Research on the Security Protection of Enterprise Financial Data in the Cloud Computing Environment: Taking Aliyunsec as an Example

Yukun Liu[a]
School of Foreign Languages, Shanghai Maritime University, 200135, Shanghai, Harbor Main Road, China

Keywords: Financial Cloud, Data Security, Cloud Computing.

Abstract: With the continuous advance of financial technologies, financial cloud has been adopted on a large scale and cloud financial data security of enterprises has garnered increasing attention. But diverse data breach methods and rapidly evolving vulnerability attack techniques have gradually made the traditional self-defense strategies and sketchy filtering abilities ineffective. In order to explore as many solutions for protecting cloud financial data from risks as possible, this study takes Aliyunsec, a top CWPP market share leader for three consecutive years, as an exemplary case. By analyzing its multi-layered protection strategies, which mainly include encryption, access control, and threat detection, this study proposes a systematic framework for cloud security providers. Findings of this case demonstrate the outstanding efficacy of Aliyunsec's strategy system composed of multi-layered encryption, Cloud Bastionhost access management, and AI-powered large model detection. This case in study offers strategic and technological reference value for advancing cloud data security capabilities.

1 INTRODUCTION

With the acceleration of financial digital transformation, cloud computing technology has held an irreplaceable position in financial technologies due to its distinctive advantages of elastic scalability, cost-effectiveness, and collaborative convenience. Numerous enterprises have flexibly adopted cloud computing to optimize traditional financial accounting processes and operational efficiency. However, in accordance with the financial accounting industry's stringent requirements for data security, while cloud service providers seize business opportunities to develop cloud computing platforms, the security and confidentiality of these platforms have raised deep concerns among financial accounting professionals regarding data protection risks in cloud-based accounting environments. Thus, mitigating security risks for financial accounting data has become a key future research priority for cloud computing developers.

Given that most cloud security providers in the market have failed to establish a comprehensive and systematic foundational security architecture, this study chooses Aliyunsec—the CWPP market share leader for three consecutive years—as the case to research. By examining Aliyunsec's practical data and protecting cases in financial accounting data security protection as an industry-leading example, this study aims to explore its technological distinctiveness and methodological innovations. The research seeks to summarize technical approaches for financial accounting data security, providing actionable insights and exploratory directions for other cloud-based financial data security providers about system architecture design and the application of emerging technologies in cloud security frameworks.

2 THE SECURITY OF FINANCIAL ACCOUNTING DATA IN CLOUD COMPUTING ENVIRONMENT

2.1 The Three Security Elements of Financial Accounting Data

The security of financial accounting data in cloud computing environment is mainly influenced by three

[a] https://orcid.org/0009-0006-1184-1878

Liu, Y.
Research on the Security Protection of Enterprise Financial Data in the Cloud Computing Environment: Taking Aliyunsec as an Example.
DOI: 10.5220/0013833400004719

In *Proceedings of the 2nd International Conference on E-commerce and Modern Logistics (ICEML 2025)*, pages 94-101
ISBN: 978-989-758-775-7

elements, confidentiality, integrity, and availability. Confidentiality mandates means data access exclusively to authorized personnel (Mark Stamp, 2023). Integrity requires system to prevent or detect unauthorized data modifications (Mark Stamp, 2023). Availability ensures that authorized users can maintain uninterrupted access to data resources for legitimate operations whenever they need (Mark Stamp, 2023).

2.2 The Impact of Cloud Computing on Financial Accounting Data Security

2.2.1 Changes in Data Storages and Transmission Modes

Due to the fundamental alignment of data acquisition channels between traditional management accounting and financial accounting, where core data directly or indirectly reflect enterprise operational activities, this structural synergy has evolved into a dominant trend in financial development with the help of leveraging cloud computing platforms' data-sharing capabilities (Wang Fang. 2020).

The storage methods for financial data have transitioned from physical vouchers and invoices to digital files, achieving cost reduction in physical storage expenditures. Meanwhile, the transmission modes have changed into online sharing mechanisms and cloud data transfers, which not only facilitate real-time verification accessibility but also eliminate convention costs.

