Proceedings of CONF-SPML 2026 Symposium: The 2nd Neural Computing and Applications Workshop 2025
DOI: 10.54254/2755-2721/2026.TJ28888

Analysis of Security Risks and Prevention Strategies for Enterprise Big Data in Cloud Computing Environments

Yangzi Yang

Faculty of Digital Science, Shanghai Lida University, Shanghai, China
rhmbwt2052@outlook.com

Abstract. The open, shared, and virtualized nature of the cloud also introduces numerous security threats, which posing significant challenges to big data security in enterprises. Through case studies and comparative methods, this paper systematically identifies core security issues related to big data in cloud environments, including data breaches, unauthorized access, cloud platform vulnerabilities, and cross-border data compliance dilemmas. This paper constructs a tripartite integrated security framework encompassing technology, management, and compliance: at the technical level, end-to-end encryption, multi-factor authentication, and zero-trust architecture are adopted; at the management level, a full lifecycle security management mechanism is established, incorporating the principle of least privilege, regular assessments, disaster recovery, and training; at the compliance level, adherence to relevant domestic and international regulations is emphasized, with clear requirements for data sovereignty and cross-border data transfer. The research recommends that enterprises develop a security governance framework integrating "defense-in-depth, continuous optimization, and shared responsibility." By strengthening technical measures, optimizing management practices, and ensuring regulatory compliance, enterprises can comprehensively enhance the confidentiality, integrity, and availability of data in cloud environments, thereby providing a secure and reliable foundation for their digital transformation.

Keywords: Cloud Computing Security, Enterprise Big Data, Security Risks, Security Mitigation Strategies

1. Introduction

In the digital economy, cloud computing has become a key enabler for enterprise big data operations due to its scalability, on-demand provisioning, and efficiency gains. However, its open and virtualized nature breaks traditional security boundaries, leading to increased risks such as data leaks, unauthorized access, and platform vulnerabilities. These challenges hinder digital transformation and demand urgent attention. Current research primarily addresses isolated aspects of cloud security, such as encryption or access control, or promotes point solutions like blockchain or AI. Yet, a holistic approach is lacking—few studies integrate technical, managerial, and compliance dimensions into a unified framework. Critical issues like cross-border data flows, shared responsibility models, and privacy-utility balance remain understudied.

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.TJ28888

This study adopts a tripartite methodology: literature analysis to consolidate existing knowledge, case studies of real-world incidents, and comparative analysis of technical solutions, management frameworks, and compliance mechanisms. The research aims to answer: (1) What are the main security risks for enterprise big data in the cloud and their characteristics? (2) How do technical flaws, management gaps, and legal ambiguities jointly cause these risks? (3) How can an integrated strategy harmonize technology, management, and compliance to ensure security without compromising development? Theoretical contributions include refining cloud security risk frameworks and promoting interdisciplinary integration. Practically, the study offers enterprises an actionable model to secure data throughout its lifecycle while maximizing cloud benefits.

2. Overview of cloud computing and enterprise big data

The integration of cloud computing and enterprise big data represents a significant evolution in information technology infrastructure and data processing methodologies. This convergence has not only transformed enterprise IT architectures but has also emerged as a critical driver of digital transformation [1]. Gaining a precise understanding of the core characteristics of cloud computing, the dimensions of value in enterprise big data, and the current state of their integration forms the essential foundation for a systematic analysis of associated security risks and mitigation strategies.

2.1. Core characteristics of cloud computing

Cloud computing is a service model that integrates technologies such as distributed computing, virtualization, and automated management [2]. Its key characteristics include: (1) on-demand self-service. Users can unilaterally provision computing capabilities as needed automatically without requiring human interaction with each service provider, greatly enhancing the efficiency and flexibility of resource allocation. (2) broad network access. Services are available over the network and accessed through standard mechanisms that promote use by heterogeneous client platforms, enabling ubiquitous and location-independent access to resources. (3) resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. Centralization of resources creates economies of scale, reducing operational costs [3]. (4) rapid elasticity. Capabilities can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand. This allows users to dynamically adjust resource usage in response to business changes, avoiding both shortages and waste. (5) measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. This enables pay-per-use billing and fine-grained cost management.

