Exploring Security Risks of Cloud Services in Enterprises

Zuli Zhao, Binhui Tang

School of Computer and Software, Jincheng College of Sichuan University, Chengdu 611731, Sichuan, China

Abstract: ***SaaS cloud services have become deeply embedded in enterprise application environments. This paper first outlines the basic concepts of SaaS services, analyzes the various security risks faced by client enterprises during their use of SaaS services, and proposes several factors influencing these security risks, aiming to raise security awareness while enterprises adopt cloud services.***

Keywords: Cloud computing; Security risk; SaaS cloud service.

1. OVERVIEW OF SAAS SERVICE SYSTEMS

SaaS: Software-as-a-Service, a new software application model based on the Internet. Providers deliver applications running on cloud computing infrastructure to client enterprises, which can access them via client interfaces on various devices. Enterprises can obtain customized software services according to their actual needs and pay on demand. Compared with traditional software purchases, this saves substantial upfront costs for acquisition or development. By renting web-based software from providers, enterprises avoid back-end maintenance, saving significant human resources and costs, allowing them to focus on core business and improve operational efficiency.

Service providers integrate vast computer hardware and software resources, delivering business services over the Internet. The SaaS model uses a multi-tenant architecture with virtualization technology to allocate appropriate hardware and software resources to each tenant. Providers can continuously update infrastructure configurations, making it easier for back-end staff to solve problems and maintain equipment, while also reducing client enterprises' software upgrade costs. Wang and Shih (2024) proposed a hybrid recommendation system integrating MMoE and XGBoost for enhanced personalization [1], while Fu et al. (2025) developed adversarial prompt optimization techniques to address LLM vulnerabilities [2]. Zheng et al. (2025) introduced FinGPT-Agent for adaptive financial report generation [3], complemented by Weng et al. (2025)'s SafeGen-X framework strengthening LLM security and compliance [4]. For multimodal models, Chen et al. (2025) presented SyntheClean for adaptive data synthesis [5]. Domain-specific QA systems advanced through Jiang et al. (2025)'s knowledge-enhanced multi-task model [6] and Zhuo et al. (2025)'s transformer with domain adaptation [7]. Generative capabilities expanded via Zhang et al. (2025)'s attention-guided video synthesis [8] and Zhao et al. (2025)'s KET-GPT for knowledge updating [9]. Dialogue systems benefited from Shih et al. (2025)'s dual-stage transformer [10], while multimodal fusion advanced with Li et al. (2025)'s MLIF-Net combining ViTs and LLMs [11]. Visualization tools progressed through Xie and Chen (2025)'s InVis [12] and CoreViz [13] systems, with Zhu (2025) introducing TraceLM for temporal analysis [14]. Deployment safety was addressed by Zhang (2025)'s CrossPlatformStack [15] and SafeServe [16], while ad creation leveraged Hu (2025)'s AdPercept [17] and UnrealAdBlend [18]. Healthcare innovations included Ding and Wu (2024)'s self-supervised biosignal review [19] and Restrepo et al. (2024)'s multimodal approach for low-resource settings [20]. Financial AI advanced with Jiang et al. (2025)'s Investment Advisory Robotics 2.0 [21], while medical imaging built upon Chen et al. (2023)'s text-guided segmentation [22]. NLP developments featured Yu et al. (2025)'s transformer-based summarization [23] and Sun et al. (2025)'s LLM-powered AutoML framework [24], concluding with Pal et al. (2025)'s AI-driven credit risk assessment [25].

From a technical perspective, as API calls increase, cross-layer applications are becoming more common. For example, in statistical tools, the SDK portion is completed at the PaaS layer, while all subsequent report viewing and analysis are done on the web side (SaaS layer). The SaaS layer in the cloud computing hierarchy is shown in the figure:

Figure 1: Cloud Computing Hierarchy Diagram

1.1 Characteristics of SaaS Services

1.1.1 On-demand provisioning: In the SaaS model, users can "tailor" services to their needs, giving the software service greater flexibility; SaaS vendors can recombine the various modules of the software application according to customer requirements to create a personalized software service.

1.1.2 Multi-tenant architecture: The multi-tenant architecture of the SaaS model allows SaaS vendors to design a standardized software system at relatively low development cost and provide it to thousands of users, thereby achieving economies of scale in software services [2].

1.1.3 Network characteristics: SaaS services are delivered to customers via network transmission, and many network-technology features are evident in SaaS services. Client enterprises can interact with the server over the network through a web browser or a dedicated client platform; most data processing operations are still handled on the server side, and only the required results are transmitted back to the client over the network.