2.2.2 Potential Risks Brought by the Application of Cloud Service Platforms

When the cloud service platforms have been commonly used, three potential risks demand more critical scrutiny: First, cloud data storage causes more financial data breaches and malicious alterations, predominantly attributable to algorithmic vulnerabilities and unauthorized intrusions (Sandesh Achar. 2018). Second, vast service range and imperfect international law increase difficulties in cross-border legal enforcement (Xu Ziyi, 2022). Third, insufficient training easily leads to errors and low efficiency even if financial cloud computing platforms have been used.

3 OVERLOOK OF ALIYUNSEC

3.1 Basic Frameworks of Aliyunsec

Since establishing in 2009, Aliyunsec has maintained strategic focus on advancing cloud computing establishment and reinforcing cyber defense infrastructures. As an industry pacesetter, Aliyunsec has delivered substantial contributions to China's cloud data security domain through its advanced security construction and adaptive threat mitigation frameworks. Its technological progress, characterized by persistent innovation in defense mechanisms, establishes critical reference value for industry counterparts in cybersecurity capability development.

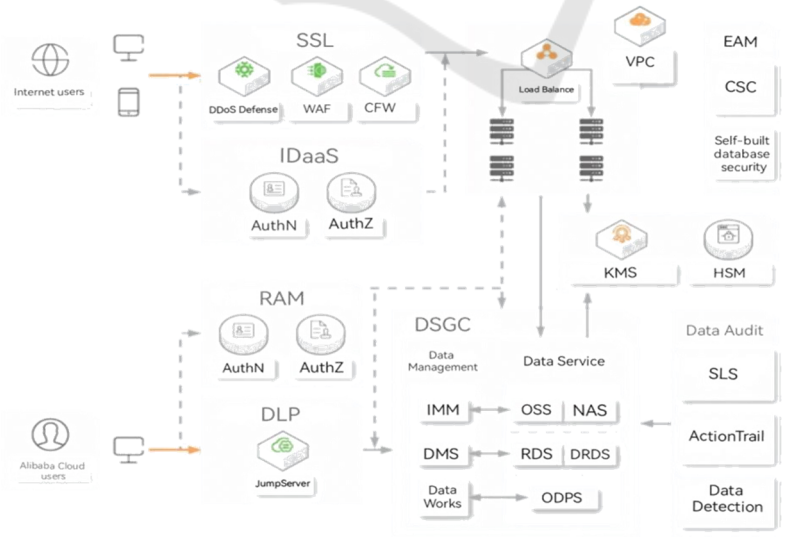

Figure 1: Aliyunsec data security solution (Aliyunsec, 2020).

As is shown in Figure 1, Key Management Service (KMS) is a key-oriented security protection method, which can help produce, store, verify, control and manage the keys and financial data encrypted by keys. The newly added Extensible Key Management (EKM) of Aliyunsec can significantly improve the controllability of keys (Mir Ali Rezazadeh Baee et al., 2024).

Besides, Aliyunsec users with certification services including managing and arranging Aliyunsec's SSL certifications or private certifications. Secure Sockets Layer (SSL) constitutes a transport-layer cryptographic protocol specifically designed to secure data-in-transit through digital certificate mechanisms. Its operational foundation lies in public-key cryptography implementations, where asymmetric encryption algorithms authenticate communication endpoints and negotiate session-specific encryption parameters (Leonard W. Wakoli, 2024). Aliyunsec also increases the technological support for rapid deployment of certification and unified management of multiple accounts.

In addition, Aliyunsec delivers diverse encryption solutions, including Transparent Data Encryption (TDE) mechanisms that perform real-time cryptographic processing of Input/Output operations (I/O) for cloud-hosted databases like RDS (Evaristus Didik Madyatmadja et al., 2021); cloud disk encryption which guarantee the unavailability of leaked data by adopting block storage infrastructure to encrypt the whole data disk; etc.