2.2. Value attributes of enterprise big data

Enterprise big data has evolved from an operational byproduct into a core strategic resource and a key factor of production [4]. Its value is reflected not only in its sheer scale but also through the "4V" characteristics and the ensuing business value it generates: (1) Volume: The scale of data often reaches terabytes or even petabytes, exceeding the processing capacity of traditional databases. (2) Variety: Data exists in structured, semi-structured, and unstructured forms, constituting a multimodal information ecosystem. (3) Velocity: Data is generated and processed at high speeds, requiring enterprises to possess real-time or near-real-time stream data processing capabilities.

DOI: 10.54254/2755-2721/2026.TJ28888

Fourthly, Value: Big data exhibits low value density, necessitating the use of advanced analytical techniques to extract meaningful insights from massive datasets.

2.3. Current state of integration between cloud computing and enterprise big data

Currently, integration primarily manifests in three models: (1) IaaS supports big data storage and computation: Enterprises leverage virtual servers, storage, and network resources provided by cloud service providers to build big data processing environments, avoiding the high costs and management burdens associated with constructing private data centers. (2) PaaS facilitates big data application development: Cloud platforms integrate frameworks such as Hadoop and Spark, allowing enterprises to focus on analytical business logic without managing underlying clusters, thereby reducing development complexity and time. (3) BDaaS enables new forms of data analytics services: Providers encapsulate big data capabilities into APIs or analytical services (e.g., facial recognition, business intelligence), enabling small and medium-sized enterprises to access advanced analytical tools at low cost and promoting the widespread adoption of data applications. However, it should be noted that new challenges have emerged during this integration process, such as ambiguous data ownership, complex shared responsibility models for security, and compliance issues in cross-border data transfer. These have become critical issues that enterprises must address [5].

3. Security risks of enterprise big data in cloud computing environments

The deep integration of cloud computing and enterprise big data significantly enhances resource efficiency and business agility. However, the inherently open, shared, and virtualized nature of cloud environments also introduces security threats rarely encountered in traditional IT systems [6]. These risks not only jeopardize the confidentiality, integrity, and availability of corporate data but may also undermine competitive advantage and compliance standing [6,7]. This section systematically analyzes three core security risks facing enterprise big data in cloud environments.

3.1. Risk of data breaches

Data leakage represents one of the most common and damaging security issues in cloud environments. Its primary causes include: (1) Misconfigurations are the most frequent cause. For example, over-permissive default settings in object storage services can easily lead to public exposure of sensitive data if enterprises fail to apply detailed configurations following the principle of least privilege. (2) Supply chain attacks have emerged as a new threat vector. Vulnerabilities in third-party applications, APIs, or open-source components relied upon by enterprises can be exploited by attackers as entry points to infiltrate core data environments. (3) Internal threats also play a critical role. Employees with data access privileges may cause leaks either unintentionally (e.g., accidental file uploads) or maliciously (e.g., data theft).

3.2. Risk of unauthorized access

Unauthorized access primarily stems from failures in identity authentication and permission management. In cloud environments, identity has replaced the network perimeter as the core of security. Weak authentication is a common vulnerability. If only username and password are used without multi-factor authentication (MFA), attackers can easily steal identities through methods such as credential stuffing [6]. Overly broad permission assignments also pose significant risks. For

DOI: 10.54254/2755-2721/2026.TJ28888

administrative convenience, enterprises often assign users permissions beyond what is necessary, violating the principle of least privilege. A compromised high-privilege account can lead to severe data exposure. Furthermore, traditional IP-based static access policies struggle to adapt to the dynamic nature of microservices and containers in the cloud, potentially resulting in unauthorized services accessing data [8].

3.3. Risk of cloud platform vulnerabilities

Due to their complex architecture and multi-layered dependencies, cloud platforms possess inherent security weaknesses, which primarily include: (1) Virtualization Layer Vulnerabilities Pose Foundational Risks: Security flaws in virtualization components such as hypervisors may allow attackers to breach isolation constraints and access other tenants' data—a scenario known as "virtual machine escape" [8]. API Interfaces Represent a Common Attack Surface: Cloud services heavily rely on APIs for management and operations. If these interfaces suffer from unauthorized access or injection vulnerabilities, attackers can exploit them to infiltrate the system. (2) Shared Technology Model Introduces the "Noisy Neighbor" Effect: In multi-tenant environments where physical resources are shared, defects in isolation mechanisms may allow one user's activities to adversely affect the performance and security of others. (3) Cloud Management Console Vulnerabilities Are Highly Critical: The console possesses the highest level of privileges. If compromised, attackers could gain control over the entire cloud environment [8].

