European Journal of AI, Computing & Informatics

Vol. 1 No. 2 2025

Article **Open Access**

Research on Enterprise Data Security Protection Technology on Cloud Platforms

Yu Pan [1,*]

[1] Matthews Real Estate Investment Services, El Segundo, California, 90245, USA
* Correspondence: Yu Pan, Matthews Real Estate Investment Services, El Segundo, California, 90245, USA

Abstract: With the popularization of cloud computing technology, enterprises are increasingly relying on cloud platforms for data storage and processing. Although cloud platforms bring flexibility and scalability to enterprises, data security concerns have become increasingly prominent. Due to the openness and resource sharing characteristics of cloud platforms, enterprises face multiple security challenges in data storage, transmission, and access permission management. This article elaborates on the basic definition of data security and provides an in-depth analysis of the data protection management model in cloud computing platforms. It further discusses the technical security challenges in multiple aspects such as data storage, transmission, and identity verification, and introduces various protective measures such as data encryption, data backup, and strengthened access permission management. By adopting these technological solutions, enterprises can effectively defend against the risks of data leakage and unauthorized access, ensuring the confidentiality, integrity, and availability of cloud platform data.

Keywords: cloud platform; data security; data protection; access control; encryption technology

Received: 05 May 2025
Revised: 13 May 2025
Accepted: 11 June 2025
Published: 12 June 2025

1. Introduction

In recent years, the application of cloud computing technology in enterprise information construction has become increasingly widespread, and many enterprises have chosen to transfer key data and core businesses to cloud platforms. Although cloud platforms bring flexible data processing and storage advantages to enterprises, their openness and resource sharing features also bring new security issues. Enterprise data in the cloud faces security threats such as information leakage, data tampering, and unauthorized access. Currently, data security has become a core issue that enterprises must face in cloud platforms. Against the backdrop of increasingly stringent information security regulations, data security protection for cloud platforms is not only a technical issue, but also involves multiple levels such as law, management, and corporate governance. This article aims to deeply analyze the technical challenges faced by enterprises in data security protection on cloud platforms, and explore the challenges in data storage, transmission process, user authentication, and other aspects. Effective technical measures will be proposed to enhance enterprises' ability to ensure data security on cloud platforms.

2. Theoretical Basis of Cloud Platform Data Security

2.1. Basic Concepts of Data Security

Data security refers to the confidentiality, integrity, and availability of data throughout its entire lifecycle through a series of technologies and management strategies. Confidentiality means that data is only open to authorized users, avoiding unauthorized disclosure or access; Integrity ensures that data is protected from improper alteration or destruction during storage, transmission, and processing; Availability ensures that data can be accessed by authorized users in a timely manner when necessary [1]. The core concept of data security is usually summarized as the "CIA Three Principles"-confidentiality, integrity, and availability.

In the cloud platform environment, the protection framework required to ensure data security integrates technical guarantees and management measures. The commonly adopted security theoretical framework covers multiple aspects such as permission management, data encryption, data backup, and disaster recovery. With the gradual maturity of cloud computing service models (IaaS, PaaS, SaaS), data storage, processing, and transmission have surpassed the scope of traditional local servers and shifted towards a multi-tenant resource-sharing architecture. Therefore, the challenges faced by cloud platforms in terms of data security are becoming increasingly diverse, requiring attention to both the protection of the data itself and the challenges of multiple dimensions such as virtualization technology application, network security, and isolation between multi tenant data [2].

2.2. Cloud Platform Data Security Management Model

The cloud platform data security management model is a comprehensive framework specially constructed to ensure the security of data in various aspects of the cloud, such as storage, processing, and transmission processes. This model integrates a variety of security protection mechanisms, covering security policies at multiple levels such as physical, network, application, and management. Specifically, this security management architecture implements multi-level and multi-angle security protection measures to ensure data security and compliance at all stages. The commonly used security management models involve role-based access control (RBAC), encryption and backup policies, as well as data isolation and data leakage protection systems [3]. Table 1 provides a detailed list of the key components and their roles of the cloud platform data security management model.

Table 1. Key Components of Cloud Platform Data Security Management Model.