3.2 The Position of Aliyunsec in Cloud Computing Security Providers

Aliyunsec has spearheaded the establishment of the Cloud Security Consortium, a multi-stakeholder framework that substantially advances collaborative risk mitigation in cloud production systems. This initiative not only operationalizes collective defense mechanisms against platform-level vulnerabilities but also embodies the organization's strategic commitment to co-evolutionary cloud ecosystem development.

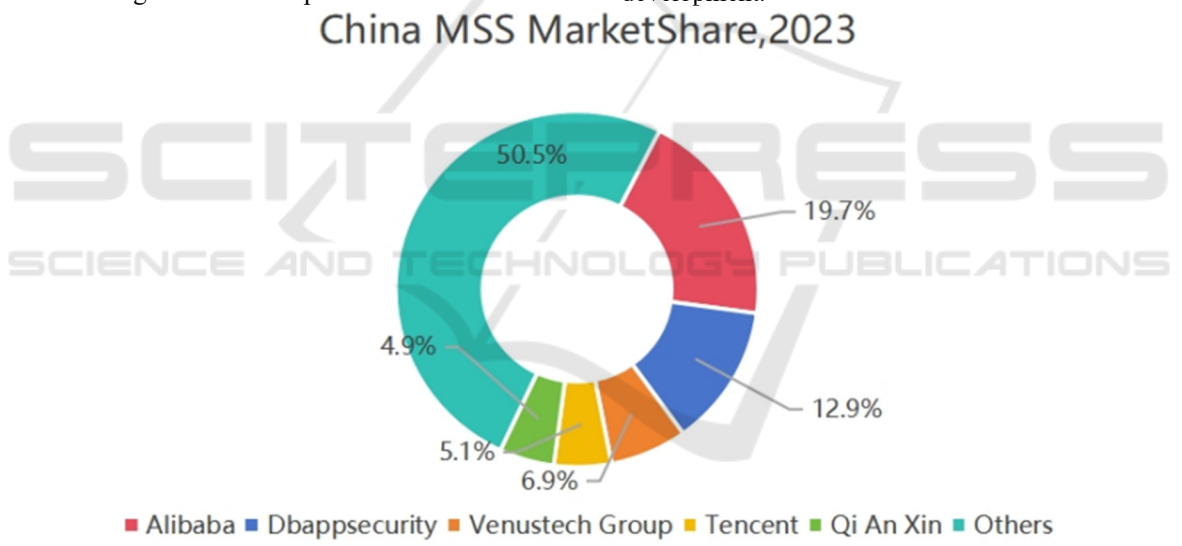

Figure 2: IDC China's cloud hosting security service market share ratio (IDC, 2024).

According to data from Figure 2, Alibaba ranks first in China's cloud hosting security services market share, demonstrating its leadership in cloud platform data security protection applications in China and even globally. Aliyunsec is regarded as one of the key pioneers for data security in cloud service platforms due to its forward-thinking vision and exceptional technological capabilities.

4 STRATEGIES AND CASES OF ALIYUNSEC IN FINANCIAL ACCOUNTING DATA SECURITY PROTECTION

4.1 Financial Accounting Data Encryption Strategies

Aliyunsec designs Figure 3, which exhibits Aliyunsec’s basic encryption framework.

