Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Addressing the Challenges of Data Security and Privacy in Cloud-Based Financial Systems

Nagesh Shenisetty
FedEx Express, USA
Corresponding Author: Nagesh Shenisetty, **E-mail**: reachshenisetty@gmail.com

| ABSTRACT

Cloud computing has brought about a paradigm shift in the financial sector, delivering enhanced scalability, economic efficiencies, and greater operational flexibility. Nevertheless, this technological evolution introduces considerable security and privacy imperatives that financial institutions must diligently confront. This analysis will delve into the distinct security hazards confronting cloud-integrated financial infrastructures, encompassing data breaches, sophisticated persistent threats, and susceptibilities inherent in multi-tenant architectures. Furthermore, it will examine the intricate regulatory framework, where mandates such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and cross-border data transfer limitations significantly influence cloud deployment decisions. This discourse will also articulate crucial data safeguarding methodologies, including encryption, tokenization, and the zero-trust paradigm, in conjunction with robust identity and access management protocols like multi-factor authentication and privileged access management. Finally, it will elaborate on the comprehensive monitoring, detection, and incident response capabilities vital for upholding security within cloud environments, underscoring the pivotal role of Security Information and Event Management (SIEM) systems, behavioral analytics, and automated incident remediation workflows in protecting sensitive financial information.

| KEYWORDS

Cloud security, Financial compliance, Data protection, Identity management, Threat detection

| ARTICLE INFORMATION

ACCEPTED: 01 May 2025 **PUBLISHED:** 30 May 2025 **DOI:** 10.32996/jcsts.2025.7.5.31

1. Introduction

The financial services sector is experiencing a profound metamorphosis, propelled by the widespread integration of cloud computing technologies. Financial institutions are increasingly leveraging cloud infrastructure for critical operations, including transaction processing, customer data storage, and the provision of digital services. Scholarly research indicates that cloud technology is fundamentally reshaping banking paradigms, with projections suggesting that financial institutions will evolve into more interconnected, open, intelligent, and experiential entities by the year 2030, thereby catalyzing the next generation of financial service delivery [1]. This transformative journey necessitates that financial institutions strike a delicate equilibrium between fostering innovation and implementing rigorous security protocols as they migrate pivotal functions to cloud platforms.

While adopting cloud solutions presents many advantages, notably enhanced cost-effectiveness, superior scalability, and amplified operational agility, it concurrently introduces intricate security and privacy dilemmas that demand meticulous attention. Research findings reveal that the financial services industry has incurred the highest average cost per data breach, amounting to $4.62 million, a figure significantly exceeding the global cross-industry average of \$4.45 million [2]. These financial ramifications are even more substantial for large-scale financial enterprises, underscoring the paramount importance of deploying exhaustive security measures within cloud environments.

As financial institutions transition from conventional on-premises infrastructures to dynamic cloud environments, they must adeptly navigate a novel and evolving landscape of security threats and stringent compliance mandates. Research underscores the imperative for financial institutions to embrace cloud technologies to formulate a strategic and well-defined roadmap for cloud migration, one that intrinsically incorporates robust security controls and meticulous consideration of regulatory stipulations [1]. Concurrently, research analysis highlights a concerning trend: data breach costs for financial organizations have escalated by 10.3% since 2020, with the average time to identify and contain a breach extending to 233 days. This escalating risk profile creates an undeniable urgency for the implementation of enhanced security frameworks across all cloud deployments within the financial sector [2].

2. Unique Security Risks in Cloud Computing for Financial Institutions

Financial institutions that operate in cloud environments encounter unique security challenges that necessitate specialized mitigation strategies. The centralization of sensitive financial data within cloud repositories makes them attractive targets for cybercriminals. The 2023 Data Breach Investigations Report reveals that the financial industry remains a primary target, with 637 incidents and 297 confirmed data breaches in the past year [3]. A successful breach can expose personally identifiable information (PII), account credentials, and transaction histories, with 95% of breaches in financial services motivated by financial gain and 60% involving compromised credentials that enable unauthorized access to sensitive data.

Advanced Persistent Threats (APTs) and multi-stage attacks are used by sophisticated threat actors to specifically target financial institutions. These attacks can go undetected for extended periods, allowing attackers to monitor activities and extract data gradually. While the global median dwell time for attackers has decreased to 16 days, Mandiant's M-Trends 2023 report indicates that financial institutions still experience longer dwell times due to the sophisticated nature of attacks targeting them [4]. The report highlights that 21% of security incidents involving cloud environments were caused by state-sponsored attackers who target financial institutions for both economic gain and strategic intelligence.