1.1.4 Programmability: SaaS vendors can use APIs to create and modify cloud computing resources, and can also program cloud resources with code tools such as AWS CloudFormation. Automated management through programming enables faster detection and correction of configuration errors and deviations than traditional data centers, improves rapid self-healing capabilities, and protects important and sensitive data.

2. ANALYSIS OF SECURITY RISKS FACED BY ENTERPRISES

2.1 Sources of Security Risk

2.1.1 Hackers: Typically use specialized computer and network technologies to attack target computers or servers and steal data of high economic value to the enterprise. Threats from hackers to SaaS services often occur during data transmission over the wide-area network.

2.1.2 Computer viruses: Viruses are a major hidden danger in cloud computing environments; once an operator or enterprise is infected, system performance can degrade and the entire system may even be paralyzed. Examples include worm viruses, Trojan horses, script viruses, and so on.

2.1.3 Insiders: Insiders possess partial data-management privileges; a small number of employees may exploit their positions to steal data for economic gain, and insider risk is one of the hardest factors to control.

2.1.4 Physical disasters: Physical threats to computers include man-made physical disasters, natural disasters, environmental accidents, and human error. Some natural disasters such as fires, rodent damage, lightning strikes, and earthquakes are usually unavoidable risks.

2.2 Security Risk Factors

2.2.1 Data Risk

Data is extremely important to enterprises; it plays a vital role. Once a company's data is damaged, it will cause immeasurable losses. If the service provider fails to take timely remedial measures to restore the data, the customer

enterprise is highly likely to face the risk of being eliminated by the market. Therefore, ensuring data security in cybersecurity is a critical issue for SaaS services.

2.2.2 Data Lock-in Risk

Because enterprises do not have full control over their data, they face the risk of data being locked due to hackers, market competition, and other factors. In January 2017, MongoDB experienced a database ransomware incident in which more than 33,000 databases were illegally breached. The data was plundered by hackers, who left ransom notes demanding Bitcoin payments to recover the data.

2.2.3 Unauthorized Use of Data

Data is crucial to enterprises, containing vital information such as financial, managerial, and product data, as well as highly valuable customer information. Under the SaaS model, the physical storage medium resides with the service provider, and enterprises cannot fully control the functions of that medium. Consequently, enterprises worry that their core data may be used without authorization by the provider.

2.2.4 Data Transmission Risk

In the SaaS model, data is stored and exchanged via network transmission. During this process, it is frequently subjected to illegal network attacks. With the continuous development of networks, attack incidents have become common, such as DDoS, ICMP flood attacks, TCP/UDP flood attacks, and ARP attacks. These all represent illegal intrusions during data transmission. For example, attackers send forged ARP packets to maliciously modify the ARP entries of gateways or other hosts in the network, causing abnormal packet forwarding for users or the network. The figure below illustrates the ARP spoofing attack process:

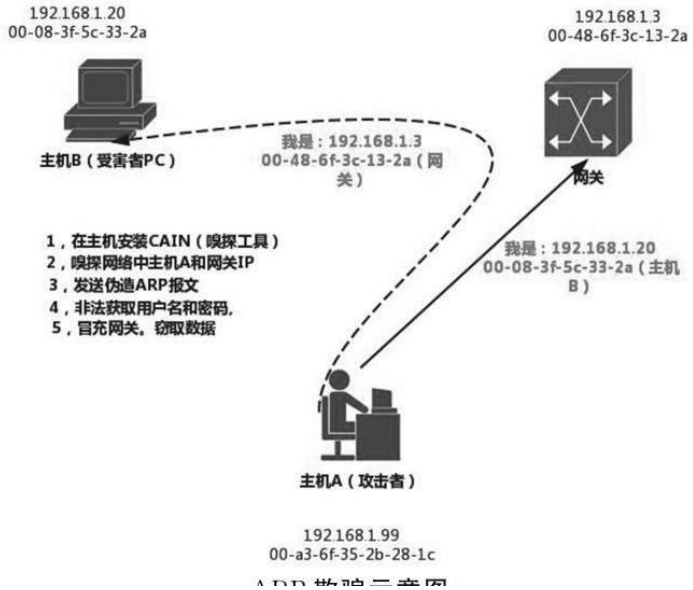


Figure 2: ARP Spoofing Diagram

2.2.5 Data Tampering

After enterprises transmit data to the service provider, they have no visibility into how the provider processes it. They cannot know whether the data has been altered in the background, so customer enterprises face risks to the integrity of stored data.