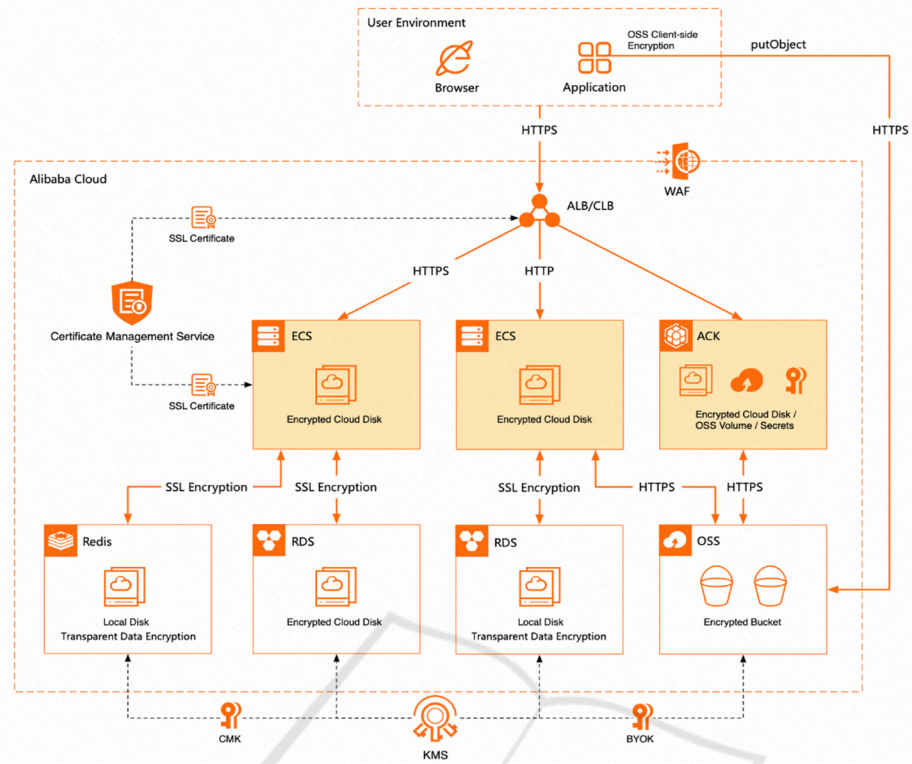

Figure 3: Aliyunsec financial data transmission encryption scheme (Aliyunsec, 2024).

Among it, the KMS service mainly forms the data storage encryption and updates EKM service in 2025. Besides, KMS provides encryption capabilities encompassing Object Storage Service (OSS) server-side/client-side encryption and Elastic Compute Service (ECS) system disk/data disk encryption. Its main function is summarized in Figure 4.

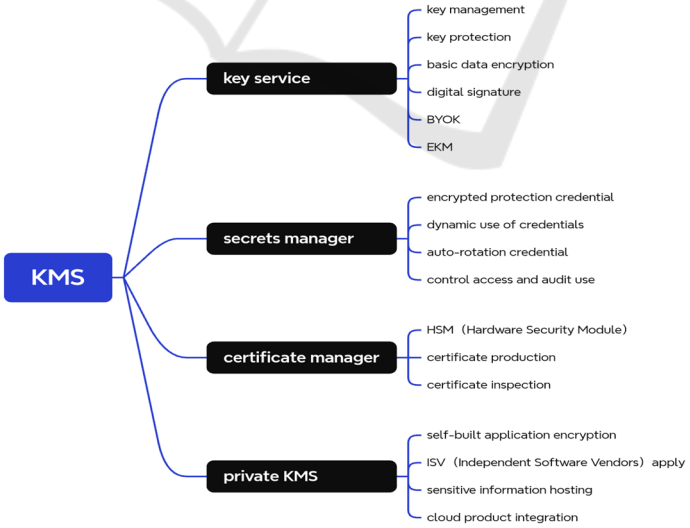

Figure 4: Services served in Aliyunsec KMS (Photo credit: Original).

Furthermore, Aliyunsec adopts Hypertext Transfer Protocol Secure (HTTPS) protocol secures data transmission between clients and Aliyunsec web-based business applications, enterprise applications, and OpenAPI interfaces; SSL-secured tunnels encrypt network data transmission during

connectivity establishment; OSS implements client-server encryption.

4.2 Access and Control Strategy

In order to strictly control the authority and operation of data access personnel and relevant people, Aliyunsec establishes Bastionhost.

