Best Practices for Securing Financial Data and PII in Public Cloud

Pankti Desai
University of Bolton

Thaier Hamid, PhD
University of Bolton

ABSTRACT

The financial sector has been one of the more cautious industries when it comes to adoption of new technologies. However, considering the massive benefits and opportunities cloud adoption can potentially provide, financial institutions are now ready to get on to the cloud adoption journey. This introduces a number of challenges for these institutions around storage of sensitive financial data and personal identifiable information (PII) in public cloud.This research reviews the challenges faced by financial institutions in storing their financial data and PII in public cloud infrastructure and aims to derive best practices based on their learnings. Senior stakeholders from large UK organisations were interviewed for collecting details based on their real-life experiences. The learnings are then validated by comparing to the industry best practices. As a result, this paper provides insights into several best practices around storing sensitive data in the public cloud that will further guide other financial institutions adopting the cloud.

Keywords

Public Cloud, financial data, PII, cloud security, financial institutions, cloud security best practices, data privacy, data security.

1. INTRODUCTION

Cloud computing is emerging very fast due to the benefits it can provide compared to traditional computing services. It provides computing resources like processing power, storage, and other resources as a pay-per-use package for consumers. As banking and financial services industry is heavily dependent on information technology,it can surely benefit from theadvantagesoffered by cloud computing around cost, resiliency, and scalability to provide high-quality, economical service to its consumers.

However, one of the fundamental challenges around cloud adoption for financial institutions is the security of the infrastructure and data stored in the public cloud. In addition, the increasing number of cyber-attacks and regulatory and compliance requirements around privacy of customer data and Personal Identifiable Information (PII) make the cloud adoption further tricky for financial institutions. Additionally, feworganisations using the public cloud to host theirsystems have highlighted concerns and challenges around security of personal identifiable information (PII), data breaches, and gaps around segregation of duties.

This research is based on real-life experiences around data security in public cloud implementations for financial institutions and outlines best practices based on lessons learnt.

1.1 Sensitive Data on Public Cloud

Cloud computing enables convenient, ubiquitous, on-demand access to a shared pool of computing resources. These resources like networks, servers, storage, and applications are all configurable through self-servicing admin portals provided by cloud service providers [17]. Processing capacity on Cloud infrastructure can be rapidly increased or decreased on demand, with minimal manual effort involved [10].

While there's quite a lot of research available around issues relevant to cloud adoption, not many cover the security challenges pertaining to storing financial data and Personal Identifiable Information (PII) in the public cloud and the solutions for them. Considering that most financial institutions worldwide are now moving to public cloud infrastructure, secure storage of financial data and PII becomes a significant yet untapped area for research that this study addresses.

This research aims to outline the **best practices based onreal-life learnings for securing financial data and PII in public cloud infrastructure**. This overall aim is further split into specific objectives as below,

- Evaluate Cloud adoption in financial institutions
- Assess real-life security challenges faced by these financial institutions with respect to PII and financial data
- Outline best practices based on lessons learnt by financial institutions

This research is mainly focussed around two research questions (Q1 – Q2) as below,

- Q1 – Is it feasible to develop a methodology for storing sensitive financial data and PII in public cloud that also caters for applicable data protection regulations?
- Q2 – How best can the features provided by public cloud providers utilised to minimise security threats?

1.2 Significance of the Study

This research contributes to the broader computer science practice and, more specifically, to cloud adoption. This research involves assessing various security provisions in public cloud infrastructures and validates how financial institutions can best utilise them to secure critical customer data like PII.

The results of this research would help decision-makers in financial institutions to better understand the factors influencing cloud adoption. This will further facilitate necessary considerations in designing new approaches and solutions to effectively secure financial data and PII in public cloud infrastructure to achieve optimal results.

The study only focuses on financial data and PII for financial institutions, and sensitive data about other industry domains is not considered for this study.

This research covers real-life lessons learnt by financial institutions and outline best practices for other organisations planning to migrate their systems to public cloud infrastructure.This research was conducted through interviews of senior professionals in financial institutions and technology organisations, by evaluating and measuring their experiences in adopting and managing cloud-computing technology for their organisations.