2.3 Physical Security

Also known as hardware security, it encompasses essential elements such as power supply, infrastructure, communication facilities, and the system environment of the SaaS provider. Since all SaaS resources are stored on the provider's servers and must be available 24/7, natural disasters or system crashes pose significant threats to SaaS data and privacy. On April 21, 2018, the cloud provider Amazon experienced a large-scale outage that

affected customer services such as the news site Reddit, the location-tracking service FourSquare, and the Q&A platform Quora. Due to the Amazon cloud service interruption, Reddit's service capacity was degraded for nearly four days, causing substantial losses to the customer enterprise.

2.4 Client-Side Risks

Because most current SaaS services adopt a browser- and server-oriented B/S architecture, the WAN environment exposes the client to many security threats. Moreover, today's client browsers still contain vulnerabilities such as SQL injection, cross-site scripting, and HTTP header tracking. If the client is compromised, user input can be stolen and the corresponding server inevitably affected, ultimately causing severe harm to the enterprise. The unique nature of the SaaS model means that a client-side security incident can have an immeasurable, wide-ranging impact.

A common cross-site scripting vulnerability (XSS) is exploited when attackers insert a link to a malicious URL via a site's comment, review, or email features. When the user opens the URL in a web browser, the malicious script is executed [3], achieving the attacker's goal. The attack flow is shown in the figure:

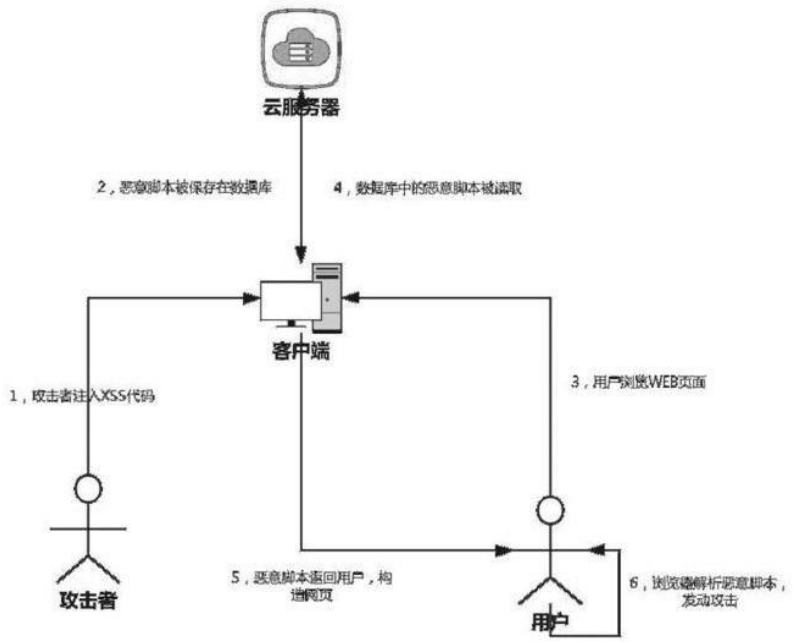


Figure 3: XSS Attack Flow Diagram

2.5 Account Privilege Issues

In the SaaS model, the service provider holds super-user privileges over all accounts. Therefore, any change to a customer's account permissions requires manual intervention by the provider's super user. If a privileged employee leaves the company and the account is not promptly revoked or modified, the ex-employee may retain resource-management rights, posing a serious threat to the enterprise's data security.

2.6 Improper Human Operations

When using SaaS services, the super user manually grants the customer enterprise certain rights to manage data resources and assigns them to relevant administrators. Holders of high-level privileges must possess professional expertise; otherwise, a major operational error could disrupt the secure operation of the server system.

2.7 Strategic Risk

Due to the characteristics of SaaS services, enterprises must integrate information-technology outsourcing and adjust internal resource deployment, organizational structure, and business processes accordingly, thereby losing control over some resources and affecting brand perception, corporate culture, and strategic planning. Outsourced

software development and information-processing technologies diminish the enterprise's IT innovation capacity. For enterprises with large user bases, the outsourced applications, infrastructure, and edge services provided by suppliers can erode user confidence in the brand and even degrade service availability and user experience.

2.8 Risk of Increased Costs

The most immediate driver for enterprises to adopt SaaS is cost. While the SaaS model can save substantial upfront investment in information systems, from a long-term strategic perspective, as enterprise needs expand, the growing demand for customization and elasticity, together with hidden costs such as telephone support, training, and other services provided by SaaS vendors, will continuously increase marginal costs. Eventually, the enterprise may revert to traditional models, at which point rebuilding the information management system will become extremely difficult and capital-intensive.

