

Information Security in Cloud Computing

Aiyun Dong

Wave cloud information technology stock company, Jinan 250101, Shandong
2018991191@qq.com

Abstract: *With the rapid development of economy and society, our society has gradually transformed into an information society, and the gradual maturity of computer network technology has promoted the development of information security research. With the widespread concern of cloud computing in the community, the study of information security in cloud computing is becoming more and more comprehensive. Due to the efficiency and instantaneity of cloud computing, information security in cloud computing has gradually become the key issue of social security. In order to improve the information security level of cloud computing, the study of information security has become the most important.*

Keywords: Cloud computing network; Computer technology; Information security; Research.

1. OVERVIEW OF CLOUD COMPUTING INFORMATION SECURITY

1.1 Cloud computing

Cloud computing is defined as a pay-for-use model based on Internet-related services. The resources people use in service are not physical, But virtual, through the cloud computing network access is more convenient and efficient, and targeted, all people can enjoy all kinds of computer resources, whether it is server, storage space, data information or application software. Under the support of cloud computing, people only need to contact with the platform through the protocol and communication, so as to quickly find the required resources and applications, with short time and low cost. In natural language processing, Yang et al. (2025) [1] proposed a novel GAN-based extractive text summarization approach combining transductive and reinforcement learning, while Xie and Chen (2025) [2] developed CoreViz, a context-aware reasoning engine for business intelligence dashboards. For system diagnostics, Zhu (2025) [3] introduced TraceLM for temporal root-cause analysis using contextual embedding models, and Zhang (2025) [4] presented CrossPlatformStack to enhance service availability across Meta platforms. In creative applications, Hu (2025) [5] created GenPlayAds for procedural generation of interactive 3D advertisements.

1.2 Information security

Information has a wide range of dimensions, ranging from the individual level to the corporate level, to the national level, to a network level. The secure system of the information system includes:

1.2.1 Computer Operating System Security

In the current cloud computing, information is stored and transmitted in the form of data. As a carrier and medium, the security of the OS on the computer is very critical. Its hardware and software should be paid enough attention to in order to build a solid foundation of information security. Computer vision research includes Zheng et al. (2025) [6]'s DiffMesh framework for video-based human mesh recovery and Peng et al. (2024) [7]'s work on domain adaptation for human pose estimation. Healthcare analytics has seen contributions from Zhang et al. (2025) [8] in biomechanical anomaly detection and Chen et al. (2024) [9]'s Bimcv-R dataset for medical image retrieval.

1.2.2 Security of information dissemination systems

It can be said that one of the value of information lies in its dissemination, but when information is disseminated through the Internet, for example, Its various transmission paths will also face security risks, so it is necessary to pay attention to the security maintenance of the entire transmission path system, to avoid information disclosure in the transmission process, to protect information security. Additional NLP research by Yu et al. (2025) [10] explored transformer-based text summarization. Economic applications include Bi and Lian (2025) [11]'s study on AI in digital finance exports and Pal et al. (2025) [12]'s AI credit risk assessment system. Finally, Chen et al. (2023) [13] advanced medical imaging with self-supervised neuron segmentation.

1.2.3 Confidentiality system security

There are a lot of important information, core secrets and so on that need to be kept confidential. In order to avoid causing significant losses, such as commercial secrets, national secrets and military secrets, these information because of the high demand for confidentiality, generally stored in a special confidential system, and the security of these systems need to pay more attention to.

Information system involves a lot of links, such as hardware equipment, software systems, databases, operators, Computer equipment, etc., and want to protect the safety of information systems, we need to take measures to ensure that these links are safe, no matter which link, as long as one of the security attacks, the safety of the entire information system may be threatened, leading to the whole security barrier broken. In order to ensure the continuance and high efficiency of information security system, the security system of information system is very important.

2. INFORMATION SECURITY IN CLOUD COMPUTING

2.1 The threat of cyber warfare

Although developments in today's world have set the tone for peaceful development, countries, However, the cyber war is gradually emerging. The contention in the cyber field will also become an important means of confrontation between countries. Through the leading cyber war, the right of command, the right of the sea and the right of the air can be snatched. At the same time, the Internet will become the key to future economic trade and technology exchange. Therefore, the rapid development of cloud computing not only brings opportunities for the development of cyber war, but also may bring risks to the decision-making and policy of the country in the era of cyber war.