2. BACKGROUND STUDY

Cloud technology has transformed the way of accessing computational resources. While many organisations aspire to adopt cloud, the risk of losing important data is one of the reasons why some of them are hesitant in migrating their existing infrastructure to public cloud. This chapter outlines the existing work related to different aspects of the cloud security challenges, the importance of personal identifiable information (PII), and practices to securely store sensitive data in public cloud infrastructure.

Study [21] covers the security issues involved with cloud architecture concerning different layers of cloud infrastructure. The paper also covers data storage issues affecting various organisations and provides high-level recommendations to mitigate these issues.

The research [4] applies a risk assessment framework based on Microsoft's STRIDE model (that stands for "Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege") to cloud computing. It further outlines the top security risks associated with Cloud adoption.Finally, it proposes a detailed security risk assessment to identify the most appropriate security controls to protect the data hosted on cloud infrastructure.

[6]offers an excellent overview of cloud concepts and bifurcates cloud security issues in multiple different categories. It elaborates on privacy issues relevant to financial institutions storing PII on cloud infra and covers relevant regulatory and compliance aspects.

Personal Identifiable Information as defined by GDPR [13] refers to "Personal data relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The paper [1] details the impact of cyber activities on business proceedings and objectives through a systemic literature review. It also proposes a framework for taking up similar impact assessments for specific business scenarios. Finally, the paper discusses the gaps in the available literature and highlights the areas for future research.

The research [19] focuses on data breaches of personal identifiable information and puts the costs of these data breaches into perspective, highlighting that the Banking and Financial industry is the sector worst affected by these. It also provides a view of the importance of PII from the government's outlook and elaborates on the regulatory and legal implications applicable to the healthcare and financial sectors.

Table 1: Cost and impact of some of the data breaches

Company	People affected	Cost of Data Breach (mil. $)
Yahoo	3 billion	502
Equifax	147 million	1445
Anthem	78 million	406.5
Sony PSN	77 million	193
Home Depot	56 million	340

Research [14] provides a background of cloud architecture and elaborates various vulnerabilities associated with cloud computing very effectively. It also recommends countermeasures to safeguard against these vulnerabilities and focuses on protecting sensitive and personal identifiable information in public cloud infrastructure.

The study [2] focuses on PII data captured and stored in high volumes on public cloud-based infrastructure. To cater for the security challenges around storing PII on public cloud, it recommends a defence-in-depth approach to apply security techniques at different layers of the cloud setup. The solutions described in the paper can be leveraged for various use cases for storing sensitive data in the cloud.

The paper [15] proposes using a Multi-Tiered Cloud Security (MTCS) approach for achieving data protection in public cloud environments. It accurately presents the security challenges faced in public cloud adoption. Further, it elaborates how MTCS can be leveraged to achieve cloud security and data protection.

The research [16] focuses on data security in healthcare domain and explains how sensitive medical data for patients can be securely stored in public cloud infrastructure. It recommends utilising MTCS by extending it in specific industry sectors. While the paper focuses on the healthcare sector, it also provides valuable insights into how multi-tiered cloud security can be utilised for other industry verticals and motivates further research.

3. RESEARCH METHODOLOGY

This study is carried out as a qualitative research based on interviews using a thematic content analysis to assess responses and outline the findings. Existing literature around the topic was reviewed too to identify, evaluate, and effectively interpret relevant research available to this topic of interest [8].

Senior stakeholders in major UK financial institutions and technology organisations were interviewed to understand their real-life cloud adoption experiences and learn best practices to secure PII in the public cloud. Thematic content analysis was carried out on the basis of interview responses.

Literature search looked for academic sources like journals, books, working reports, conference proceedings, and thesis. The search terms used to identify relevant literature primarily focused on "securing sensitive financial data and PII in the public cloud". Additionally, a combination of terms "financial data", "PII", "public cloud security", "cloud security best practices", "data privacy", "compliance", "data security" and

"cloud adoption in financial institutions" were used to ensure no relevant material is left out.