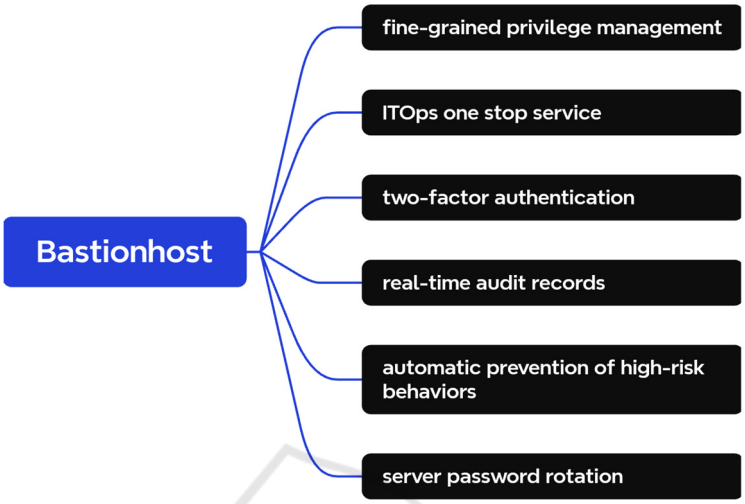

Figure 5: Main functions of aliyunsec bastionhost (Photo credit: Original).

Bastionhost offers six functions in Figure 5, which shows its enormous application advantages in fields with high data sensitivity requirements, like finance and economy. Bastionhost performs real-time monitoring and abnormal detection on Operation and Maintenance (O&M) servers while preventing privileged user overreach and sensitive data breach (Sahana Bailuguttu et al., 2023).

4.3 Strategies for Threat Detection and Prevention

Leveraging the Qwen AI model, Aliyunsec's Large Language Model (LLM) optimizes code instructions to reduce general risk identification costs by 80% while achieving 200% efficiency gains in annotation processes (Aliyunsec, 2024). Besides, after adding the integrating supervised fine-tuning (SFT) technology, Aliyunsec has achieved 44% accuracy gains in metaphorical analysis, 32% improvements among visual adversarial attacks, and 14% detection rate enhancements in adversarial advertising detection (Aliyunsec, 2024). Given the restrictions upon computing capability and memory, Aliyunsec chooses the Knowledge Distillation (KD) achieves latency reduction in LLM networks and financial data security reinforcement.

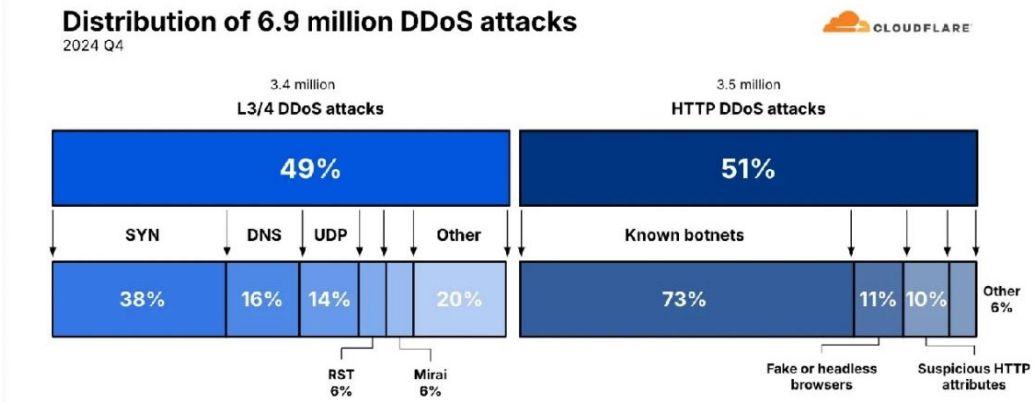

Figure 6: Distribution of DDoS attacks in the forth quarter of 2024 (Cloudflare, 2025).

From analysis of Figure 6, 2024 witnessed DDoS campaigns adopting Multi-Vector Precision-Strike Convergence (MVPSC) tactics against cloud infrastructures. Traditional Distributed Denial of Service (DDoS) countermeasures are hard to deal with these, prompting Aliyunsec's deployment of multi-layered anomalous traffic scrubbing with IP reputation shielding.

The Web Application Firewall (WAF) executes preventions including identifying and preventing malicious signatures from business traffic in networks or APPs, intercepting SQL-injection dominant attacks, mending vulnerabilities by virtual patches, automatically identifying and dealing with risks of data or assets, and dynamically updating through AI learning and real-time cases (Muhammad Annaset et al., 2024).