Distributed Denial of Service (DDoS) attacks are another significant threat to cloud-based financial services. These attacks can overwhelm network resources, disrupting critical customer-facing applications and transaction processing systems. Research shows that DoS attacks accounted for approximately 46% of all system intrusion incidents across industries [3], with financial services experiencing more targeted and sophisticated variations that specifically aim to disrupt high-value transaction processing during peak business hours.

Insider threats pose particularly challenging security problems for financial institutions. Privileged users within both the financial institution and the cloud service provider have potential access to sensitive data. Approximately 19% of breaches involved internal actors [3], with financial services seeing elevated risk due to the high value of the data being handled. These insider-originated incidents often bypass traditional security controls and can remain undetected for longer periods.

In shared cloud environments, multi-tenancy risks arise when vulnerabilities in the infrastructure potentially allow attackers to bypass isolation controls between different tenants. Research analysis of cloud security trends notes that attackers increasingly target cloud misconfigurations and develop specialized techniques to exploit shared infrastructure [4]. These attacks create risks of data leakage between organizations, with threat actors specifically focusing on environments where high-value financial data might be accessed.

Cloud services rely heavily on APIs for integration, creating additional attack surfaces that may be exploited. The report indicates that web applications were involved in 90% of breaches in the financial sector, with a significant portion involving API vulnerabilities [3]. These entry points can be exploited to gain unauthorized access to financial data or systems, requiring institutions to implement specialized security controls for their cloud-based interfaces.

Threat Type	Percentage	Additional Metric
Breaches Motivated by Financial Gain	95%	297 confirmed breaches in financial industry
Credential-Based Attacks	60%	Primary method of unauthorized access
DDoS/System Intrusion Attacks	46%	Most common disruption technique

State-Sponsored Attacks	21%	Target cloud environments specifically
Insider Threat Incidents	19%	Often bypass traditional controls
Web Application/API Exploits	90%	Most common entry point for breaches

Table 1: Prevalent Attack Vectors in Cloud-Based Financial Systems [3, 4]

3. Regulatory Compliance Challenges

Financial institutions must navigate a complex web of regulatory requirements when implementing cloud solutions. According to research analysis, the regulatory landscape for cloud adoption in financial services has evolved significantly, with 58% of regulatory authorities across 17 jurisdictions having issued specific guidance related to cloud outsourcing and risk management [5]. This regulatory fragmentation creates substantial compliance burdens for institutions operating across multiple regions.

The General Data Protection Regulation (GDPR) imposes strict requirements on data protection, including the right to be forgotten, data portability, and explicit consent for data processing. These requirements can be particularly challenging to implement in cloud environments where data may be distributed across different geographic locations. The research indicates that data protection and privacy regulations remain among the top barriers to cloud adoption in financial services, with 76% of surveyed institutions citing these concerns as significant obstacles [5]. The study further reveals that many financial institutions establish dedicated teams focused on maintaining GDPR compliance in their cloud environments.

Financial institutions processing card payments must ensure their cloud environments comply with Payment Card Industry Data Security Standard (PCI DSS) requirements. According to the 2023 The Payment Security Report, organizations face significant challenges in this area, with only 47.5% successfully achieving and maintaining PCI DSS compliance during validation [6]. The report highlights that Requirement 4 (encrypting transmissions of cardholder data) and Requirement 10 (tracking and monitoring access) present particular challenges in cloud environments, with compliance rates of 76.6% and 63.7% respectively.

Regulations such as the Gramm-Leach-Bliley Act (GLBA) in the United States, the Financial Services and Markets Act in the UK, and similar frameworks worldwide impose specific requirements on financial data handling. The analysis found that 43% of surveyed institutions reported difficulties in adapting their cloud strategies to accommodate varying interpretations of confidentiality requirements across different jurisdictions [5].

Many jurisdictions impose limitations on transferring financial data across national boundaries. The study reveals that data localization requirements exist in 68% of the jurisdictions analyzed, creating significant challenges for global cloud deployments [5]. These requirements often necessitate complex architectural solutions to ensure data sovereignty while maintaining operational efficiency.

Financial institutions must maintain comprehensive audit trails and reporting capabilities to demonstrate compliance. The research report notes that organizations struggle particularly with PCI DSS Requirement 11 (regularly testing security systems and processes) in cloud environments, achieving only a 63.3% compliance rate [6]. This challenge is compounded by the need to coordinate audit activities across multiple cloud service providers and environments, often requiring specialized monitoring tools and processes.