Relevant search terms were used to look for content on the most popular, widely used and cited academic online libraries.

4. BEST PRACTICES FOR STORING FINANCIAL DATA AND PII INPUBLIC CLOUD

Considering the benefits provided by cloud infrastructure, it is inevitable that the financial institutions would like to adopt cloud sooner rather than later. As a result, Cloud security encompassing processes, controls and policies around the cloud infrastructure including systems and data becomes very crucial. With one in four organizations confirming a security incident related to cloud during 2019, overall, 93% of organizations surveyed by Coalfireconfirmed that they are moderately or extremely concerned about security of their systems and data in cloud [7].

4.1 Cloud Security Strategy

A detailed cloud security strategy to protect application data, while adhering to regulatory compliance, and protecting data privacy for customers especially is key for organisations moving to hybrid cloud. This also eventually helps organisations to remove dependencies from any specific cloud provider, protect themselves from any financial and reputational loss due to data breaches and also safeguards them against legal ramifications of data loss [5].

The objective of the cloud security strategy should be to make organisation's cloud infrastructure more trustworthy through a critical set of capabilities required to secure systems and data in cloud, while making them accessible across the globe. The strategy must be comprehensive to cover private and public cloud as well as multi-cloud setups to allow organisation to have a uniform approach to security. The cloud security strategy should further leverage automation for creation and enforcement of these security policies to best extent possible to avoid any potential errors introduced through manual activities.

The focus for these should remain on the three key attributes – Infrastructure, Data and People for both private and public cloud environments [18].

Therefore, the cloud strategy should consider various aspects like authentication, access controls, user behaviours, data classification, encryption, and logical segmentation of data while ensuring there is adequate logging and reporting available to track any unexpected data access. Security strategy should also cater for regulatory compliance challenges and safeguard against data breaches and insider threats [11].

Key principles for an effective cloud security strategy,

- **Shared Responsibility** – Organisations should think of hybrid cloud security as a shared responsibility. Leaving the security setup for an organisation's critical data to cloud service providers is a risky proposition prone to oversight and errors.
- **Proactive approach** – Maintaining security requires a proactive identification of all potential risks and effective mitigation. Reacting to security incidents and recovering systems and data after being compromised is never easy, even with the best-equipped cloud providers.
- **Standardise processes** – Organisations are encouraged to have the same set of processes for their private and public cloud environments. This allows prevent manual errors and avoid potential security loopholes.
- **DevSecOps** – Human errors in cloud environment can be minimised through practices like codifying the process into workflows that can be triggered at the click of a button.
- **Zero-Trust policy** – Conventional network perimeters are ineffective most of the times when dealing with hybrid cloud computing environments as the data and processes may be spread across different geographic locations and separate infrastructures. Traditional perimeter-based protections therefore don't work in these scenarios. Access to each asset and data element should therefore be protected by adopting the "never trust, always verify" attitude for all requests.
- **Uniform IAM framework** – Framework for overall IAM setup should mirror the concept of least-privilege for every aspect of the hybrid cloud environment including private and public infrastructure.
- **Safeguard data** – As a standard practice for any cloud environment, data protection strategies like encryption, tokenisation and pseudo-normalisation should be applied wherever feasible.

4.2 Shared Responsibility Model

Due to the nature of cloud infrastructure setup, where systems and components are spread across multiple organisations and geographic locations, it is not feasible to control security aspects centrally through single ownership. As a result, the responsibility to manage security of the overall end-to-end infrastructure is a shared responsibility between the consumer and cloud service provider.

The below image provides a high-level framework for shared responsibility model for IaaS, PaaS and SaaS cloud setup [22].

