International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Fortifying Financial Data and PII (Security Strategies for Public Cloud Environments)

Siva Kumar Mamillapalli

siva.mamill@gmail.com

Abstract

The financial sector has traditionally been cautious about adopting new technologies. However, with the significant benefits and opportunities that cloud adoption can offer, financial institutions are now prepared to embark on the cloud journey. This shift brings several challenges, particularly regarding the storage of sensitive financial data and personally identifiable information (PII) in public cloud environments. This research examines the challenges faced by financial institutions in storing such data in the public cloud and aims to develop best practices based on their experiences. Interviews were conducted with senior stakeholders from large UK organizations to gather insights from their real-world experiences, which were then compared with industry best practices. The paper concludes with valuable insights into best practices for securely storing sensitive data in the public cloud, providing guidance for other financial institutions making the transition.

Keywords: Public cloud, financial data, personally identifiable information (PII), cloud security, financial organizations, best practices for cloud security, data privacy, data protection.

1. Introduction

Cloud computing is rapidly gaining traction due to its advantages over traditional computing services. It offers resources such as processing power, storage, and other services on a pay-per-use basis for consumers. As the banking and financial services sector heavily relies on information technology, it stands to benefit significantly from cloud computing's advantages in cost, resiliency, and scalability, allowing for high-quality and cost-effective services to consumers.

However, a major challenge for financial institutions adopting cloud technology is ensuring the security of infrastructure and data stored in the public cloud. The rising number of cyberattacks, along with regulatory and compliance requirements regarding customer data privacy and Personally Identifiable Information (PII), complicate the adoption process. Furthermore, some organizations using the public cloud have expressed concerns about the security of PII, data breaches, and issues related to segregation of duties.

This research draws on real-life experiences regarding data security in public cloud implementations for financial institutions and provides best practices derived from these lessons.

1.1 Sensitive Data in the Public Clouds

Cloud computing offers easy, widespread, on-demand access to a shared pool of computing resources, such as networks, servers, storage, and applications, all of which can be configured through self-service admin portals provided by cloud service providers. The processing capacity of cloud infrastructure can be quickly scaled up or down as needed, with minimal manual intervention.

Although there is considerable research on various aspects of cloud adoption, few address the security challenges related to storing financial data and Personally Identifiable Information (PII) in the public cloud, along with the solutions to these issues. As many financial institutions globally transition to public cloud infrastructure, ensuring the secure storage of financial data and PII has become a critical but underexplored area for research, which this study aims to explore.

This research identifies best practices for securing financial data and PII in public cloud environments. The objectives of the study are as follows:

- Evaluate cloud adoption within financial institutions
- Assess the real-life security challenges faced by these institutions regarding PII and financial data
- Outline best practices drawn from lessons learned by financial institutions

The research primarily focuses on two key questions:

- Q1: Is it possible to develop a methodology for securely storing sensitive financial data and PII in the public cloud that also complies with relevant data protection regulations?
- Q2: How can the features provided by public cloud providers be best utilized to minimize security risks?

Literature Review

Cloud technology has revolutionized how computational resources are accessed. While many organizations aim to adopt cloud solutions, the fear of losing critical data is one of the reasons to be reluctant to move their infrastructure to the public cloud. This section reviews existing research on various aspects of cloud security challenges, the significance of personally identifiable information (PII), and best practices for securely storing sensitive data in public cloud environments. It also discusses the security challenges associated with cloud architecture, focusing on the different layers of cloud infrastructure, data storage concerns faced by organizations and provides high-level recommendations for mitigating these issues.

According to the GDPR, Personally Identifiable Information (PII) refers to “personal data related to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, especially through an identifier such as a name, identification number, location data, online identifier, or one or more factors related to the person’s physical, physiological, genetic, mental, economic, cultural, or social identity. The paper provides a detailed analysis of the impact of cyber activities on business operations through a systematic literature review. It proposes a framework for

conducting similar impact assessments for specific business scenarios and identifies gaps in the existing literature, suggesting areas for future research.