Component	Function Description
access control	Restricting user permissions to prevent unauthorized access
data encryption	Protecting the confidentiality of data
identity authentication	Verification of user identity legitimacy
Data isolation	Ensure the security of multi tenant data
Leakage protection	Preventing data leakage and abuse

3. Technical Issues Regarding Enterprise Data Security Protection on Cloud Platforms

3.1. Data Storage Security

The security of data storage on cloud platforms has become one of the core challenges faced by enterprises. Due to the widespread reliance on distributed architecture in cloud storage, data is distributed across multiple storage nodes in different regions. While this approach improves data access efficiency, it also increases the likelihood of data being illegally accessed, lost, or tampered with. Enterprises often find it difficult to fully control the specific location and storage devices where data is stored, leading to potential vulnerabilities that may be exploited by malicious individuals to steal data. In cloud platforms,

multiple users share the same storage resources [4]. If the isolation effect of virtualization technology is poor, there is a possibility of data leakage or mutual access of different user data. Although cloud service providers typically encrypt data, the storage of encryption keys carries hidden risks. Once the key is leaked or managed improperly, the integrity of encrypted data will be greatly threatened. In addition, the development of data backup and recovery plans is also crucial. If backup data is not properly stored or if the recovery process contains defects, the risk of data loss or failure to recover after a disaster will significantly increase [4].

3.2. Data Transmission Security

Data is susceptible to risks such as man in the middle interference, eavesdropping, and illegal modification during network transmission. Transmission processes that have not been encrypted, particularly over the open Internet, are more likely to be intercepted by undesirable elements, resulting in the leakage of key information. Meanwhile, data in cloud platforms often comes from different channels, multiple terminals, and cross regional sources, which undoubtedly increases the likelihood of network attacks. The compliance challenges faced by cross-border data transmission are even more severe, as different countries or regions have varying regulations on data protection, which may cause damage to the confidentiality and integrity of data. Although cloud service providers generally use encrypted communication protocols (such as TLS/SSL) to protect data transmission, if there are omissions in encryption key management or defects in the protocol itself, there is still a risk of unauthorized access or tampering during data transmission. Enterprises have limited capabilities in data transmission security control, making it difficult to achieve complete control over every security link [5].

3.3. Access Control and Identity Authentication

The multi tenant structure pattern enables different enterprises and individuals to jointly use the same resources. Once access control is not strict, unauthorized users have the opportunity to access critical data, which may lead to data leakage or tampering. In addition, traditional user authentication methods, such as username and password, are vulnerable to brute force cracking and phishing attacks and are no longer sufficient to meet security requirements. Due to the dynamic changes in the cloud platform environment, the management of identity verification has become more complex. The verification of enterprise users and third-party services requires coordination among numerous services, and if lacking centralized control, this can easily lead to security vulnerabilities or inconsistencies [6]. Although single sign on (SSO) technology makes the login process more convenient, there is still a risk of being exploited by attackers if not combined with multi factor authentication (MFA), who may steal authentication information to gain access. If there is a lack of efficient access control and identity authentication mechanisms, it will greatly weaken the security protection of the system, increase the possibility of data leakage and improper use.

3.4. Data Leakage and Illegal Access

Due to the high openness of the platform and the architecture of multi-user coexistence, data is often exposed to vulnerable network environments, thereby increasing the likelihood of data being stolen by criminals. The risk of data leakage may arise from internal factors (such as unauthorized operations by employees) or external factors (such as illegal intrusion by hackers). Unauthorized access is generally achieved through stealing user credentials, forcibly cracking passwords, or circumventing authentication measures, allowing attackers to gain access to critical information. Even with access control measures in place, if permission settings are not strict enough, inappropriate access events may still occur [7]. The leakage and illegal access of data may not only result in property damage,

but also have a negative impact on the reputation of the enterprise, and even violate relevant laws and regulations on data protection.

4. Enterprise Data Security Protection Technology Strategy on Cloud Platforms

4.1. Strengthen Data Encryption and Backup

Data encryption and backup are two key means to ensure enterprise data security on cloud platforms. Greatly reduces the risk of data leakage, tampering, or loss. Encryption technology maintains data confidentiality during storage and transmission, making it difficult to interpret or modify even in the event of illegal intrusion. In the encryption process, a dual layer mechanism of symmetric encryption and asymmetric encryption is often used to reinforce the security protection of data.