Regulatory Challenge	Percentage	Context
Regulatory authorities with cloud-specific guidance	58%	Across 17 jurisdictions
Financial institutions citing data protection as significant obstacle	76%	Major barrier to cloud adoption
Successful PCI DSS compliance achievement rate	47.5%	During validation assessments
PCI DSS Requirement 4 (encrypting transmissions) compliance rate	76.6%	Cloud environment specific
PCI DSS Requirement 10 (tracking and monitoring) compliance rate	63.7%	
PCI DSS Requirement 11 (testing security systems) compliance rate	63.3%	
Organizations reporting difficulties with confidentiality requirements	43%	Across different jurisdictions
Jurisdictions with data localization requirements	68%	Creating global deployment challenges

Table 2: Regulatory Hurdles for Financial Institutions in Cloud Adoption [5, 6]

4. Data Protection Strategies and Technologies

To effectively address the multifaceted security challenges inherent in cloud-based financial systems, institutions can strategically deploy a range of robust protection mechanisms that judiciously balance stringent security imperatives with essential operational exigencies. Pertinent research focusing on financial services within the cloud environment underscores that security apprehensions remain a paramount impediment to widespread cloud adoption, with a significant 91% of surveyed financial institutions identifying data protection as their foremost concern [7].

The implementation of comprehensive end-to-end encryption, encompassing both data at rest and data in transit, stands as a cornerstone for safeguarding sensitive financial information. A report by the Cloud Security Alliance (CSA) reveals that while a substantial 83% of financial institutions have adopted encryption for data in transit, a notable lacuna persists in achieving holistic encryption coverage, particularly for data residing in multi-cloud deployments [7]. Financial institutions should give due consideration to advanced cryptographic techniques, such as homomorphic encryption, which permits computation on encrypted data without the necessity of decryption. However, the CSA report also indicates that the adoption of this sophisticated technology within the financial sector remains in its nascent stages.

The strategic substitution of sensitive data elements with non-sensitive surrogates through the process of tokenization can substantially mitigate risk exposure while preserving data usability for critical processing and analytical functions. Research findings indicate that tokenization has evolved into a pivotal security strategy for 76% of financial institutions operating within cloud environments, proving particularly efficacious in shielding payment card details and personally identifiable information [7].

Furthermore, the deployment of Data Loss Prevention (DLP) solutions empowers institutions to identify and proactively prevent the unauthorized transmission of sensitive financial data beyond the defined organizational perimeter. Market research within the cloud security domain indicates a rapid growth trajectory for DLP solutions, with the overall cloud security market projected

to burgeon from USD 40.8 billion in 2022 to an impressive USD 77.5 billion by 2027, exhibiting a Compound Annual Growth Rate (CAGR) of 13.7% [8].

The convergence of network security functionalities with Wide Area Network (WAN) capabilities through the implementation of Secure Access Service Edge (SASE) frameworks facilitates secure access to cloud services irrespective of the user's geographical location. Market research highlights SASE as one of the most rapidly expanding segments within the cloud security landscape, demonstrating the financial sector's increasing inclination towards integrated security paradigms that effectively accommodate distributed workforces [8].

Deploying Cloud Access Security Brokers (CASBs) as strategic security policy enforcement junctures positioned between users and cloud services enables institutions to meticulously monitor user activity and rigorously enforce defined security policies. Cloud security market analysis identifies CASBs as a mission-critical component within the security architecture, with the market for these solutions anticipated to experience substantial growth through 2027 as financial institutions progressively embrace multi-cloud strategies [8].

Finally, the adoption of a "never trust, always verify" philosophy through the implementation of a Zero Trust Architecture necessitates stringent verification protocols for every user and device attempting to gain access to organizational resources. The CSA report underscores that a significant 67% of financial institutions have either already implemented or are actively in the process of implementing Zero Trust principles, recognizing its demonstrable effectiveness in safeguarding distributed cloud environments [7]. This security paradigm has gained particular salience as the traditional demarcations between internal and external networks continue to blur within cloud-based financial systems.