Company	People Affected (in Billion)	Cost of Data Breach (Mil $)
Yahoo	3	486
Equifax	147	1440
Anthem	78	406.5
Sony PSN	77	193
Home Depot	56	321

Table 1: Cost of some of data breaches

Cloud Security Strategy

Given the advantages offered by cloud infrastructure, it is inevitable that financial institutions will adopt cloud solutions sooner rather than later. As a result, cloud security, which includes processes, controls, and policies related to cloud infrastructure, systems, and data, becomes essential. In 2019, one in four organizations reported a security incident related to the cloud, and overall, 93% of organizations surveyed by Coalfire expressed moderate to extreme concern about the security of their systems and data in the cloud.

A comprehensive cloud security strategy is essential for protecting application data, ensuring regulatory compliance, and safeguarding customer data privacy, particularly for organizations transitioning to hybrid cloud environments. This strategy helps organizations reduce reliance on specific cloud providers, protect themselves from financial and reputational damage due to data breaches, and avoid the legal consequences of data loss.

The goal of a cloud security strategy should be to enhance the trustworthiness of an organization's cloud infrastructure by implementing critical capabilities to secure systems and data while ensuring global accessibility. It should be thorough enough to address both private and public cloud environments, as well as multi-cloud configurations, enabling a consistent security approach. Furthermore, the strategy should incorporate automation for the creation and enforcement of security policies, minimizing the risk of errors that may arise from manual processes. The primary focus should remain on three key areas—Infrastructure, Data, and People—in both private and public cloud environments.

Hence, the cloud strategy should address several factors, including authentication, access controls, user behavior, data classification, encryption, and logical data segmentation, while ensuring proper logging and reporting mechanisms are in place to monitor any unauthorized data access. The security strategy should also account for regulatory compliance requirements and provide protection against data breaches and insider threats.

Key principles for an effective cloud security strategy include:

- **Shared Responsibility** – Organizations should view hybrid cloud security as a shared responsibility. Relying solely on cloud service providers for securing critical data is risky, as it may lead to oversights and errors.
- **Proactive Approach** – Maintaining security requires proactively identifying potential risks and implementing effective mitigation strategies. Reacting to security incidents and recovering compromised systems and data can be difficult, even with the best cloud providers.
- **Standardized Processes** – Organizations should standardize processes across both private and public cloud environments to prevent manual errors and minimize security vulnerabilities.
- **DevSecOps** – Human errors in cloud environments can be reduced by codifying processes into workflows that can be triggered with a single click.
- **Zero-Trust Policy** – Traditional network perimeters are often ineffective in hybrid cloud environments, where data and processes are distributed across various locations and infrastructures. A "never trust, always verify" approach should be applied to secure access to all assets and data.
- **Uniform IAM Framework** – The Identity and Access Management (IAM) framework should follow the principle of least privilege across both private and public cloud infrastructures.
- **Data Protection** – Data protection strategies, such as encryption, tokenization, and pseudonymization, should be implemented as standard practices in any cloud environment where feasible.

Shared Responsibility Model:

Given the distributed nature of cloud infrastructure, with systems and components spread across multiple organizations and geographic locations, it is impractical to centrally control security aspects through a single entity. Therefore, the responsibility for managing the security of the entire end-to-end infrastructure is shared between the consumer and the cloud service provider.

The following image illustrates a high-level framework for the shared responsibility model across IaaS, PaaS, and SaaS cloud setups.

- **People**: The organization is responsible for managing identity and access, including authentication, authorization, MFA, SSO, certificates, access keys, and password management.
- **Data**: The organization controls data usage and access; the cloud service provider has no visibility into the data.
- **Virtual Networks**: For PaaS and SaaS, the cloud provider manages the network. For IaaS, the organization is responsible for security configuration and monitoring.
- **Hypervisors**: The cloud provider controls virtualization, including provisioning physical resources and ensuring isolation.
- **Servers and Storage**: The cloud provider owns and secures physical servers and storage, handling their security configuration and monitoring.
- **Physical Networks**: The cloud provider manages and secures physical networks and controls access.