2.9 Legal Risks

Because legislation lags behind technological advances, traditional leasing laws are increasingly ill-suited to the new SaaS model. Relevant contract and leasing statutes are incomplete, leading to potential legal disputes. The software distribution and licensing methods under SaaS have evolved in both technical characteristics and business models, creating several latent copyright issues among the three parties: the software copyright holder, the cloud service provider, and the cloud user [4].

Rapid cloud-computing growth has so far failed to produce authoritative third-party certification bodies or a sound, authoritative, and fair oversight system. Consequently, enterprises and operators lack a reliable foundation and security guarantees when conducting business. For example, during the 2018 Amazon Web Services outage, the provider did not legally breach the Amazon EC2 Service Level Agreement (SLA) because the failures occurred in EBS and RDS, not EC2. Thus, what truly protects both customers and providers is not merely such agreements, but robust technical standards and contractual safeguards.

3. ENTERPRISE COUNTERMEASURES AGAINST SECURITY RISKS

3.1 Adopt a Segregated and Tiered Management Model

Assign management permissions according to different security levels; personnel handling critical data must strictly follow regulations and procedures, and all operations must be logged in detail. This prevents excessive concentration of power and reduces the risk of data theft driven by economic incentives.

3.2 Establish Network Access Control Systems

3.2.1 Access control systems can govern critical privilege, attribute, and network access controls, restricting user permissions by tier and prohibiting unauthorized operations.

3.2.2 Deploy firewalls to isolate internal and external networks, intercept sensitive or malicious data, and prevent its leakage to the external network, thereby playing a vital role in safeguarding both enterprise and user data.

3.2.3 Real-time monitoring: use filter technologies (Vericept or Web-sense) to continuously monitor user data transfers or remote operations; once suspicious data or illegal intrusion and sabotage are detected, promptly filter and block them to prevent Trojan attacks and user data leakage [5].

3.3 Build a Cloud Security Protection System

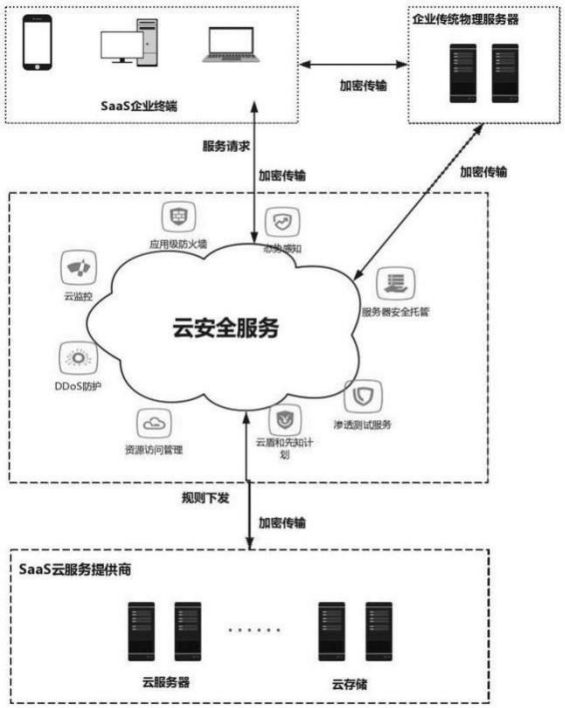
Client-side network security protection is also required; there are two approaches: first, configure a firewall and install antivirus software—when the computer is attacked by Trojans or viruses, the antivirus software will issue an alert, effectively safeguarding the computer and blocking illegal intrusions; second, use port-scanning tools or detection software to monitor the information-receiving system, cutting off the network immediately upon detecting any illegal intrusion [6].

3.4 Data Encryption

Confidentiality in computer network technology is usually achieved through physical and mathematical means to ensure that information is not leaked during transmission and storage; this is a proactive measure against information-security issues [6]. By combining the DES data encryption standard with the RSA system, data are encrypted before transmission and decrypted upon arrival at the receiving point, ensuring security during network transit.