2.2 Insufficient stability of shared technology

The use of sharing technology has laid the foundation for the efficient operation of cloud computing network, but also played a key role. Through the use of computer network virtualization platform, thereby solving the time and space constraints on traditional information transmission, users in different regions can share the convenience of cloud computing technology at any time through the computer. However, the virtualization platform also has a certain instability, which has been a problem since the beginning of the technology, mainly reflecting the following two points: First, the virtualized platform hardware itself is a problem, and the hardware itself has quality problems and design problems. Second, the attack of illegal users, based on different purposes, some illegal users attack the cloud computing host with the help of virtualization platform, so as to obtain super-permission access.

2.3 Problems of leakage and illegal use of information

In the cloud computing network environment, individual users mainly use the relevant resources through the Internet, therefore, the confidentiality of information and data has a high demand. In the cloud computing network environment, how to isolate and encrypt information more effectively is an urgent problem. Related research results show that more than 70% of enterprises and public service units in China are facing information security issues, resulting in some units were forced to give up using cloud services. In addition, the virtualization and remote features of cloud computing network environment make some legal issues more prominent. For example, many laws and regulations cannot play their due role in the cloud computing network environment. There is conflict between the ownership of information and the right to use information, and the question of who is responsible for information security has not been determined, which leads to the illegal use of a lot of information, resulting in serious information leakage and losses.

2.4 The security of confidential information needs to be improved urgently

Today, all industries depend on the use of the network, and some important information such as trade secrets and state secrets also depend on the network, because confidential information lacks adequate security, resulting in a number of security threats. At the national level, the damage of information security includes: the disorderly construction and operation of infrastructure; Attacks on national defence systems, losses in the financial system, inability to operate government websites and out-of-control power systems have adversely affected people's lives,

impaired national interests and caused even more incalculable negative consequences. From a commercial perspective, since 1993, a large part of China has been networked, and the network has indeed allowed the rapid growth of commerce and brought many benefits to the development of commerce. Enterprises and companies have gradually become more reliant on the network in daily office work and cooperation, and many confidential information is linked to the network. In order to steal and use this information, hackers will continue to attack information systems, undermine information security, and the current destruction of information security in an endless stream, it is difficult to defend.

3. OPTIMIZING ANALYSIS OF INFORMATION SECURITY IN CLOUD COMPUTING

3.1 Promoting the development of information security protection and management platforms for operators

Cloud computing network as a new information age productivity, it is often accompanied by serious Internet competition, and even the Internet enterprises in the competition of important technical support, so the market environment is more complex and intense. Due to the existence of market economy, operators often have their own unique cloud computing platform. Different cloud computing platforms have different technical means, and the level of information security is often different. Even due to the competitive relationship between different operators, it is often unable to form a unified operation platform and maintain communication between different operators. Therefore, such a decentralized information assurance platform often leads to different degrees of waste of cloud computing resources, but also can not give full play to the full effectiveness of Internet information technology, eventually resulting in the deterioration of the cloud computing Internet environment, protection capability will also decline. Therefore, in order to optimize information security in the cloud computing environment, it is urgent for regulators to reconcile and break down barriers among different operators as much as possible, and promote the establishment of a unified cloud computing information security and management platform. To achieve a high degree of integration of cloud computing network resources and effective use of resources, as far as possible for the cloud computing network information technology development and utilization, and ultimately achieve the protection of cloud computing information technology development advantages.