- **Applications**: Except for SaaS, the organization manages and secures applications, including code repositories, regular testing, and access control throughout the software development lifecycle.
- **Operating System**: In IaaS, the organization secures and controls the operating system. For PaaS and SaaS, the cloud provider manages the operating system.

Identity and Access Management (IAM)

Identity and Access Management (IAM) is crucial for protecting technology assets from cyber threats. It validates user identity and ensures authorized access to resources. IAM combines access policies and authentication mechanisms to control who can access what data and applications, and their permissions.

Best practices for effective IAM implementation include:

- **Clear Definition** – Ensure proper understanding of technology and business processes for correct access authorization.
- **Strong Foundation** – Align IAM policies with risk assessments, organizational IT infrastructure, and security policies.
- **Step-by-Step Implementation** – Use an iterative, agile approach to avoid complexity.
- **Knowledge Sharing** – Provide training for teams on technology, product capabilities, and scalability.
- **Primary Security Perimeter** – Treat IAM as the first line of defense against malicious actors.
- **Multi-Factor Authentication (MFA)** – Add extra layers of authentication beyond user ID and password.
- **Optimize Single Sign-On (SSO)** – Simplify user authentication with a single set of credentials across resources.
- **Zero-Trust Policy** – Assume all access requests are threats unless verified and validated.
- **Strong Password Policy** – Enforce strong, regularly changed passwords across the organization.
- **Privileged Accounts** – Limit privileged access and isolate accounts from potential exposure.
- **Regular Audits** – Conduct security audits and access recertification regularly, revoking unnecessary access.

Physical Security

Physical security is a critical aspect of cloud security, ensuring that unauthorized access to cloud providers' hardware in their data centers is prevented. Measures such as security doors, CCTV, uninterrupted power supplies, alarms, fire protection, and air and particle filtration are essential components of physical security.

The physical locations hosting cloud servers must be protected from both human threats and natural disasters, including hurricanes, radiation, earthquakes, tsunamis, solar flares, and terrorism. While cloud solutions provide enhanced disaster resilience, physical security in data centers must be carefully considered, as any breach could affect services across all cloud data centers. The physical security strategy should cover areas like security perimeter definition, alarms, controlled access to critical areas, uninterrupted power, risk and issue management, fire protection, and air and particle filtration.

Threat Intelligence, Monitoring, and Prevention

Threat Intelligence, IDS (Intrusion Detection Systems), and IPS (Intrusion Prevention Systems) are crucial for cloud-based platforms, just as they are for on-premises infrastructure. While Threat Intelligence and IDS help identify attackers targeting cloud-hosted systems, IPS not only detects but also mitigates attacks, providing alerts to trigger further response actions.

In cloud security, IPS is generally preferred over IDS for several reasons:

- IDS only detects and highlights security threats, while IPS can prevent them.
- Alerts from IDS require additional effort from security teams to analyze and act, whereas IPS automatically takes predefined actions when a threat is detected.

Though IPS is a more effective security solution, it adds overhead to networks as it intercepts all network traffic. IPS requires sufficient capacity based on traffic load and may become a single point of failure if it malfunctions [3].

IPS uses different methods to detect and prevent security threats in cloud infrastructure:

- **Signature-based Detection**: Most intrusion detection and prevention systems use this method, which searches for known malicious activities based on predefined signatures, similar to a virus scanner. While effective at detecting known attacks, it may fail to detect new threats if no signature exists.
- **Anomaly-based Detection**: This method overcomes the limitations of signature-based detection by establishing a baseline of normal network behavior and identifying deviations from it.
- **Passive Network Monitoring**: This technique involves monitoring network traffic at key points to detect malicious behavior. Security thresholds are set to distinguish between acceptable and malicious activities.

Encryption and Tokenization

Storing financial data and PII in the cloud involves transferring large amounts of data to and from the cloud provider's platform. Encryption adds an extra layer of security in such environments by encoding data both during transmission and while stored. Strong encryption techniques make it nearly impossible to decipher the data without the decryption key.