4.4 Enterprise Case

4.4.1 Basic Information About Enterprise

Changan Automobile, China's automotive flagship enterprise, expects to cooperate with Aliyunsec to ensure the security of users' and enterprise's data and assets during its Customer Data Platform (CDP) system migration and operation.

4.4.2 Situations and Challenges in Financial Data Security Before Adopting Aliyunsec

Changan Automobile requires CDP system construction and security protection to deliver stable personalized services for vehicle owners, safeguard owner privacy data along with internal financial and automotive manufacturing data, and ensure CDP system compliance. The massive data volume, complex transmission channels, and stringent security requirements pose significant challenges to Aliyunsec's protection capabilities.

4.4.3 Aliyunsec's Deployment and Configuration Process

Aliyunsec designed Changan Automobile's customized CDP platform to meet requirements, employing encryption methods like SSL encryption to secure data transmission, implementing APP-side key encryption with KMS service for privacy protection, and deploying Bastionhost for unified O&M control, which achieves 10% O&M efficiency improvement (Aliyunsec, 2023). Fine-grained access control with data encryption reduces code vulnerability incidents by 30% (Aliyunsec, 2023). The Data Security Center (DSC) converges Al security LLMs enabling real-time threat detection and active suppression.

5 CHALLENGES AND COUNTERMEASURES IN CLOUD COMPUTING APPLICATIONS

5.1 Technological Challenges and Strategies

5.1.1 Compatibility Issues with Existing Financial Systems of Enterprises

Currently, enterprises have accumulated substantial business transaction data across diverse platforms and software categories through the evolution of computerized accounting systems. Some have even made customized adjustments to their websites. For better adaptation to emerging technologies, data security protection must ensure the safety of existing cloud platforms, software, and program data while addressing potential code vulnerabilities and clearing data transmission traces during technological integration. Furthermore, considering the software differences between subsidiaries and departments within large enterprises, cross-regional and cross-domain compatibility challenges, along with security risks in unified management of cloud platforms, impose specific technical and experiential requirements on financial data security solution providers. Others may emulate successful data protection cases and introduce AI technologies to develop specialized LLMs for compatibility resolution.The "Cloud Security Community" concept proposed by Aliyunsec serves as a preventive measure against potential compatibility issues, offering referential value for future implementations.

5.1.2 Effects of Security Functions in Complex Network Environments

To fulfill departmental requirements, financial accounting data security services must encompass multiple protective dimensions: encrypted storage for financial data itself, client/server-side encryption capabilities, secure transmission channels across diverse software platforms, user authentication mechanisms, and permission management systems for IT personnel. Given the extensive scope of these security strategies, cloud platform protection services

must simultaneously ensure data integrity while minimizing network bandwidth consumption during code execution – a dual requirement posing significant challenges for technical teams in code optimization and strategic resource allocation. After consulting Aliyunsec's security framework, enterprises could adopt hierarchical control models to distribute bandwidth usage efficiently. Continuous refinement of these security protocols remains imperative, with iterative program enhancements serving as an ongoing operational priority.

5.2 Challenges and Strategies for Management

5.2.1 Improvements in Staff Training and Security Consciousness Cultivation

The security protection of financial accounting data cannot be thoroughly resolved solely by enhancing technologies. For new employees and some senior staff, inadequate proficiency in cloud platform operations may compromise business processing efficiency, while increasing risks of operational errors or vulnerability exposure. Additionally, during initial adoption of cloud platforms for financial operations, unclear division of responsibilities within finance departments frequently leads to mismatches between employee authority and real-time job requirements (Zhou Pin, 2022). Therefore, advanced comprehensive training programs about cloud platform usage and data confidentiality awareness demonstrate measurable effectiveness in reinforcing security measures for financial accounting data within cloud environments.