4. Analysis of the causes of security risks

4.1. Technical deficiencies

Ineffective access control mechanisms also represent a major concern. In complex cloud environments, traditional static boundary-based controls are often inadequate, leading to widespread over-provision of permissions and violations of the principle of least privilege. Additionally, the insufficient adoption of multi-factor authentication (MFA), coupled with weak passwords or compromised credentials, makes identity impersonation easier to execute [8]. Furthermore, inadequate security auditing and monitoring capabilities are frequently observed. Many organizations lack end-to-end real-time monitoring and unified log analysis in their cloud environments. Dispersed logs and insufficient correlation analysis make it difficult to detect anomalous behavior in a timely manner, delaying responses to data leaks, misuse, or external attacks [7].

4.2. Vulnerabilities in management systems

While advanced technologies rely on effective management for implementation, deficiencies in management are a primary cause of many security incidents. On one hand, there are shortcomings in full data lifecycle management. Many enterprises fail to classify and categorize data effectively, resulting in a lack of differentiated protection for information of varying sensitivity levels. Throughout the stages of data creation, storage, usage, sharing, and destruction, clear security protocols are often absent, with migration and destruction phases being particularly vulnerable to leakage. On the other hand, security policies and procedures are incomplete. After migrating services to the cloud, many organizations neglect to develop or adapt security policies suitable for cloud environments. Ambiguous responsibility assignments, missing or outdated contingency plans, and irregular daily operations further exacerbate risks. Inadequate risk assessment and management

DOI: 10.54254/2755-2721/2026.TJ28888

of third-party suppliers also increase the potential for supply chain attacks. Furthermore, a shortage of professionals and weak security awareness remain significant issues. The lack of cloud security expertise, coupled with slow skill updates among existing IT staff, leads to frequent misconfigurations. More broadly, insufficient employee security training makes staff susceptible to phishing attacks or operational errors, creating critical security gaps [7].

4.3. Ambiguity in legal liability definitions

The cross-border nature of cloud services introduces significant complexity in legal and compliance matters. A primary issue is the misunderstanding of the shared responsibility model. Under different service models such as IaaS, PaaS, and SaaS, cloud providers and users bear distinct security responsibilities. Many enterprises mistakenly assume that "moving to the cloud ensures security," shifting full responsibility to the service provider while neglecting their own obligations in data security and identity management, resulting in critical security gaps [1]. Secondly, cross-border data flows face legal conflicts. When operations involve data storage and processing across multiple countries, enterprises must comply with varying jurisdictional requirements as well as the EU's GDPR. Differences in regulations concerning data export, privacy protection, and other aspects can lead to high compliance costs and legal risks. Lastly, lagging and incomplete compliance standards pose practical challenges. The rapid development of cloud computing and big data technologies has outpaced updates in relevant laws, regulations, and national standards. In some areas, the absence of clear and unified mandatory security standards forces enterprises to navigate compliance independently, increasing operational uncertainty.

5. Strategies for security risk prevention and control

5.1. Technical prevention and control measures

Technical measures form the foundational approach to ensuring data security, with a focus on implementing protection throughout the entire data lifecycle. The foremost priority is strengthening data encryption and key management. For data at rest, high-strength encryption algorithms should be applied. Enhancing identity authentication and fine-grained access control is critical. The principle of least privilege should be fully implemented to eliminate over-provisioned permissions. Widespread deployment of Multi-Factor Authentication (MFA) enhances account security and prevents identity theft. In terms of control models, dynamic permission strategies such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC) should be adopted to achieve more refined resource access management [9].