In contrast, tokenization involves converting meaningful data, such as an account number, into a token that has no inherent value. These tokens are typically generated as random strings of characters, so they are useless even if breached. Tokens serve as references to the original data but cannot be used to retrieve the actual values. Unlike encryption, which uses mathematical algorithms to encode data, tokenization uses random characters without relying on a key or algorithm. The actual value of the data is stored in a secure token vault, which is protected at rest, often with strong encryption.

Cloud Security Assessments

To maintain and enhance the security of cloud-based solutions, it is essential to regularly evaluate the overall system's vulnerabilities through web and mobile application assessments, vulnerability scanning, phishing simulations, and penetration testing. Architectural design reviews and code audits are also crucial for securing application code. Educating developers on secure coding practices is key, while solution architects must ensure that no sensitive data is transferred to the cloud without proper encryption or tokenization.

This proactive approach allows for the identification of potential weaknesses and exploits in the cloud infrastructure. Once vulnerabilities are identified, corrective actions, such as applying patches, can be taken to address these issues and strengthen overall cloud security.

2. Conclusion

There is a common misconception that the public cloud is unsuitable for storing sensitive data such as PII. However, this research demonstrates that this belief is unfounded. By fully leveraging the advanced technology and best practices available in the public cloud, enterprises can enhance efficiency, reduce costs, and significantly improve their overall risk profile, leading to highly favorable outcomes.

Financial institutions have successfully adopted the public cloud, storing sensitive financial data and PII securely, in compliance with data protection regulations. The insights gained from these institutions can serve as a guide for developing a methodology for storing sensitive data in the cloud, which can be utilized by other organizations transitioning to the public cloud.

While the lack of a physical perimeter in the cloud presents challenges, the security solutions offered by cloud providers have evolved to meet these concerns. Tools and techniques from cloud providers and third parties now safeguard applications and data, ensuring cloud infrastructure security is on par with on-premises setups.

As with any technology, organizations must remain vigilant to prevent data breaches. Although the division of security responsibilities between cloud providers and clients may not always be clear, a well-defined shared responsibility model can help mitigate security gaps.

For future research, this study could be expanded to explore the effectiveness of the best practices outlined in this paper across a broader range of use cases in different industries. This would help validate and update the recommendations on an ongoing basis.

References

1. Bahşi, H., Udokwu, C.J., Tatar, U., and Norta, A. (2018) Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review, in: International Conference on Cyber Warfare and Security, Academic Conferences International Limited, United Kingdom, pp. 11-20, X-XI.
2. Bird, D., (2018). Information Security risk considerations for the processing of IoT sourced data in the Public Cloud. Living in the Internet of Things: Cybersecurity of the IoT - 2018, [online].

3. Bruma, L., (2020). An Approach for Information Security Risk Assessment in Cloud Environments. Informatica Economica, [online] 24(4/2020), pp.29-40.
4. Coalfire, (2019). Cloud Security Intelligence Report. [online]
5. Hamza, M., Abubakar, H. and Danlami, Y., (2018). Identity and Access Management System: a Web-Based Approach for an Enterprise. [online]
6. Huang, D., Chowdhary, A. and Pisharody, S., (2020). Microsegmentation: From Theory to Practice. [online]
7. Iwasokun, G., Omomule, T. and Akinyede, R., (2018). Encryption and Tokenization-Based System for Credit Card Information Security. [online]
8. Koch, R., (2019). What is considered personal data under the EU GDPR? - GDPR.eu. [online] GDPR.eu.
9. Kumar, R. and Goyal, R., (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, [online] 33, pp.1-48.
10. Lee, H. and Tao, Y., (2016). Bridging Cloud Security and Data Protection, using MTCS and ISO27018. [online]
11. Song, H., (2020). Testing and Evaluation System for Cloud Computing Information Security Products. [online]
12. Subramanian, N. and Jeyaraj, A., (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, [online] 71, pp.28-42.
13. Synopsys, (2019). Synopsys Cloud Security Report 2019. [online]