- **People** – managing identity and access for all aspects of cloud-hosted applications including authentication and authorization mechanisms, multi-factor authentication (MFA), single sign-on (SSO), certificates, access keys, and password management are owned by the organisation.
- **Data** – controlling who can use the data and how, is organisation's responsibility and the cloud service provider may not have any visibility at all for the data.
- **Applications** – apart from the SaaS model, managing applications on public cloud (IaaS and PaaS) is the organisation's responsibility. These server-based cloud environments are provided as blank slates much similar to on-premise hosts. The organisations also own application logic and code too and it's their responsibility to secure them and control them throughout the entire software development lifecycle. This should also include mechanism to secure code repositories from malicious misuse or intrusion, regular testing for the application throughout the development and integration processes, securing production access, and ensuring strong security for all connected systems.
- **Operating System** –barring the IaaS model, the cloud provider owns and controls the operating system. However, an operating system for IaaS instance will need to be secured and controlled by the financial organisation opting for IaaS model. For PaaS and SaaS setup, the cloud provider will allow access to the

configuration setup for the cloud instance through the control panel.

- **Virtual networks** –similar to operating systems, the cloud service provider can only maintain the network for PaaS and SaaS cloud offerings. Virtual network setup for IaaS is a financial organisation's responsibility from a security configuration and monitoring perspective.
- **Hypervisors** –virtualization isentirely controlled by the cloud service provider. Therefore, provisioning physical resources, ensuring CPU segmentation and isolation, storage, GPU and memory, are all providers responsibilities.
- **Servers and storage** – all the physical servers and storage are owned by the cloud service provider. Therefore, the security configuration and monitoring for them will always be the cloud service provider's responsibility.
- **Physical networks** – all biological networks are again the cloud service provider's responsibility to manage security and control access.

4.3 Identity and Access Management

Identity and access management (IAM) covers two very important aspects of securing technology assets against any cyber threat. The identity part of it helps validate whether the user is actually what they claim to be, and access element of IAM ensures the identified user can only access the resources that they are authorised to. IAM combines user access policies and authentication mechanisms, to control who can access what applications and data, and what they can do with them [9].

Effective implementation of Identity and Access Management (IAM) is subject to below best practices.

1. **Clear definition** – it is fundamental for successful implementation of IAM that both technology and business processes are understood correctly, and access authorised accordingly only for users and systems that actually need it.
2. **Strong foundation** – IAM is one of the building blocks for cloud systems that will be utilised over a period of time by new platforms migrated to the cloud too. As a result, while the IAM policy needs to have a practical risk assessment based on IAM product capabilities, it should also remain in sync with organisational IT infrastructure and security policies.
3. **Step-by-step implementation** – IAM should follow an iterative, agile approach to implementation to avoid complexities.
4. **Knowledge sharing** – all the teams involved with IAM setup and maintenance should have adequate amount of training for underlying technology landscape, product capabilities and scalability.
5. **Primary security perimeter** – IAM should be considered as the first line of defence against any malicious actors. With increasing usage of cloud, the physical network perimeter is becoming less effective and identity management therefore should be used to centrally manage security controls.
6. **Multi-Factor Authentication (MFA)** – this provides an additional means to authenticate the users by expanding the number of checks beyond the conventional user id and password check.
7. **Optimise Single Sign-On (SSO)** – SSO provides users the convenience to use the same set of credentials across different resources and allows IAM to avoid the challenge of managing too many different sets of credentials for each user.
8. **Zero-Trust Policy** – this model assumes that every access request made to any resource in scope of the IAM policy is a threat, unless verified and confirmed to be a legitimate request. This applies to requests both inside and outside of the network and enforces all the requests are thoroughly validated.
9. **Strong password policy** – organisation wide password policy should enforce users to set up strong passwords and regularly change them.
10. **Privileged accounts** – limit the number of users having privileged access to critical assets. Further isolate privileged accounts from any activities potentially at risk of exposure to cybercriminals.
11. **Regular audits** – security audits and access recertification should be carried out at regular intervals and any accesses no longer required should be revoked accordingly.

4.4 Physical Security

Physical security is another essential, very crucial aspect of cloud security. Suitable measures should be taken to prevent direct access to cloud providers' hardware in their data centres. Physical security includes controlling direct access by means of security doors, CCTV, uninterrupted power supplies, alarms, fire protection, air and particle filtration, and more.