3.5 Build a Cloud Security Protection System

Hacker attacks often cause significant economic losses, so establishing a robust security protection system is essential. Enterprises can leverage one-stop cloud security products and services, using a big-data platform to create a comprehensive defense system that integrates detection, defense, auditing, and incident response. The figure below shows the cloud security protection system model:



3.6 Enhance Security Education and Training for Internal Personnel

Through regular security training, continuously standardize internal employee management, deepen professional ethics and integrity, and strengthen education on relevant laws and regulations. Employees should also keep learning new cloud-computing technologies, stay informed about developments in network-security knowledge, and cultivate a strong awareness of network-security precautions.

4. CONCLUSION

In short, in today's highly developed Internet era, network security is a prominent issue in cloud-computing applications. While enjoying the convenience of SaaS cloud services, customer enterprises must pay greater attention to the various risks of data storage and transmission, and when setting long-term strategic goals, they must recognize the importance of building an independent information system. Customer enterprises should actively confront the security risks encountered during development, enhance overall corporate strength, and improve competitiveness.

REFERENCES

[1] Wang, Yang, and Kowei Shih. "Hybrid multi-modal recommendation system: Integrating mmoe and xgboost for enhanced personalization and accuracy." 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC). IEEE, 2024.

[2] Fu, Lei, et al. "Adversarial Prompt Optimization in LLMs: HijackNet's Approach to Robustness and Defense Evasion." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.
[3] Zheng, Haoran, et al. "FinGPT-Agent: An Advanced Framework for Multimodal Research Report Generation with Task-Adaptive Optimization and Hierarchical Attention." (2025).
[4] Weng, Yijie, et al. "SafeGen-X: A Comprehensive Framework for Enhancing Security, Compliance, and Robustness in Large Language Models." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[5] Chen, Yang, et al. "SyntheClean: Enhancing Large-Scale Multimodal Models via Adaptive Data Synthesis and Cleaning." 2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA). IEEE, 2025.
[6] Jiang, Gaozhe, et al. "A Knowledge-Enhanced Multi-Task Learning Model for Domain-Specific Question Answering." 2025 7th International Conference on Information Science, Electrical and Automation Engineering (ISEAE). IEEE, 2025.
[7] Zhuo, Jiayang, et al. "An Intelligent-Aware Transformer with Domain Adaptation and Contextual Reasoning for Question Answering." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[8] Zhang, Hanlu, et al. "Dynamic Attention-Guided Video Generation from Text with Multi-Scale Synthesis and LoRA Optimization." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.
[9] Zhao, Shihao, et al. "KET-GPT: A Modular Framework for Precision Knowledge Updates in Pretrained Language Models." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[10] Shih, Kowei, et al. "DST-GFN: A Dual-Stage Transformer Network with Gated Fusion for Pairwise User Preference Prediction in Dialogue Systems." 2025 8th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). IEEE, 2025.
[11] Li, Xuan, et al. "MLIF-Net: Multimodal Fusion of Vision Transformers and Large Language Models for AI Image Detection." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[12] Xie, Minhui, and Shujian Chen. "InVis: Interactive Neural Visualization System for Human-Centered Data Interpretation." Authorea Preprints (2025).
[13] Xie, Minhui, and Shujian Chen. "CoreViz: Context-Aware Reasoning and Visualization Engine for Business Intelligence Dashboards." Authorea Preprints (2025).
[14] Zhu, Bingxin. "TraceLM: Temporal Root-Cause Analysis with Contextual Embedding Language Models." (2025).
[15] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).
[16] Zhang, Yuhan. "SafeServe: Scalable Tooling for Release Safety and Push Testing in Multi-App Monetization Platforms." (2025).
[17] Hu, Xiao. "AdPercept: Visual Saliency and Attention Modeling in Ad 3D Design." (2025).
[18] Hu, Xiao. "UnrealAdBlend: Immersive 3D Ad Content Creation via Game Engine Pipelines." (2025).
[19] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.
[20] D. Restrepo, C. Wu, S.A. Cajas, L.F. Nakayama, L.A. Celi, D.M. López. Multimodal deep learning for low-resource settings: A vector embedding alignment approach for healthcare applications. (2024), 10.1101/2024.06.03.24308401
[21] Jiang, G., Yang, J., Zhao, S., Chen, H., Zhong, Y., & Gong, C. (2025). Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance. Preprints. https://doi.org/10.20944/preprints202504.1735.v1
[22] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).
[23] Yu, Z., Sun, N., Wu, S., & Wang, Y. (2025, March). Research on Automatic Text Summarization Using Transformer and Pointer-Generator Networks. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 1601-1604). IEEE.
[24] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.
[25] Pal, P. et al. 2025. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. Journal of Theory and Practice in Economics and Management. 2, 3 (May 2025), 1–9.