Symmetric encryption algorithms, such as AES, are commonly used for data storage and can quickly and efficiently encrypt large-scale data. When performing encryption operations, the system will create a key (K). Furthermore, convert the raw data into (P) Convert to ciphertext (C). The ciphertext can only be decrypted when the user or system holds a matching key. In cloud platforms, AES-256 (256 bit key length) can be used, and its encryption process can be described by the following formula:

$$C = E(K, P)$$

Among them: C is ciphertext; E representing encryption operations; K it is an encryption key; P it is plaintext data. Asymmetric encryption (such as RSA) is used for key exchange and identity confirmation, with the core purpose of ensuring that data is not tampered with or intercepted during transmission. In this process, the sender of the data encrypts it using the receiver's public key, while the receiver decrypts it using their own private key, thus achieving secure transmission of the data.

With appropriate backup strategies, enterprises can thoroughly back up all data to ensure that the original data can be fully restored. The full backup method is suitable for situations where the amount of data is small or backup operations are not frequent. Organizations may choose to only back up data that has changed since the last backup operation. This incremental backup method can reduce storage space usage while improving backup efficiency. Differential backup backs up all data changes that have occurred since the last comprehensive backup. Compared to incremental backup, differential backup is faster in data recovery, but it requires higher storage space.

To enhance data protection capabilities, carefully screen the datasets to be backed up and determine whether to perform full or incremental backups. Encrypt the selected data using the same encryption method and key as the original to ensure the security of backup data. Store encrypted backup data in local or remote data storage centers and adopt multi copy storage technology (such as RAID technology) to enhance data backup redundancy. Periodically perform practical exercises for data recovery to verify the integrity and recovery capability of backup data, ensuring rapid data recovery in emergency situations. By relying on these encryption and backup solutions, enterprises can effectively mitigate the risks of cloud platform data leakage, tampering, or loss, ensuring that data maintains its integrity and availability in all situations.

4.2. Use of Secure Transmission Protocols and Protection

In cloud platforms, data is vulnerable to various security threats during transmission, including eavesdropping, data tampering, and man in the middle attacks. To protect data confidentiality, integrity, and availability, enterprises need to adopt secure transmission protocols and implement a series of protection strategies to ensure the security of the transmission process. The widely adopted secure transmission mechanism is the TLS/SSL protocol, which uses encryption to protect transmitted data. The TLS/SSL protocol uses public key cryptography for key exchange and identity verification during the handshake phase, and symmetric key encryption for data transmission to ensure efficiency and security. During the TLS handshake phase, public key encryption is responsible for identity

confirmation and key exchange, ensuring the authenticity of the identities of both parties in communication; In the data exchange stage, private key encryption is used to encrypt the data content, avoiding data leakage or tampering [8]. When accessing cloud services through HTTPS, the browser automatically initiates a TLS connection, creating an encrypted communication tunnel to ensure the security of data transmission.

Enterprises can also use the IPsec protocol, especially in VPN or internal network scenarios, to build encrypted communication channels, ensuring the protection of data transmission from internal networks to cloud platforms. With the help of Key Management Scheme (KMS), the security of keys is strengthened, preventing the risk of key leakage. In the encryption process, once the key is lost or leaked, data security will be threatened. Therefore, KMS is crucial for managing the generation, storage, and distribution of keys. In addition, using multiple factor authentication (MFA) and digital certificates can help defend against unauthorized access attempts. By using TLS/SSL and IPsec encryption protocols, coupled with rigorous key management and authentication policies, enterprises can effectively defend against data interception or tampering during transmission, ensuring the security of data in cloud platforms.

4.3. Strengthen Access Control and Identity Authentication Mechanisms

With the continuous improvement of enterprise informatization level, the data confidentiality threats faced are becoming increasingly complex. Especially in cloud environments where multiple tenants coexist, ensuring that data resources are only used by authorized users, avoiding illegal intrusion and abuse of permissions, has become an important issue that enterprises urgently need to address.

Enterprises need to implement the principle of minimum authorization based on employees' functions, positions, and actual work needs, ensuring that each employee can only access the necessary information resources within their scope of responsibility. This approach requires configuring detailed access control lists (ACLs) or role-based access control (RBAC) systems in the cloud platform. These mechanisms grant different levels of access to users based on their identities and roles. For example, system administrators should have comprehensive resource access permissions, while general staff can only access limited datasets or software applications. Through this refined permission configuration, the possibility of excessive opening or improper use of permissions can be reduced. Given that traditional user authentication methods, such as username and password, are no longer sufficient to resist increasingly complex security attacks, enterprises should adopt Multi Factor Authentication (MFA) mechanisms, which require users to provide multiple forms of authentication such as passwords, dynamic verification codes, and biometric data like fingerprint recognition. during the login process. This approach not only enhances the reliability of identity verification, but also effectively prevents the risk of login credentials being illegally used.