The physical locations hosting the servers providing cloud offerings must be protected against both human-originated threats. In addition, natural calamities, such as hurricanes, radioactive radiation, large magnitude earthquakes, tsunamis, sun flare outbursts, and terrorism require a periodic re-evaluation. While cloud-based solutions offer better resilience to disasters, it requires further consideration to physical security in all these cloud data centres as a malicious actor in any of these can wreak havoc across all the services provided through all cloud data centres.

The processes driving physical security strategy for organisations has to cover, aspects like Area security definition, Alarms, Controlled access to key areas, Uninterrupted power supplies, Risk and issue management, Fire protection and Air and particle filtering.

4.5 Threat Intelligence, Monitoring, and Prevention

Even for the cloud-based platforms Threat Intelligence, IDS (Intrusion Detection Systems), and IPS (Intrusion Prevention Systems) are equally important as they are for on-premise infrastructure. While Threat Intelligence and IDS help identify attackers, that are currently targeting to breach into cloud hosted systems, IPS allow mitigating attacks and alert on the occurrences of attack so that additional steps to respond can be taken.

Considering cloud security, IPS is preferable in the majority of the cases compared to IDS as,

- While IDS can only detect and highlight security threats, IPS can even prevent them.
- Alerts added by IDS require security teams to spend further effort to analyse and act upon them, IPS saves time by taking pre-defined actions when threat is identified.

While IPS is preferrable as a security solution, it adds overhead on networks and intercepts all network traffic. IPS needs sufficient capacity depending on the network's traffic load and can become a single point of failure in case of a malfunction [3].

Intrusion Prevention Systems use different mechanisms to intercept and prevent security threats in cloud infrastructure.

- **Signature-based detection** – The majority of intrusion detection and prevention systems use signature-based detection. They search for already known malicious activities, similar to a virus scanner, based on the signature for different intrusion events. While this is really efficient at detecting known attacks, it requires creating a signature for every episode. As a result, any new attacks may go undetected.
- **Anomaly-based detection** – Signature-based detection cannot identify dynamic attack patterns effectively. This is where Anomaly-based detection helps by creating a baseline for network behaviour and monitoring events that deviate from this baseline behaviour.
- **Passive network monitoring** – Another mechanism is to monitor network traffic at specific points passively and identify malicious behaviour. This is achieved through various security thresholds that can be used to determine if the attempted activity is acceptable or is malicious.

4.6 Encryption and Tokenisation

Storing financial data and PII in the cloud requires sending massive amounts of data to the cloud provider's platform and retrieving the same from there. Encryption provides another layer of security in such cloud environments, by encoding the data both in transit and when at rest. Using strong encryption techniques makes it near impossible to decipher encrypted data without a decryption key.

On the other hand, Tokenisation is the process of converting a meaningful piece of data, like an account number, into a token that has no significant value. Tokens are usually generated using a random string of characters so that it doesn't serve any weight even if breached. Tokens can be considered as a reference to the original data but cannot actually be used to derive the actual values of the data. Unlike encryption, which uses a mathematical process to encode sensitive data, tokenisation uses random characters without involvement of any key or algorithm. Tokenization uses a lookup, called a token vault, to identify the actual value relating to the token. The data in the vault is additionally secured at rest, often using strong encryption [12].

4.7 Cloud Security Assessments

Another best practice to maintain and improve the security of solutions implemented in the cloud is to regularly assess the vulnerability of the overall solution through web and mobile application assessments, vulnerability scanning, phishing exercises and penetration testing. Architectural design reviews and code reviews too play a very important part in securing the application code. Developers can be educated to ensure they use secure coding practices. Solution architects can confirm there are no sensitive data elements moving to cloud infrastructure without proper encryption or tokenisation.

This helps to proactively identify any potential weaknesses and exploits in cloud infrastructure. Once the vulnerabilities are known upfront, corrective measures can be implemented to apply necessary patch to fix these vulnerabilities and improve the overall cloud security [20].

4.8 Micro-Segmentation

Micro-segmentation is increasingly common technique in implementing cloud security. It is a method of creating multiple zones by dividing your cloud infrastructure into distinct and isolated security segments, in order to secure them individually.