Data Protection Strategy/Technology	Adoption/Growth Rate	Additional Context
Financial institutions citing data protection as primary concern	91%	Top barrier to cloud adoption
Encryption for data in transit	83%	Widely implemented
Tokenization for sensitive data	76%	Critical strategy in cloud environments
Zero Trust Architecture implementation	67%	Either implemented or in process
Cloud security market size (2022)	$40.8 billion	Baseline measurement
Cloud security market size (projected 2027)	$77.5 billion	Future projection
Cloud security market CAGR	13.7%	Growth rate 2022-2027

Table 3: Data Protection Strategy Implementation in Financial Services [7, 8]

5. Identity and Access Management

Robust identity and access management is critical for cloud security in financial systems, serving as the cornerstone of data protection strategies. According to industry analysis, financial institutions face unique IAM challenges, with 63% of cybersecurity incidents in the banking sector involving compromised credentials and identity-related vulnerabilities [9].

Implementing Multi-Factor Authentication (MFA) for all access to financial systems and data has become essential, particularly for privileged accounts with administrative capabilities. Research indicates that MFA implementation significantly reduces the risk

of unauthorized access, with financial institutions reporting up to 99.9% fewer account compromise incidents after deployment [9]. This technology is particularly critical for cloud environments, where traditional network perimeters are less defined.

Establishing strict controls over privileged accounts through Privileged Access Management (PAM) solutions, including just-in-time access provisioning and comprehensive activity monitoring, helps prevent credential abuse. According to Sectona's analysis, PAM can help the finance and banking sector adapt to regulatory requirements like PCI DSS, GDPR, and SOX by controlling and monitoring access to critical systems and data [10]. Financial institutions implementing PAM solutions report enhanced compliance posture and significantly reduced audit findings related to access control.

Implementing automated processes for identity governance, including identity lifecycle management, access certification, and role-based access control, ensures that users have only the permissions necessary for their roles. IAM finance capabilities such as user authentication, authorization, and workflow automation enable banks and financial institutions to verify a user's identity before a transaction is processed [9]. This approach has proven particularly valuable in cloud environments, where entitlement management becomes increasingly complex.

Enabling secure identity federation between on-premises and cloud environments maintains consistent authentication and authorization controls across hybrid infrastructures. This capability is especially important considering that financial institutions typically manage hundreds of applications across multiple environments, with 87% operating in hybrid cloud scenarios [9].

Deploying continuous authentication technologies that monitor user behavior patterns can detect anomalies that might indicate compromised accounts. These technologies are increasingly important in the financial sector, where credential theft remains the primary attack vector. Behavioral analytics and continuous monitoring provide an additional security layer that complements traditional authentication methods [10].

The adoption of sophisticated biometric authentication modalities, encompassing facial recognition, fingerprint scanning, and behavioral biometrics, serves to fortify identity verification processes while concurrently enhancing the overall user experience. Privileged Access Management (PAM) solutions that integrate biometric factors empower financial institutions to attain a more robust security posture, effectively addressing the intricate challenges associated with cloud migration and broader digital transformation initiatives [10]. These cutting-edge technologies are particularly advantageous for securing high-stakes financial transactions and controlling administrative access to sensitive financial systems operating within cloud environments.

6. Monitoring, Detection, and Response

Financial institutions must establish comprehensive security monitoring capabilities to protect their cloud-based systems effectively. According to research analysis, financial services organizations face unique challenges in cloud environments, with 89% of respondents in a cloud security survey citing compliance requirements as a significant cloud security challenge [11].

Implementing Security Information and Event Management (SIEM) solutions that aggregate and correlate security events across cloud environments is essential for identifying potential security incidents. Financial services companies must monitor and log activities across their cloud environments to detect unauthorized access or suspicious behavior that could indicate a security breach. The research points out that comprehensive visibility across multi-cloud environments is particularly challenging, with many organizations struggling to achieve consistent monitoring coverage [11].

Deploying User and Entity Behavior Analytics (UEBA) solutions enables detection of anomalous user activities that might indicate account compromise or insider threats. According to Digital Defense Report, 80% of security breaches involve compromised identities, making behavior-based detection critical for financial institutions [12]. The report emphasizes how behavioral analytics helps identify subtle indicators of compromise that traditional rule-based systems often miss.

The persistent surveillance of cloud infrastructure configurations through the implementation of Cloud Security Posture Management (CSPM) solutions aids in the identification of security misconfigurations and deviations from established compliance mandates. Scholarly research underscores that misconfigurations constitute one of the most prevalent cloud security vulnerabilities for financial institutions, with frequently encountered issues including excessive permissions granted, the storage of sensitive data in an unencrypted state, and the inadvertent exposure of critical assets to the public internet [11]. CSPM solutions furnish the continuous visibility requisite for upholding secure configurations across the fluid and dynamic landscape of cloud environments.