In order to enhance the rigor of identity authentication, enterprises need to adopt single sign on (SSO) technology to simplify the user identity confirmation process and optimize the user's operational experience. Single sign-on technology relies on a centralized identity provider (IdP), allowing users to access multiple systems and applications with just one login operation, without the need to repeatedly enter account information. This measure significantly improves the user experience and reduces the complexity of managing multiple login credentials.

4.4. Deploying Data Leakage Prevention and Monitoring System

Given the frequent occurrence of data breaches, enterprises must proactively address potential threats and continuously monitor their data security posture. The DLP system relies on real-time tracking of data transmission to effectively curb unauthorized access, transfer, or sharing of sensitive information. The system classifies critical data based on established strategies and develops corresponding security measures to prevent sensitive

information from being exposed to unauthorized or unsecured environments. DLP technology typically includes content inspection capabilities that can detect sensitive information such as personal identifiers or financial data in documents, emails, and other communication channels. When a violation is detected, the DLP system may block data transmission, encrypt files, or alert administrators to maintain data integrity.

At the same time, the data monitoring system analyzes log information, user interactions, and network data streams in real-time, helping the security team identify possible intrusions and abnormal behaviors in a timely manner. With the help of intrusion detection and protection systems (IDS and IPS), enterprises can monitor network abnormal actions in real time, effectively curbing the risk of data leakage. In addition, monitoring mechanisms should be integrated with Security Information and Event Management (SIEM) systems to aggregate and analyze diverse security events from multiple sources, and to respond quickly to potential threats.

In cloud environments, monitoring systems need to include high-precision permission auditing mechanisms to ensure that only authorized users have access to critical data and can monitor any unauthorized access in real time. Regular security training and vulnerability assessments are essential for ensuring system effectiveness, which helps to detect and respond to new security threats in a timely manner. By properly configuring DLP and monitoring systems, enterprises can effectively avoid data breaches, identify and handle security incidents in a timely manner, thereby reducing the risks caused by data breaches.

5. Conclusion

With the widespread application of cloud computing technology, cloud platforms have become an important environment for enterprise data storage and processing. However, the openness and resource sharing characteristics of cloud platforms also bring new data security issues. This article delves into the key technologies of encryption and backup technology, transmission security, access control and identity authentication, as well as preventing data leakage and establishing monitoring systems. This paper proposes targeted strategies — including advanced encryption, multi-level identity verification, and real-time monitoring systems — to help enterprises mitigate data leakage, tampering, and unauthorized access, ensuring the confidentiality, integrity, and availability of data. As cybersecurity threats continue to evolve, enterprises must constantly update their security measures and maintain their ability to respond to new attack methods.

References

1. N. Akhtar, A. Ahmed, M. Khan, S. Iqbal, R. Ahmad, A. Khan et al., "A comprehensive overview of privacy and data security for cloud storage," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 2021, pp. 1–8, 2021, doi: 10.32628/IJSRSET21852.
2. I. Gupta, A. K. Yadav, H. Goel, P. Kumar, R. K. Yadav, S. Sharma et al., "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71247–71277, 2022, doi: 10.1109/ACCESS.2022.3188110.
3. A. T. Lo'ai and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 33, no. 7, pp. 810–819, 2021, doi: 10.1016/j.jksuci.2019.05.007.
4. R. Adee and H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, p. 1109, 2022, doi: 10.3390/s22031109.
5. F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *Int. J. Intell. Netw.*, vol. 2, pp. 18–33, 2021, doi: 10.1016/j.ijin.2021.03.001.
6. S. S. Vellela, R. Balamanigandan, and S. P. Praveen, "Strategic survey on security and privacy methods of cloud computing environment," *J. Next Gener. Technol.*, vol. 2, no. 1, pp. 1–9, 2022.
7. M. Mehrtak, S. A. SeyedAlinaghi, S. Shabani, S. Noori, H. Mirzapour, A. Mohammadi et al., "Security challenges and solutions using healthcare cloud computing," *J. Med. Life*, vol. 14, no. 4, pp. 448–456, 2021, doi: 10.25122/jml-2021-0100.
8. W. Ahmad, A. Rasool, A. R. Javed, T. Baker, Z. Jalil, M. A. Jan et al., "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, 2021, doi: 10.3390/electronics11010016.