These segments allow security architects to create policies to limit traffic between different segments or workloads utilising a zero-trust approach. Micro-segmentation allows reducing the overall attack surface and strengthens regulatory compliance by enhancing breach containment [10].

5. CONCLUSION

While there is a common misconception that the public cloud is not an acceptable environment for sensitive data such as PII, this research elaborates that this belief is not valid. Instead, by fully utilising the superior technology and practices available in the public cloud domain, an enterprise can increase efficiency and even potentially lower costs. In addition to that, they can also dramatically improve their overall risk profile in a way that will produce highly favourable results.

Financial organisations have successfully adopted the public cloud. They have been safely storing their sensitive financial data and PII in the cloud, without any issues and in accordance with various data protection regulations. The learnings from these institutions can be used as a guideline to define a methodology for storing sensitive data in the cloud and can be leveraged by other organisations migrating to public cloud.

While a significant challenge with the cloud is the lack of actual perimeter, the security solutions provided by cloud service providers have matured adequately over a period of time. Tools and techniques are available through cloud providers and other third parties to safeguard applications and data in a public cloud environment bringing security in cloud infrastructure on-par with on-premise setup.

Like with all technology setup, organisations must continue focusing on an ongoing basis to avoid data breaches. While it may not always be clear where the security responsibilities begin and end for cloud providers, security gaps can be avoided through a well-understood and agreed shared responsibility model.

As a future line of research, this study can be expanded to understand how effective the best practices included in this paper are for a wider selection of use-cases across different industry domains. This can further help revalidate and refresh the recommendations in this research paper on an ongoing basis.

6. 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] Borkar, P., (2019). IPS Security: How Active Security Saves Time and Stop Attacks. [online] Exabeam.

[4] Bruma, L., (2020). An Approach for Information Security Risk Assessment in Cloud Environments. Informatica Economica, [online] 24(4/2020), pp.29-40.

[5] Che, J., Duan, Y., Zhang, T. and Fan, J., (2021). Study on the Security Models and Strategies of Cloud Computing. [online]

[6] Chen, L., Takabi, H. and Le-Khac, N., (2019). Security, Privacy, and Digital Forensics in the Cloud. 1st ed.

[7] Coalfire, (2019). Cloud Security Intelligence Report. [online]

[8] Fink, A., (2019). Conducting Research Literature Reviews: From The Internet To Paper. Los Angeles, CA: Sage.

[9] Hamza, M., Abubakar, H. and Danlami, Y., (2018). Identity and Access Management System: a Web-Based Approach for an Enterprise. [online]

[10] Huang, D., Chowdhary, A. and Pisharody, S., (2020). Microsegmentation: From Theory to Practice. [online]

[11] HyTrust, (2021). Cloud Security Policy | Workload Security | HyTrust. [online]

[12] Iwasokun, G., Omomule, T. and Akinyede, R., (2018). Encryption and Tokenization-Based System for Credit Card Information Security. [online]

[13] Koch, R., (2019). What is considered personal data under the EU GDPR? - GDPR.eu. [online] GDPR.eu.

[14] Kumar, R. and Goyal, R., (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, [online] 33, pp.1-48.

[15] Lee, H. and Tao, Y., (2016). Bridging Cloud Security and Data Protection, using MTCS and ISO27018. [online]

[16] Lee, H. and Tao, Y., 2017. MTCS for Healthcare. 2017 International Conference on Cloud Computing Research and Innovation (ICCCRI), [online]

[17] Mell, P. and Grance, T., (2011). *1*[online] National Institute of Standards and Technology.

[18] Omoyiola, B., (2020). Strategies for Securing Cloud Services. [online]

[19] Poyraz, O., Canan, M., McShane, M., Pinto, C. and Cotter, T., (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. The Geneva Papers on Risk and Insurance - Issues and Practice, [online] 45(4), pp.616-638.

[20] Song, H., (2020). Testing and Evaluation System for Cloud Computing Information Security Products. [online]

[21] Subramanian, N. and Jeyaraj, A., (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, [online] 71, pp.28-42.

[22] Synopsys, (2019). Synopsys Cloud Security Report 2019. [online]