabilities are generally caused by programming errors and improper configuration, such as buffer overflow and insufficient input validation. Hardware defects are mainly caused by design flaws or quality issues during the manufacturing process, such as side channel attacks and backdoor operations in hardware. Human made security vulnerabilities are often caused by operational errors, management oversights, and other human factors, such as password leaks or abuse of permissions.

2.3.4 Security vulnerabilities can be classified into known vulnerabilities and unknown vulnerabilities based on the ways in which they were discovered and exploited

Known vulnerabilities refer to those that can be patched and configured after being detected and disclosed by security researchers. Unknown security vulnerabilities that have not yet been identified or made public may become a means for attackers to carry out covert attacks.

3. CLOUD COMPUTING PLATFORM SECURITY VULNERABILITY MINING TECHNOLOGY

3.1 Importance of Security Vulnerability Mining

Security vulnerability mining plays a fundamental role in the field of network security. It refers to actively detecting and verifying whether software or systems have security vulnerabilities through various technical means. Due to the wide range and complexity of services in cloud computing platforms, vulnerability mining is extremely important. On the one hand, by mining vulnerabilities, potential security issues can be discovered and fixed in a timely manner to avoid data leaks and malicious attacks on the system; On the other hand, vulnerability mining helps to improve the security and reliability of cloud computing platforms, and enhance users' trust in cloud services [2].

3.2 Methods and Tools for Vulnerability Mining

There are many methods for vulnerability mining, including static analysis, dynamic analysis, and fuzzy testing. Static analysis identifies potential security vulnerabilities by examining source code or binary files. This method has the advantages of not requiring program execution, being able to quickly detect problems, but may result in false alarms, missed alarms, and other issues. Dynamic analysis is a method of continuous monitoring during program execution, aimed at identifying abnormal behavior patterns by tracking the program's trajectory. Fuzzy testing is a method of observing program reactions by inputting a large amount of random or abnormal data into the program, with the aim of identifying potential security vulnerabilities.

Using multiple tools during vulnerability mining can significantly improve mining efficiency and accuracy. For example, source code analysis tools can help developers conduct security checks on their code; Binary analysis tools can parse compiled programs; Network scanning tools can detect whether there are security vulnerabilities in the network. In addition, some automated vulnerability detection tools, such as fuzz testing tools, can automatically generate test cases, thereby improving the efficiency of data mining.

The process of vulnerability mining is complex and requires the comprehensive use of various technologies and methods. Due to the large scale and complex structure of cloud computing platforms, vulnerability mining has become extremely difficult. Therefore, choosing appropriate mining methods and tools and combining them with the characteristics of cloud computing platforms to carry out targeted mining is the key to improving mining effectiveness.

3.3 Process and Practice of Vulnerability Mining

Cloud computing platform vulnerability mining is a systematic engineering process from vulnerability discovery, analysis, reporting to patching. Firstly, it is necessary to have a deep understanding of the architecture and components of cloud computing platforms, and identify potential security vulnerabilities [3]. Then, by combining automated tools with manual analysis, the system achieved comprehensive scanning and detection. Once a suspicious point is found, it is necessary to conduct a thorough analysis to confirm whether it really has a vulnerability. After confirming the existence of vulnerabilities, it is necessary to prepare a detailed vulnerability report, which should include various types of vulnerabilities, their scope of impact, and how to exploit these vulnerabilities, and report this information to the cloud platform provider. Finally, the cloud platform provider needs to develop a repair plan and execution plan based on the reported content to eliminate security risks.

In practice, the process of vulnerability mining requires continuous optimization and adjustment to meet the needs of the rapid development and transformation of cloud computing platforms. For example, in the evolution of cloud computing technology, various new types of vulnerabilities and attack methods emerge one after another, requiring vulnerability miners to constantly learn new knowledge and skills in order to improve mining efficiency and accuracy.

3.4 Challenges and Countermeasures of Vulnerability Mining

Cloud computing platforms have encountered challenges from various aspects in the process of vulnerability mining. One reason is that cloud computing platforms are complex and highly dynamic, making vulnerability mining more difficult. Cloud platforms are generally composed of several layers and components, each of which may have security vulnerabilities, and as the scale of cloud services expands and updates, new vulnerabilities will continue to emerge. Secondly, cloud computing platforms have characteristics such as openness and sharing, which also increase the difficulty of vulnerability mining. The users of cloud services come from different regions and industries, and their behaviors and needs are also different. It requires vulnerability miners to have richer knowledge and experience when facing various complex scenarios.

To solve these problems, vulnerability miners must take a series of measures. Firstly, it is necessary to enhance understanding of the architecture and components of cloud computing platforms, grasp the working principles and security features of the platform, in order to more accurately discover vulnerabilities and locate them. Secondly, advanced vulnerability mining tools and technologies need to be utilized to enhance the automation and intelligence of vulnerability mining, reducing the time and effort required for manual analysis.

3.5 Future Development Trends of Security Vulnerability Mining

Against the backdrop of the increasing development and application of cloud computing technology, several new trends have emerged in security vulnerability mining [4].

3.5.1 Automated and intelligent vulnerability mining tools will receive more attention

With the continuous development of artificial intelligence and machine learning technologies, automated tools can detect and analyze vulnerabilities more quickly and accurately, greatly improving the efficiency of vulnerability mining.

3.5.2 Cloud computing platform vulnerability mining will pay more attention to combining with security protection measures

By monitoring and analyzing the real-time operation status of the cloud platform, identifying and responding to security threats in a timely manner, a dynamic and continuous security protection mechanism is formed.