5.2.2 Optimization and Management for Security Strategies

The ongoing cyber defenses between data attackers and cybersecurity defenders promotes continuous refinement of strategies on both sides, with conventional detection-based countermeasures being progressively phased out in favor of innovative adaptive protection mechanisms. This evolution is exemplified by DDoS mitigation techniques: While traditional DDoS attacks could be neutralized through bandwidth limitations, modern defense frameworks now employ AI-driven high-risk behaviors detection combined with precision traffic filtering and multi-layered inspection protocols. Such dynamic, intelligence-enhanced cloud security architectures necessitate real-time adaptive optimization of security protocols and governance capabilities to ensure robust protection for cloud-based financial accounting systems. The leaders of enterprises must accordingly prioritize the institutionalization of continuous security posture enhancement as a strategic imperative.

6 CONCLUSION

Differing from conventional non-distinctive security approaches, Aliyunsec adopts a precision-targeted collaborative defense model. Its unified control system integrates diverse protective strategies through AI LLM recognition, dynamically adjusting safeguards against financial data risks in cloud computing environments. This method reduces code redundancy while ensuring comprehensive data security, offering valuable insights for other cloud security providers. Additionally, enterprises should prioritize staff confidentiality training to collectively safeguard internal financial data. Aliyunsec's "Cloud Security Community" initiative fosters collaborative partnerships among security providers, enabling cross-enterprise strategy sharing and statistical analysis, which also establish a cooperative foundation for China's cloud data protection ecosystem.

While this research demonstrates progress, current case studies focus exclusively on Aliyunsec, revealing gaps in comprehensive financial data protection frameworks under massive kinds of cloud environments. Future studies could expand the scope by including diverse case analyses and refining cloud-based financial data protection protocols. As cloud security evolves, emerging technologies will enhance defense systems by automating optimizations and reducing manual workloads. Meanwhile, security providers are expected to deepen collaborative efforts through specialized risk-response teams targeting specific vulnerabilities, collectively strengthening cloud data protection infrastructures.

REFERENCES

Achae, S. (2018). *Security of accounting data in cloud computing: A conceptual review*. Asian Accounting and Auditing Advancement, 2018(9), 60-72.

Aliyunsec. (2023). *Changan Automobile X Alibaba Cloud, aiming at hybrid cloud "research and operation integration" security*. https://mp.weixin.qq.com/s/hTWozKhrJPeYWzBPhUul4A

Aliyunsec. (2024). *What is the experience of using AI for*

cloud security? Alibaba Cloud's security AI capabilities exposed. https://mp.weixin.qq.com/s/hTWozKhrJPeYWzBPhUul4A

Annas, M., Adek, R. T., Afrillia, Y. (2024). *Web Application Firewall (WAF) Design to Detect and Anticipate Hacking in Web-Based Applications*. JACKA, 2024(1), 52-58.

Baee, M. A. R., Simpson, L., Armstrong, W. (2024). *Anomaly detection in the key-management interoperability protocol using metadata*. IEEE Open Journal of the Computer Society, 2024(5), 156-169.

Bailuguttu, S., Chavan, A. S., Pal, O., Sannakavalappa, K. (2023). *Comparing performance of bastion host on cloud using Amazon web services vs terraform*. Indonesian Journal of Electrical Engineering and Computer Science, 2023(30), 1722-1728.

Leonard W. W. (2024). *Secure Sockets Layer/Transport Layer Security for e-commerce*. IJSRM, 12(12), 8047-8052

Madyatmadja, E. D.,Hakim, A. N., Sembiring, D. J. M. (2021). *Performance testing on Transparent Data Encryption for SQL Server's reliability and efficiency*. Journal of Big Data, 2021(8), 134.

Stamp, M. (2023). *Principles and Practices of Information Security (3rd Edition)*. Beijing: Tsinghua University Press.

Wang, F. (2020). *Research on the Integration of Management Accounting and Financial Accounting under the Background of "Big Data and Cloud Computing"*. Business Accounting, 2020(15), 89-91.

Xu, Z. (2022). *International law protection of cross-border transmission of personal information based on cloud computing and big data*. Mobile Information Systems, 2022(9), 1-9.

Zhou, P. (2022). *Exploration of risk analysis and prevention strategies for enterprise cloud accounting applications*. Commercial Accounting, 2022(3), 70-74.