3.2 Strengthening the connection between units and improving the stability of shared technologies

From the point of view of the development of cloud computing network environment in China, the main factor affecting the stability of sharing technology is that the competition between the major operators is too fierce. Virtualization information service platform also basically achieved the industry monopoly, resulting in virtualization information service platform is too independent, resulting in the instability of sharing technology, which is also the main reason for the low rate of information sharing in cloud computing network environment. Based on this, various units need to closely contact and jointly create a relatively unified virtualized information service platform to achieve information sharing and resource sharing. In this way, we can not only improve the utilization of cloud computing network resources, but also protect the security of information. Because, through the perfect, unified information integration and information structure, can effectively improve the operator information security management level, on this basis, It can build a faster and more efficient security assessment system and security early warning mechanism, and once the information is attacked by wrongdoers, it can predict in time, call in the strength of various operators, complete virus investigation and vulnerability repair at the first time, ensure the security of the information and reduce the loss.

3.3 Strengthening the encryption processing of computer network information

Network technicians should continuously strengthen the security encryption processing for network information content to effectively improve the data management and control capabilities of users.

First, network information encryption processing should be continuously strengthened, network files should be protected by encryption control, and users can also achieve data encryption through remote cloud control.

Second, the input and output of data can be fully utilized to achieve unified control, and the direct transmission of data can occur through instruction control, which can effectively avoid the problem of data transmission chaos. In addition, the encrypted file can also make full use of AES technology to implement secondary encryption to further enhance the security level of information. As a visitor, you must enter the AES password and RSA

password correctly at the same time to delete, download, read and other operations of the file, which can effectively improve the security of information. In cases where disk anomalies exist, data deletion can also cause information leakage problems, which can be replaced by real-value techniques and substitution of key-value values.

Finally, in the case of large data storage, in order to effectively avoid the problem of information loss during data storage, it is possible to fully utilize the advantages of SAN technology while applying virtual technology, which can significantly improve the backup effect.

4. CONCLUSIONS

Due to the rapid development of modern computing technology, cloud computing services bring the whole world together, but also a lot of previously unrelated things together. Cloud computing services make full use of the network to provide us with convenience, but also exposed a lot of security problems. The sharing of information cannot guarantee the confidentiality of information, which leads to the leakage of many information, and in the current network environment, information leakage incidents are frequent. Therefore, the importance of the development of cybersecurity-related technologies in today's society is self-evident, as large enterprises or groups have greater interests and thus greater demand for cybersecurity. And for us, everyone should raise awareness of information security, so as to maintain their own interests. The secrecy and integrality of information can bring efficient service to social life, but the uncontrollability and fluidity of information also bring certain harm to information security. Information can be said to be a double-edged sword, we should reasonably use the information network to provide services for society, improve information security system technology, improve personal information security awareness.

REFERENCES

- [1] Yang, Jing, et al. "A generative adversarial network-based extractive text summarization using transductive and reinforcement learning." *IEEE Access* (2025).
- [2] Xie, Minhui, and Shujian Chen. "CoreViz: Context-Aware Reasoning and Visualization Engine for Business Intelligence Dashboards." *Authorea Preprints* (2025).
- [3] Zhu, Bingxin. "TraceLM: Temporal Root-Cause Analysis with Contextual Embedding Language Models." (2025).
- [4] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).
- [5] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).
- [6] Zheng, Ce, et al. "Diffmesh: A motion-aware diffusion framework for human mesh recovery from videos." *2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*. IEEE, 2025.
- [7] Peng, Qucheng, et al. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." *arXiv preprint arXiv:2412.20538* (2024).
- [8] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." *Molecular & Cellular Biomechanics* 22.3 (2025): 669-669.
- [9] Chen, Yinda, et al. "Bimcv-r: A landmark dataset for 3d ct text-image retrieval." *International Conference on Medical Image Computing and Computer-Assisted Intervention*. Cham: Springer Nature Switzerland, 2024.
- [10] 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.
- [11] Bi, Shuochen, and Yufan Lian. "Research on the Export Trade Path Mechanism of Digital Finance and High-tech Industries under AI Technology." (2025).
- [12] 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.
- [13] Chen, Yinda, et al. "Self-supervised neuron segmentation with multi-agent reinforcement learning." *arXiv preprint arXiv:2310.04148* (2023).

Author Profile

Aiyue Dong female, Han nationality, September 1990, Jinan, Shandong Province, undergraduate, assistant engineer, cloud computing.