In addition, vulnerability mining in cloud computing platforms will place greater emphasis on interdisciplinary and cross domain collaboration. Cloud computing covers many fields such as computer science, network technology, and information security. Vulnerability mining requires the integration of knowledge and technology in these areas to form comprehensive solutions.

4. CLOUD COMPUTING PLATFORM SECURITY PROTECTION TECHNOLOGY

4.1 Basic principles of safety protection

The fundamental principle of security protection is to establish a comprehensive multi-level security system to ensure the security and reliability of cloud computing platforms.
One is to establish the principle of prioritizing security. Security is the key, and it requires consideration and strict implementation of security measures in every aspect from design, development, deployment to operation and maintenance [5].

The second is to follow the principle of minimum permission and constrain users' access to resources required for task execution through accurate control of user permissions, effectively reducing the risks of permission abuse and security breaches.

In addition, regularly conducting security audits and risk assessments, as well as comprehensive inspections of the system, helps us to promptly identify potential security vulnerabilities and threats, and take timely maintenance and improvement measures.

4.2 Key Technologies for Security Protection

Key technologies provide a basis for ensuring information security, involving many fields such as identity authentication, access control, data encryption, intrusion detection and defense, and security auditing. Identity verification technology utilizes various verification methods, such as passwords and biometric technology, to ensure that system resources are only accessible to legitimate users. Access control technology is based on roles or attributes, which meticulously manages user access to resources to prevent unauthorized access and potential data leakage. Data encryption technology encodes information during data transmission and storage to ensure data confidentiality and integrity, avoiding illegal interception and interpretation of sensitive information.

Intrusion detection and defense technologies have been deployed in networks and systems, which can effectively identify and prevent malicious attacks through real-time traffic monitoring and analysis, thereby protecting the system from damage. The technical means of security auditing is to provide solid data support for the tracking, research, and evidence collection of security incidents by detailed recording of user behavior and events in the system.

4.3 Implementation strategy for security protection

The implementation strategy mainly focuses on physical security, network security, application security, and data security. The physical security strategy mainly includes data center physical access control and environmental monitoring; The network security strategy covers firewalls, intrusion prevention systems, and other network boundary protection measures; The application security strategy mainly includes application security coding, vulnerability scanning, and repair; The data security strategy mainly focuses on data encryption, backup, and recovery. In addition, an emergency response mechanism should be established and a thorough security incident

handling process should be developed to ensure that once a security incident occurs, it can be quickly and effectively handled.

5. CONCLUSION

The article provides an in-depth analysis of security vulnerability mining and protection technologies for cloud computing platforms, revealing the challenges and opportunities faced in the field of cloud computing security. Domestic and foreign scholars widely believe that cloud computing platform security is a complex system with multiple dimensions and levels, which requires the comprehensive use of technology, management, and legal measures from multiple perspectives.

The research conclusion shows that mining security vulnerabilities in cloud computing platforms is a key part of security threat detection and prevention, and efficient security protection technologies are the cornerstone of ensuring the smooth operation of the platform. By reviewing existing security vulnerability mining methods and discussing them in conjunction with security protection technologies, a series of targeted strategies and technical measures aimed at improving the security and reliability of cloud computing platforms have been proposed.

REFERENCES

[1] Guo, Y., & Tao, D. (2025). Modeling and Simulation Analysis of Robot Environmental Interaction. Artificial Intelligence Technology Research, 2(8).
[2] 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
[3] 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.
[4] Yang, Y. (2025). Research on Site Reliability Optimization Technology Based on Synthetic Monitoring in Cloud Environments.
[5] 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.
[6] Tan, C., Gao, F., Song, C., Xu, M., Li, Y., & Ma, H. (2024). Highly Reliable CI-JSO based Densely Connected Convolutional Networks Using Transfer Learning for Fault Diagnosis.
[7] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.
[8] Yang, J. (2025, July). Identification Based on Prompt-Biomrc Model and Its Application in Intelligent Consultation. In Innovative Computing 2025, Volume 1: International Conference on Innovative Computing (Vol. 1440, p. 149). Springer Nature.
[9] Yang, Haowei, Yu Tian, Zhongheng Yang, Zhao Wang, Chengrui Zhou, and Dannier Li. "Research on Model Parallelism and Data Parallelism Optimization Methods in Large Language Model-Based Recommendation Systems." arXiv preprint arXiv:2506.17551 (2025).
[10] Zhang, Jingbo, et al. "AI-Driven Sales Forecasting in the Gaming Industry: Machine Learning-Based Advertising Market Trend Analysis and Key Feature Mining." (2025).
[11] Yang, Yifan. "Website Internal Link Optimization Strategy and SEO Effect Evaluation Based on Dijkstra Algorithm." Journal of Computer, Signal, and System Research 2.3 (2025): 90-96.
[12] Xu, Haoran. "UrbanMod: Text-to-3D Modeling for Accelerated City Architecture Planning." Authorea Preprints (2025).
[13] Hsu, Hsin-Ling, et al. "MEDPLAN: A Two-Stage RAG-Based System for Personalized Medical Plan Generation." arXiv preprint arXiv:2503.17900 (2025).
[14] Yuan, Yuping, and Haozhong Xue. "Cross-Media Data Fusion and Intelligent Analytics Framework for Comprehensive Information Extraction and Value Mining." (2025).
[15] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[16] Zhang, X. (2024). Research on Dynamic Adaptation of Supply and Demand of Power Emergency Materials based on Cohesive Hierarchical Clustering. Innovation & Technology Advances, 2(2), 59–75. https://doi.org/10.61187/ita.v2i2.135