5.2. Management-based prevention and control

A well-structured management system is essential to ensure the effective implementation of technical measures and to enhance organizational security resilience. Key initiatives include establishing a security management process for the entire data lifecycle. Enterprises should begin by classifying and categorizing data to implement differentiated protection based on sensitivity levels. Security requirements and responsibilities must be clearly defined for each phase—from creation, storage, and usage to sharing and destruction—with particular emphasis on standardizing secure procedures for data migration and disposal [9]. Additionally, it is critical to develop and regularly test an incident response plan, conduct regular organization-wide cybersecurity training to improve

DOI: 10.54254/2755-2721/2026.TJ28888

awareness of cloud policies, phishing attacks, and compliance requirements—empowering employees to become active participants in defense.

5.3. Legal and standards-based prevention and control

Laws and compliance requirements form the normative framework and legal basis for corporate security practices. Enterprises must strictly adhere to regulations such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law [9]. From a technical implementation perspective, they should follow national standards like the Multi-Level Protection Scheme (MLPS 2.0) and Security Capability Requirements for Cloud Computing Services (GB/T 31168) to ensure compliance capability building [7]. It is essential to clarify the shared responsibility mechanism with cloud service providers. Companies must clearly understand the division of security responsibilities between themselves and providers under different service models (IaaS, PaaS, SaaS) to avoid security gaps. Generally, providers are responsible for the security of the cloud (i.e., the underlying infrastructure), while users are responsible for security in the cloud (i.e., data, identity, and access management). Furthermore, cross-border data flows must be strictly regulated. Compliance assessments must be conducted for any data exit, with priority given to storing data domestically. When cross-border transfer is necessary, enterprises should use lawful channels such as security assessments, certifications, or standard contractual clauses to mitigate legal risks [9].

6. Conclusion

This study systematically analyzes security risks and mitigation strategies for enterprise big data in cloud environments, focusing on three core questions. Three major risk categories are identified: data breaches, unauthorized access, and cloud platform vulnerabilities. These are inherent to the cloud's open and virtualized architecture, often interconnected and more damaging than in traditional IT settings. The research reveals that risks stem from the interplay of technical flaws, management failures, and legal ambiguities. These factors collectively form systemic vulnerabilities.

A multidimensional control framework is proposed. Technologically, it advocates end-to-end encryption, multi-factor authentication, and zero-trust architecture. Managerially, it emphasizes data classification, least privilege, and incident response planning. Compliantly, it requires adherence to regulations like China's Data Security Law and clarified responsibility models. Study limitations include a focus on large enterprises, with less coverage of SMEs and specific sectors, limiting generalizability. Proposed strategies also require further empirical validation. Future research should expand case coverage, test strategies in real-world pilots, and explore threats from new technologies like AI and quantum computing. Additionally, cross-border data flow compliance and AI-powered active defense systems warrant in-depth investigation. Enterprises should adopt a dynamic, adaptive security governance approach that integrates technical and managerial measures to ensure continuous data protection throughout cloud-enabled digital transformation.

References

[1] Feng, D., et al. (2011). Research on Cloud Computing Security. Journal of Software, 22(1), 71-83.
[2] Sun, L., et al. (2014). Research Progress on Big Data Security and Privacy Protection. Chinese Journal of Computers, 37(1), 1-27.
[3] Li, T., et al. (2012). Research on Data Security Storage and Access Control Mechanism in Cloud Computing. Computer Science and Exploration, 6(5), 385-394.

DOI: 10.54254/2755-2721/2026.TJ28888

[4] Li, H., et al. (2013). Cloud Computing Security: Architecture, Mechanisms and Models. Chinese Journal of Computers, 36(3), 440-452.
[5] Wei, Q. (2024, March 15). Broad Prospects for the Cloud Computing Industry. China Economic Net. [Newspaper Article]
[6] Suo, Y. (2022). A Preliminary Study on Major Security Risks and Countermeasures in Cloud Computing Services. China Information Security, (4), 88-90.
[7] China Electronics Standardization Institute. (2023). Security Guide for Cloud Computing Services: GB/T 31167-2023 [National Standard of the People's Republic of China].
[8] Zhu, X., et al. (2024). Data Security Risks and Suggestions for Cloud Computing Services. China Information Security, (2), 95-98.
[9] Ministry of State Security of the People's Republic of China. (2025). Beware of Leaks! Risks in Uploading to the "Cloud"! [Online Report], February 28. Retrieved from https: //www.mss.gov.cn