The strategic integration of threat intelligence feeds empowers financial institutions to proactively discern nascent and evolving threats specifically targeting their sector. A recent research report indicates an alarming surge in password attacks, now reaching a staggering rate of 4,000 attempts per second, thereby emphasizing the critical need for timely and actionable threat intelligence to effectively anticipate and mitigate potential attack vectors [12]. Financial institutions derive significant benefits

from the acquisition and utilization of industry-specific intelligence, which directly addresses the unique and nuanced threats confronting their particular segment of the financial ecosystem.

Implementing automated incident response workflows helps contain and mitigate security incidents quickly. Research analysis reveals that the median time to remediate vulnerabilities has grown to 97 days, emphasizing the need for automation to accelerate response [12]. Automated playbooks for common incident types enable financial institutions to respond consistently and rapidly to security events across cloud environments.

Conducting regular penetration tests specifically designed for cloud environments helps identify and address vulnerabilities before they can be exploited. The research recommends that financial institutions implement a continuous testing approach rather than point-in-time assessments to match the dynamic nature of cloud environments [11]. These specialized tests should evaluate cloud-specific risks including identity management controls, API security, and containerized application vulnerabilities.

7. Conclusion

Financial institutions embracing cloud technologies confront the dual imperative of capitalizing on innovation while rigorously safeguarding sensitive customer data and adhering to stringent regulatory mandates. Establishing effective cloud security necessitates a multi-tiered strategy that synergistically integrates technological solutions with well-defined governance frameworks and robust operational practices. As the adoption of cloud services accelerates across the financial sector, institutions must implement all-encompassing protection strategies that incorporate robust encryption protocols, sophisticated identity management systems, and continuous, vigilant monitoring. The ever-evolving threat landscape demands the cultivation of proactive security postures, compelling organizations to consistently evaluate their existing security controls and adapt swiftly to emerging risks. Ultimately, those financial institutions that establish resilient cloud security foundations will be optimally positioned to harness the transformative benefits of cloud computing while preserving invaluable customer trust and meeting the escalating expectations of regulatory bodies within an increasingly intricate digital financial ecosystem.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Chris Tozzi, "4 Cloud Security Considerations for Financial Services Companies," Orca Security, 2023. [Online]. Available: https://orca.security/resources/blog/cloud-security-considerations-for-financial-services-companies/
[2] Cloud Security Alliance, "State of Financial Services in Cloud," Cloud Security Alliance, 2023. [Online]. Available: https://cloudsecurityalliance.org/artifacts/state-of-financial-services-in-cloud
[3] Deloitte, "Cloud banking: More than just a CIO conversation," Deloitte, 2023. [Online]. Available: https://www.deloitte.com/za/en/Industries/financial-services/perspectives/bank-2030-financial-services-cloud.html
[4] Deloitte, "Regulatory barriers to cloud adoption in financial services," Deloitte Financial Services Perspectives, 2022. [Online]. Available: https://www.deloitte.com/lu/en/Industries/financial-services/perspectives/regulatory-barriers-cloud-financial-services.html
[5] IBM Security, "Cost of a data breach 2024: Financial industry," IBM, 2024. [Online]. Available: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
[6] Jurgen Kutscher, "M-Trends 2023: Cybersecurity Insights From the Frontlines," Google Cloud Blog, 2023. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2023
[7] MarketsandMarkets, "Cloud Security Market by Offering (Solution and Services), Solutions (CASB, CWPP, CSPM, CDR, and CIEM), Services (Professional and Managed), Service Model (IaaS, SaaS, and PaaS), Type, Vertical, and Region - Global Forecast to 2028," MarketsandMarkets, 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-security-market-100018098.html
[8] Microsoft, "Microsoft Digital Defense Report," Microsoft Threat Intelligence, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports
[9] Sectona, "Privileged Access Management for Finance and Banking," Sectona, 2025. [Online]. Available: https://sectona.com/technology/pam-for-finance-and-banking-industry/
[10] Veritis, "5 Reasons Why Financial Sector Needs Identity and Access Management (IAM)," Veritis, 2025. [Online]. Available: https://www.veritis.com/blog/5-reasons-why-financial-sector-needs-identity-and-access-management-iam/
[11] Verizon Business, "2023 Payment Security Report: PCI DSS Compliance Insights," Verizon Enterprise Solutions, 2023. [Online]. Available: https://www.verizon.com/business/resources/whitepapers/2023-payment-security-report-pci/
[12] Verizon, "2023 Data Breach Investigations Report," Verizon, 2023. [Online]. Available: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf