International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 1, Issue 12, 2022
DOI: https://doi.org/10.38124/ijsrmt.v1i12.1188

Cloud-Based Big Data Security Models for Financial Institutions

Nareddy Abhireddy[1]

[1]Independent Researcher

Publication Date: 2022/12/30

Abstract

Financial institutions face ever-increasing security challenges, prominently reflected in the dramatically rising number of breaches and incidents. Many of these institutions are undergoing a transformation in the way the deploy, and consume IT services. Rather than the traditional ‘Over-provision’ approach – in terms of scalability, complexity, risk, cost and time to deploy; the Cloud model enables firms to ‘under-provision’ provision only what is required and ‘elastic’. Cloud computing enables banks and financial institutions to deploy their infrastructure, platform and software in a more efficient manner. Cloud-based IT systems offer significant economic and scalability advantages but in the financial sector where sensitive, private and confidential information is actively processed such solutions also present a significantly increased risk and need to provide a more wooden security model compared to on-premise legacy solutions.

Banking and financial services institutions use cloud models for their infrastructure, platform, and Software-as-a-Service needs. These cloud-based deployment models enable banks to meet their business and operational needs efficiently and garner substantial savings. However, while many financial institutions have witnessed the benefits of cloud computing, security considerations inherent to these systems have hindered and delayed their mass adoption. Security is considered the most important barrier for adopting public clouds. Since all cloud services rely on the internet for service delivery, the Internet’s credibility is the main concern for the financial and banking sector. The sensitive nature of information processed and stored in such environments makes data security of utmost importance and financial service providers should approach data storage and management issues while keeping in mind the impact it might have on their reputation if they have to face a data loss incident.

Keywords: *Cloud Security in Financial Services, Banking Cloud Transformation, Financial Data Security, Cloud Computing Adoption Barriers, Elastic Cloud Infrastructure, Under-Provisioning Models, Cloud Risk Management, Public Cloud Security Concerns, Sensitive Financial Data Protection, Regulatory Compliance in Banking IT, Internet Dependency Risks, Cloud Infrastructure Platforms, SaaS in Financial Institutions, Secure Cloud Architectures, Financial Cybersecurity Threats, Data Breach Mitigation, Reputation Risk Management, Cloud Governance Frameworks, Secure Data Storage and Management, Financial IT Modernization.*

I. INTRODUCTION

Despite the myriad challenges associated with data security and privacy, financial institutions are under increasing pressure to leverage Cloud Computing effectively for Big Data Management and Processing. The combination of Cloud Computing, Big Data and Internet Technologies provides a huge opportunity for FinTech companies to create novel scalable applications and services based on Financial Data. However, because financial data are considered among the most sensitive data, security concerns are critical. Thus, Security Models are necessary in accordance with the fundamental principles of Cloud-Based Big Data Security in Financial Institutions.

Cloud Computing is a ubiquitous phenomenon in Computer Science that aims to deliver Computing Services through a network in an on-demand and convenient manner. This concept is strongly associated with Big Data since both concepts earn environment on the Internet. The issues of Big Data Security in the context of Cloud Computing Architecture have drawn a great deal of attention, notwithstanding several distinguished efforts in this aspect. In a Cloud environment, the responsibility of Data Security is divided among the Cloud Service

Provider and Cloud Service User (Data Owner) on the basis of Service Model and Deployment Model. Accordingly, Bank Data Security in a Cloud Environment can also be analyzed based on such a division. The basic aspects for Cloud Computing Big Data Security in Financial Institutions are.Data Governance and Compliance; Identity and Access Management; Sharing and Collaboration within Cloud-based Big Data Services; Privacy Preservation; Protection from Malicious Activities; Fraudulent Transactions in Financial Institutions; Exploiting the Cloud for Financial Operations by Fraud Groups and Money Launderers.

- *Overview of Cloud Security in Big Data Context*

The enormous growth of cloud-based data storage and processing is primarily driven by Big Data, a collective term that comprises a vast amount of structured and unstructured data generated each second by major organizations and societies, along with new technologies that facilitate storage, processing, and analysis. Businesses use data for various operations, including cooperation, budgeting, stock and supply chain administration, selling budget assessments, and determining advertising campaigns and expenditures. Cloud services hosted on third-party premises require customers to rely on the security measures handled by the service provider. Although third-party customer services typically receive greater testing and investment in security than many individual corporations could afford, leaks may still occur due to changes implemented by cloud service vendors without informing their partners. As outlined by experts, there is shared responsibility for security between the company deploying services into the cloud and the provider delivering the services. Cloud service agreements explicitly indicate how particular security concerns must be managed and who is ultimately responsible for what operations.

Many financial services institutions have substantially or fully migrated services and operations to cloud services from traditional data centers due to significant cost reductions. In addition to meeting compliance requirements for privacy and governance, protecting sensitive customer data in the cloud remains a top priority. Financial transaction records are subject to some of the most stringent regulations regarding security, privacy, and validity of integrity, with cloud shared responsibility models adjusted to provide security controls also for user workflows and databases in cloud environments. Financial data are attractive to malicious users, and privacy-preserving cloud data analytics of bank customer data recorded in the United States and Europe can provide considerable benefits as long as original records are not disclosed to the cloud service provider.

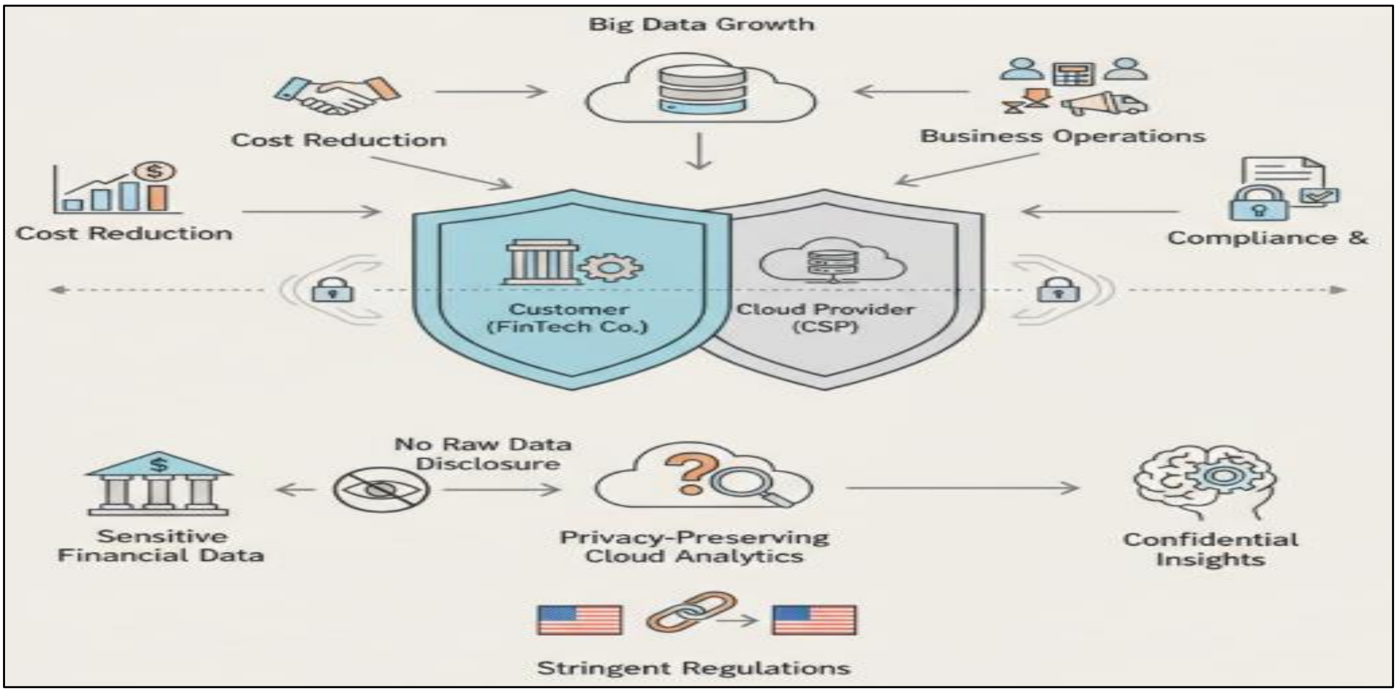

Fig 1 Privacy-Preserving Paradigms in Financial Cloud Migration: Navigating Shared Responsibility and Regulatory Integrity in the Big Data Era

II. BACKGROUND AND CONTEXT

The security of sensitive data stored in the cloud relies on the design of a security architecture that can effectively protect data in a multitenant environment. Stateless systems, network packet filtering, integrity verification, secure communication channels, and secure environment protection are important design elements. Data governance encompasses data quality, integrity, privacy, security, and governance throughout the data life cycle. To alleviate security concerns, identity and access control systems must be tailored to the cloud-computing paradigm, mapping the local identity-management domain into the cloud identity-management domain. Heterogeneity challenges must not hinder data identification and authorization at the service level. Access-management solutions must deliver scalable authorization and management capabilities. Data location is a vital aspect of cloud-based services; thus, auditing, monitoring, and logging of data access and usage help ensure the appropriate use of sensitive information. Establishing security on the basis of an effective security monitoring architecture can support anomaly detection and business policy enforcement through real-time response.

Access to customer data for online transaction processing is commonly controlled by proprietary middleware. The set of data involved in such processes is determined in advance. The middleware relays transaction requests from clients to the appropriate back-end specialized services. Access to analytical data, however, must generally be unrestricted, since the future analytical requests are not known in advance and yet the actual analysis must be performed with proper data subsets—potentially composed of data from different sources—without manually preconfiguring data access rights based on the actual queries. Consequently, security models for true online analytical processing systems differ significantly from traditional online transaction processing database-proof security models.

➢ *Key Considerations in Cloud Security Architecture*

As enterprises migrate confidential and sensitive data to public cloud providers, the importance of ensuring security in outsourced computing becomes critical. Cloud Security Architecture is essential to a cloud-based IT environment, and various frameworks have been developed that address the deployment architecture, security maturity, compliance, identity and access in public cloud. Data owners are responsible for data governance and compliance steers the implementation of controls for data residency, regulation, audit, and overall responsibility.

Many cloud-based implementations operate under the shared security responsibility model defined by the service, infrastructure, and platform models. Recommendations to enhance confidentiality and ensure that the bank customer's privacy is preserved during the development and deployment of analysis systems based on data residing in the cloud are provided. Privacy-preserving analytics for cloud-enabled big data science are also examined, utilizing a sequence of trusted computing and homomorphic encryption engines to demonstrate the analytics in the cloud without leaking any customer information. The integrity and security architecture of financial transaction histories located in the public cloud is also highlighted, detailing how the integrity of the transaction history can be checked via a third party without compromising the confidentiality of the stored data or any other architecture components.

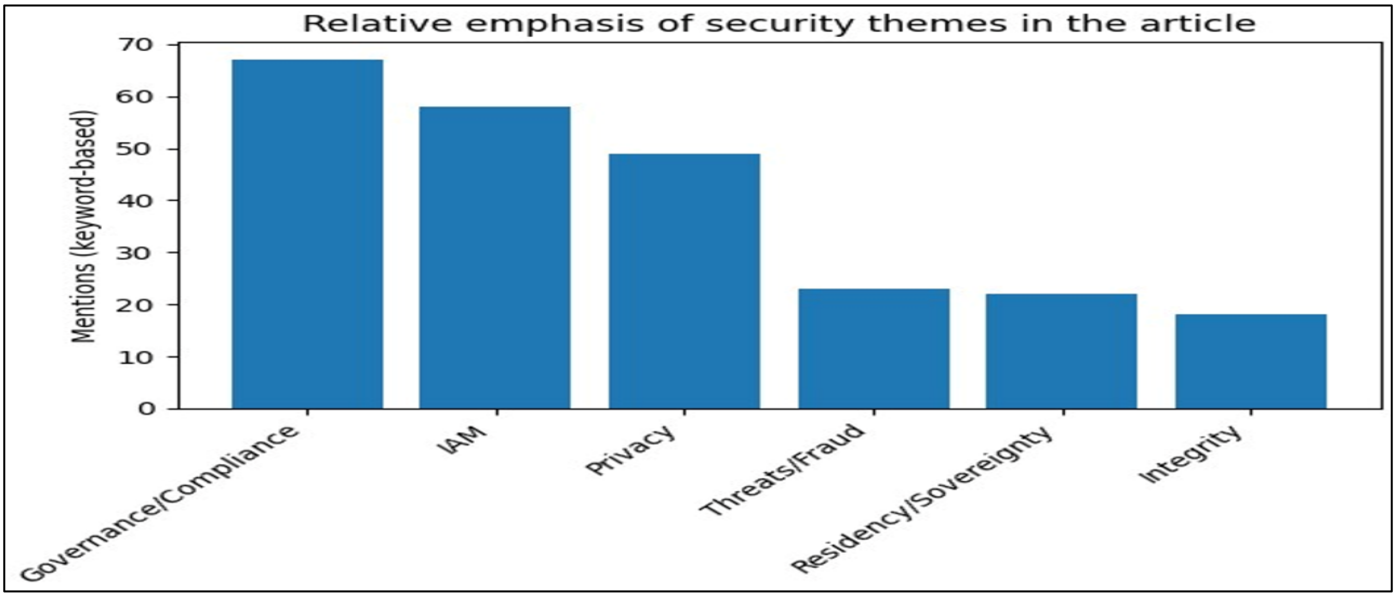

Fig 2 Cloud Security Architecture Foundations for Multitenant Big Data Protection in Financial Institutions

➢ *Equation 1) Shared Responsibility as a Control-Partition Model*

The states security responsibility is divided between the Cloud Service Provider (CSP) and the Cloud Service User / Data Owner depending on service/deployment model.

- *Step 1 (Define the Full Control Set):*

Let the total set of required security controls be

$$\mathcal{C} = \{c_1, c_2, \dots, c_n\}.$$

- *Step 2 (Partition by Responsibility):*

Split into CSP-owned and Customer-owned subsets:

$$\mathcal{C} = \mathcal{C}_{\text{CSP}} \cup \mathcal{C}_{\text{Cust}}, \quad \mathcal{C}_{\text{CSP}} \cap \mathcal{C}_{\text{Cust}} = \varnothing.$$

- *Step 3 (Service-Model Dependence):*

Let service model $m \in \{\text{IaaS, PaaS, SaaS}\}$. Then the partition is a function:

$$(\mathcal{C}_{\text{CSP}}, \mathcal{C}_{\text{Cust}}) = f(m,\text{deployment}).$$

III. ARCHITECTURAL FRAMEWORKS FOR CLOUD-BASED BIG DATA SECURITY

Designing adequate architectural frameworks that enable security in a cloud-based environment for big data is no easy task. Several frameworks exist from various industries and universities that provide guidance on building cloud and big data security architecture. While big data governance seems to be least discussed topic, privacy, identity, and access management in cloud-based information systems are well understood concepts. Many organizations are also developing big data security frameworks tailored for specific industries such as cloud-based financial transaction security architecture and for privacy-preserving big data analytics.

Establishing control over data and compliance is a key prerequisite for organizations considering the public cloud. Regulatory compliance requirements can be met with cloud service providers (CSP) supporting security models such as ISO 27001 along with service level agreements (SLAs) combining big data technology. Residency is often considered a pre-requisite for heavy adoption of public cloud in the financial services sector. Residency of data in a particular geographic region mitigates certain regulatory concerns arising from a shared services environment. However, data residency does not eliminate all the regulatory concerns associated with public cloud usage. Moreover, certain regulatory regimes impose severe restrictions on the handling of sensitive customer data and may require the data to remain within the geographical boundaries of a country (data sovereignty). Customers, therefore, have to evaluate the residency aspect while opting for public cloud services.

- *Data Governance and Compliance*

Financial institutions such as banks, insurance companies, and brokerages must ensure data governance, compliance, and data security regulation standards to comply with government regulations that protect consumers. Data governance for the use of big data and cloud computing embraces the strategic organizational decisions over the accessibility, usability, integrity, and security of the data in the organization. Data governance focuses not only on classification, usability, and accessibility but also on ensuring the ownership and accountability of the data when the institution is using cloud computing and big data in business processes. Organizations using public cloud computing in big data outsourcing may no longer be the data owner. Organizations must be cautious of how consumers can view the data that may contain sensitive information and how data can be misused by an intruder in cloud computing services.

Since financial institutions have data records of customers, they are a prime target for threats to privacy. The use of cloud computing data outsourcing provides ease of disclosure to unauthorized parties and increases the threat to data privacy. Privacy risks associated with cloud computing data outsourcing require cloud service providers, users, and auditors to ensure the privacy of sensitive data such as health records, credit card details, and social security numbers. Effective privacy-preserving data publishing projects require the help of data and mining experts. Security has become extremely important for all cloud service providers, mainly the scalability of data. A cloud security architecture for data confidentiality, integrity, and availability is needed for web services. Security verification methods for service-level agreements can help maintain security and are crucial for establishing trust in cloud computing services.

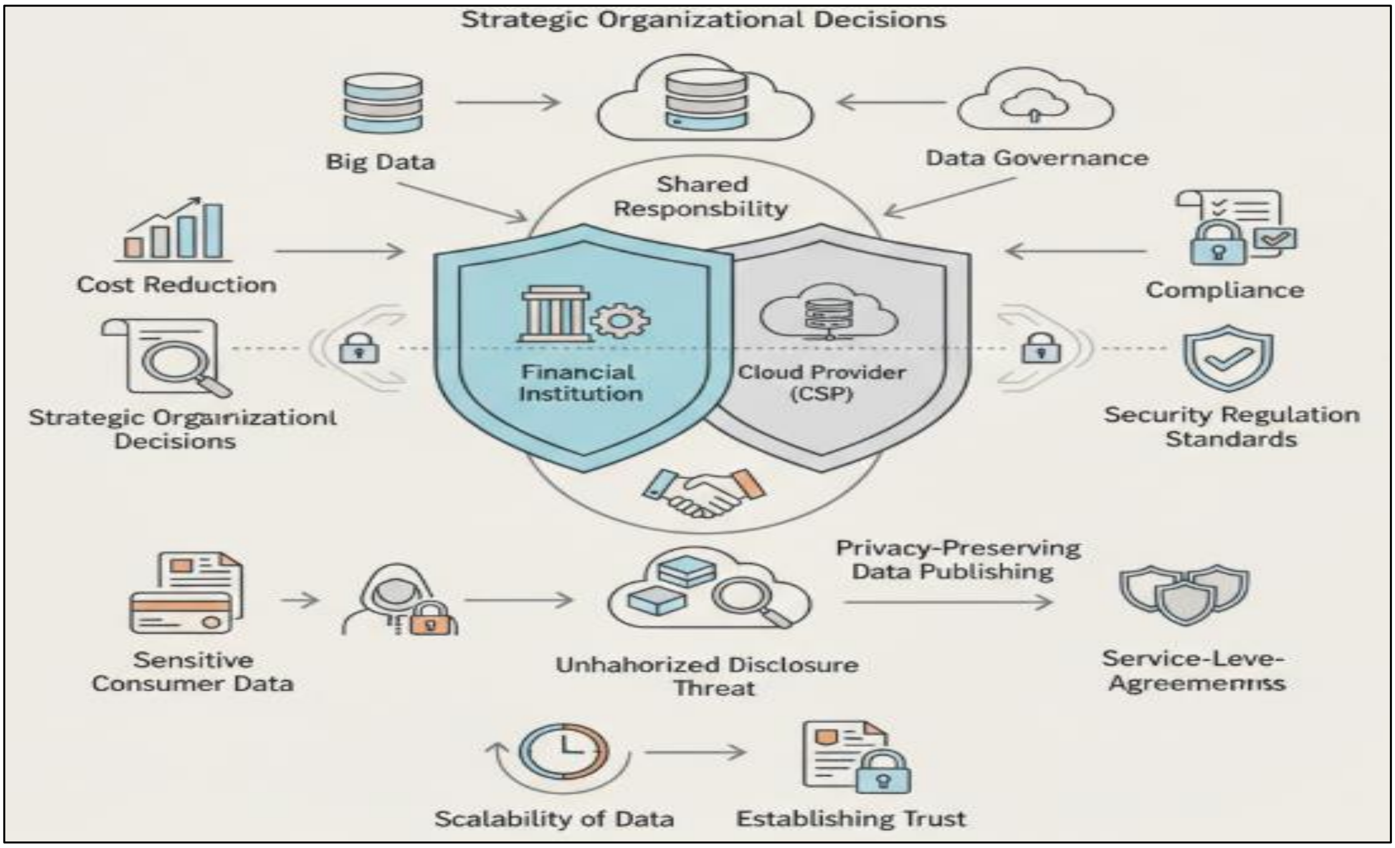

Fig 3 Governance and Trust in Financial Cloud Outsourcing: A Strategic Framework for Data Ownership, Privacy-Preserving Publishing, and SLA Verification

- *Identity and Access Management in Cloud Environments*

- *Cloud Security Architecture: Identity and Access Management*

Identity and access management (IAM) has emerged as one of the main areas of concern for organizations migrating to cloud environments. It serves to securely manage digital identities and monitor and control access to resources. IAM provisions the appropriate user access levels for cloud-hosted applications, transmitting these access privilege settings to cloud service providers (CSPs) to enable secure single sign-on (SSO) technology.

Strong authentication controls, implementable through cloud federation services, are essential to prevent unauthorized IAM access. Federation services eliminate the need for user credentials to be transmitted over the Internet. Federated SSO links an enterprise user directory with CSPs, permitting users to access multiple applications through a single authentication—including Software-as-a-Service applications not affiliated with a given enterprise. With OAuth technology, a network user can permit a third-party application to access information stored in a cloud provider without disclosing authentication credentials. A periodic review of user access rights reduces excessive permissions, while role-based access control enforces least-privilege principles. Audit trails further restrict access to audit records and track the use of sensitive administration functions.

Dynamic data leasing within public clouds can enhance data security without direct user involvement. UAAs control the use of data and apply attributes such as description, metadata, release time, level of aggregation, lifetime, and degree of trust. When other users in the virtual cloud want to access data, they need to meet the rules set by the UAA, collecting the data only after leasing permission is granted.

Despite the various security advantages provided by cloud computing, it also introduces new security challenges, the most serious of which is the cloud provider's inability to protect customer data from unauthorized access by internal malicious users. A cloud data security service model can help mitigate this risk.

Table 1 Thematic Frequency of Key Cloud Security Concepts in Financial Institutions

Theme	Mentions
Governance/Compliance	67
IAM	58
Privacy	49
Threats/Fraud	23
Residency/Sovereignty	22
Integrity	18

IV. SECURITY MODELS AND CONTROLS FOR FINANCIAL DATA

Financial data are particularly sensitive and valuable, making them a preferred target for attackers. Two specific security models addressing the privacy of sensitive data stored in the cloud are presented: privacy-preserving data-mining and data-anonymization techniques. Since a considerable share of internet-based financial transactions is based on an e-payment system, protection of e-payment transactions between customers and banks is also considered. A service-oriented solution for security of e-payment transactions in a publicly accessible cloud serves as the basis for the proposal.

Privacy-preserving data-mining methods enable the analysis of sensitive data stored in the cloud without revealing the information contained in the data to the cloud service provider. The user first requires sensitive data stored in the cloud and generates a demand signature. The server generates a response, which the user decrypts. The decrypted response gives only the information needed to answer the sensitive-data request. Further querying of the data is done by sending a request containing the miner's domain knowledge and the request signature to the server. The server responds with the mining result, which is verified and checked for soundness by the user. The method ensures that neither the cloud service provider nor an offline adversary can infer useful information about the sensitive data.

Data-anonymization techniques help protect personally identifiable information in a dataset while keeping it usable. In the cloud-computing environment, data-anonymization algorithms can be used to anonymize sensitive data before outsourcing to the cloud. A cloud service provider offers the anonymization service, which anonymizes the data based on the privacy requirements of the user. The service then outsources the anonymized data to the public cloud.

- *Privacy-Preserving Analytics*

Privacy-Preserving Analytics for Customers of Financial Institutions Owing to the fact that their primary purpose is the offering of financial services for their customers, Financial Institutions (FIs) are obliged to protect the privacy of their customers. Despite the trust of their customers in their financial institution regarding their personal information as long as they operate in the institution’s information technology (IT) environment, the common failure of FIs’ information systems has raised concerns. Consequently, in the cloud environment, many customers are still reluctant to let their financial institution carry out financial transaction analysis that requires access to their financial information.

In response to these needs, the concept of Private Information Retrieval (PIR) has been proposed for avoiding the financial institution accessing the customers' financial transactions while enabling these third-party data mining techniques to provide such services without violating the privacy of customers' transactions. A financial transaction dataset is divided into several subdatasets and each of these subdatasets is stored in a different cloud service provider in a private cloud environment. Meanwhile, these subdatasets stored in different cloud service providers are connected via a hidden network, which is constructed outside of the financial institution's environment to prevent the financial institution from deciphering the whole picture. Furthermore, these subdatasets also support the communication system inside of the hidden network.

➢ *Equation 2) Risk Scoring for Public Cloud vs on-Prem (Business-Case Framing)*

The argues the decision to use external cloud should be based on a business case rather than assuming it is secure, and that public cloud risk can be "less manageable" because of multi-tenancy and continuous attack exposure.

- *A standard Formalization Consistent with that Narrative:*

✓ *Step 1 (Define Assets and Threats):*

Assets $A = \{a_1, \dots, a_k\}$, threats $T = \{t_1, \dots, t_m\}$.

✓ *Step 2 (Likelihood and Impact):*

For each pair (a,t), define likelihood $P(t|a)$ and impact $I(a,t)$.

✓ *Step 3 (Risk Per Asset-Threat):*

$$R(a,t) = P(t|a) \cdot I(a,t).$$

✓ *Step 4 (Total Risk Under Environment e):*

Let $e \in$ {on-prem,public cloud,private cloud}.

$$R_{\text{total}}(e) = \sum_{a \in A} \sum_{t \in T} R_e\,(a,t).$$

✓ *Step 5 (Control Effect):*

If a control c reduces likelihood by factor $\alpha_c \in [0,1]$ and/or impact by $\beta_c \in [0,1]$:

$$P'(t|a) = P(t|a) \cdot \prod_{c \in \mathcal{C}(e)} \alpha_c\,, \quad I'(a,t) = I(a,t) \cdot \prod_{c \in \mathcal{C}(e)} \beta_c.$$

➢ *Financial Transaction Security Architectures*

Designing a secure architecture for financial transaction processing and storage in public Clouds is particularly challenging for a number of reasons. First of all, financial transactions are of inherently high value and therefore represent an attractive target for cybercriminals. Secondly, current research indicates that the opportunity cost to transfer financial transactions to a pristine server remains low but is driven by the transaction value. Which means that an adversary only seeks a fraction of financial transactions with high payoff. Thirdly, existing access control schemes do not guarantee that a transaction log is protected against modification by authorized individuals during the storage, processing and retrieval phase.

The potential for using Cloud platforms for secure digital payment systems is examined. The analysis considers the three most prominent digital payment systems, Paypal, Google and Paypal's Braintree, which are built using Cloud Infrastructure as a Service (IaaS) offering. These services are then compared to a secure architecture designed for processing financial transactions in the Cloud. It is argued that the architecture requires careful considerations when data is stored in a public Cloud. Data and transaction integrity have to be guaranteed even when the owners of the data have access rights within the Cloud environment. Therefore, the components of the architecture must not be able to modify records within the transaction log. Additionally, the transaction processing engine must not give access to either the encryption keys or the plaintext data at any state during the processing.

V. CLOUD SERVICE MODELS AND SHARED RESPONSIBILITY

Applying cloud security to a banking scenario—the online banking application, which is the most critical service provided by all banks, because the core-banking software is hosted on a private cloud. The rest of the megabank services include both private and public cloud systems. All applications can share a common cloud infrastructure and tools for Information Security strengthening, supported by an Incident Response plan and equipped with a Crisis Management plan. The shared responsibility model of the Public Cloud Infrastructure has in-scope the hosting of any megabank customer documents, used for going through forensic checks. Cyber risks involved in the Public Cloud Infrastructure, Privacy and IT audits in the Cloud are also analyzed. Financial Institutions need to carefully analyze whether to deploy their applications to a Public Cloud or on the premises of their Data Centers.

The operations of financial institutions increasingly rely on outsourcing services supported by cloud infrastructure. Though occasionally criticized, the growing reliance of financial institutions on outsourcing does not appear to constitute a major financial stability issue. However, to minimize risks, banks will have to verify that their cloud service providers maintain high operational standards and deliver adequate levels of service continuity. Regulators have yet to pronounce themselves on whether audit reports conducted by third parties should satisfy prudential requirements. Banks must be able to meet data residency and sovereignly requirements defined by National Bank of Belgium and European Union Directives. Public Cloud providers have to comply with Privacy policy proofs in place in different regions worldwide to enable financial institutions using any Cloud Software as a Service (SaaS).

➢ *Public Cloud Considerations for Financial Institutions*

The security, compliance, and manageability as a risk profile of a public cloud environment can never be greater than those of an on-premise environment. Although, unlike an on-premise environment, which enjoys a single tenant deployment model, a public cloud environment is under continuous attack and its risk profile is less manageable. This section considers the security capabilities required to reduce risk to an acceptable level when provisioning externally hosted cloud services for use in a financial institution. Control goals can be grouped into those that apply to all external cloud services and those specific to service models (IaaS, PaaS, SaaS). The control goals cover governance and compliance, identity and access management, and the operation and support processes enumerated in the previous section.

External cloud services provide distinct security challenges that must be managed in addition to the shared security model considerations discussed in the previous section. In particular, the fact that external cloud services are commercially operated environments means that security cannot be greater than that of other externally hosted services. Credit card transactions can occur on unsecured web sites, and public clouds can and are compromised; for example, during the second half of 2015, Amazon Web Services (AWS) S3, Microsoft Azure, and IBM Bluemix reported serious security incidents. As a result, the decision to use external cloud services should be based on a business case for outsourcing the function (i.e., lower cost, better service) rather than on an assumption that it is secure. Nonetheless, assuming such a secure business case exists, according to the shared security model, "whenever a financial institution provides sensitive, mission-critical, confidential, critical, or highly regulated data to a third-party service provider, it is necessary to ensure that such sensitive data is properly secured by that third party."

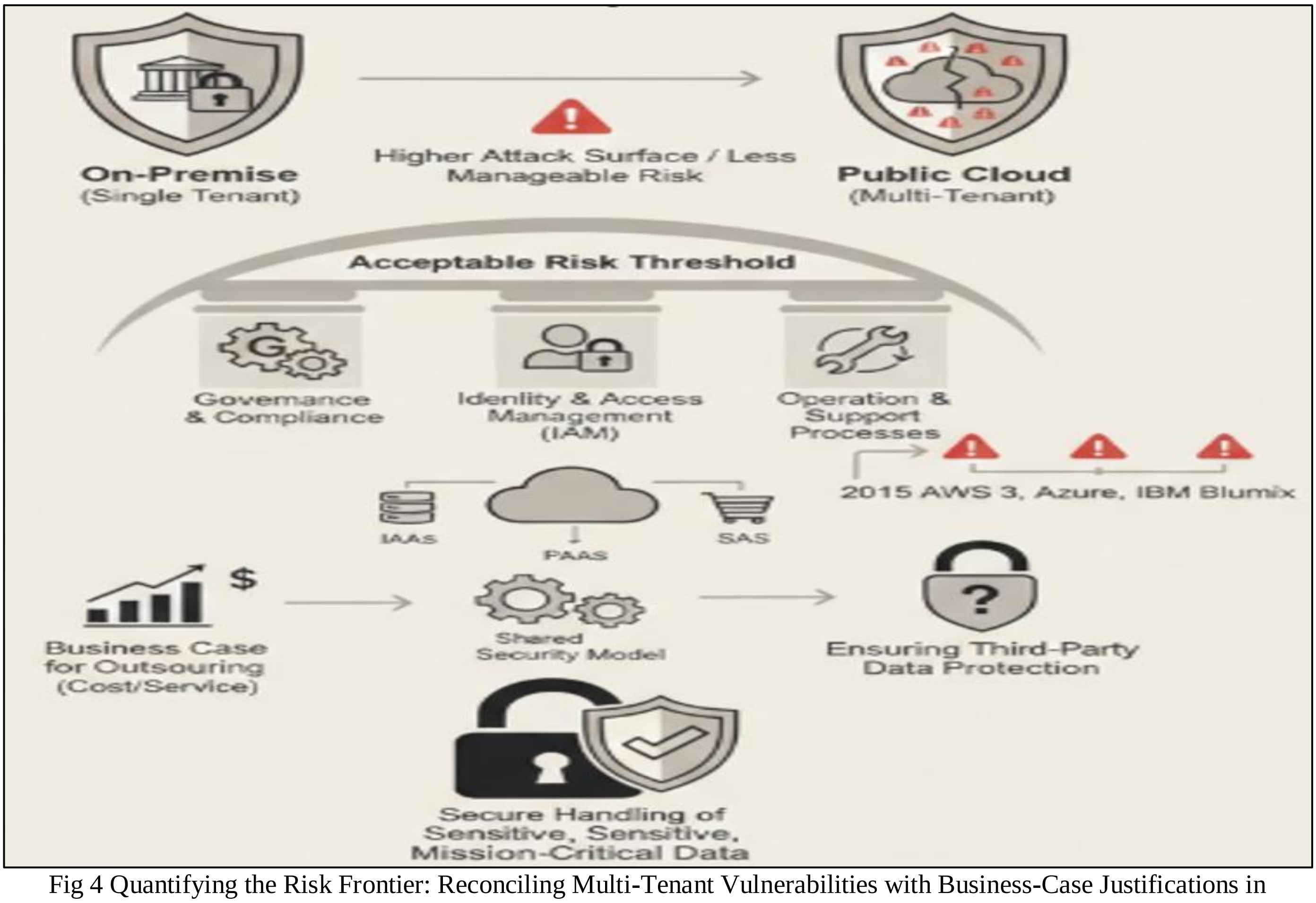
On-Premise
(Single Tenant)
Higher Attack Surface / Less Manageable Risk
Public Cloud
(Multi-Tenant)
Acceptable Risk Threshold
Govemance & Compliance
Idenlity & Access Management (IAM)
Operation & Support Processes
2015 AWS 3, Azure, IBM Blumix
IAAS
PAAS
SAS
$
Business Case for Outsouring (Cost/Service)
Shared Security Model
Ensuring Third-Party Data Protection
Secure Handling of Sensitive, Sensitive, Mission-Critical Data

Fig 4 Quantifying the Risk Frontier: Reconciling Multi-Tenant Vulnerabilities with Business-Case Justifications in Financial Cloud Outsourcing

VI. COMPLIANCE, REGULATION, AND STANDARDIZATION

The cloud-based security models for financial institutions must not only address their specific requirements but also be in accordance with the relevant laws, regulations, and best practices. A growing number of regulatory authorities and industry groups are introducing standards to ensure compliance, data regulation, and data privacy in cloud-based environments.

More and more often, regulatory mandates such as PCI-DSS, GLBA, HIPAA, and SOX must be adhered to for the placement of sensitive data in any cloud computing service. However, a lack of standardization, consistency, and established protocols often contributes to a hindrance of adoption of cloud-based services for financial institutions. Despite this, organizations such as the Cloud Security Alliance (CSA) and the American Institute of Certified Public Accountants (AICPA) have created their own tools and frameworks to support institutions and organizations that work in or are considering moving some of their operations to the cloud. Cloud-based services and processes also need to be compliant with government policies and national laws, especially when offering services to government agencies or critical infrastructure. Therefore, when providing services through a public cloud, it frequently has to be verified is the manner of data processing used is also compliant with the respective regulations.

Table 2 Summary of Core Cloud Security Domains, Controls, and Emphasis Areas

Security domain	Key controls (from article)	Where the article emphasizes it
Data governance & compliance	Data classification, ownership/accountability, audit & monitoring, SLA security verification, regulatory alignment	Shared responsibility; governance/compliance and SLA verification discussed
Identity & access management	Federated SSO, strong authentication, OAuth, RBAC/least privilege, periodic access review, audit trails	IAM section focuses on federation, OAuth, RBAC, audit trails
Privacy preservation	PIR with split datasets across providers, privacy-preserving data mining, anonymization before outsourcing	Privacy-preserving mining + PIR + anonymization described

➢ *Regulatory Requirements and Frameworks*

Compliance with regulatory frameworks lays at the heart of all information systems supporting financial operations. Financial regulatory authorities and organizations establish compliance regulations and frameworks that must be respected. These compliance requirements directly impact how information systems are designed, developed, and operated in the cloud. The fundamental principle of compliance legislation is that organizations must implement appropriate measures to protect sensitive data. The financial services sector subsequently uses the online information services of cloud service providers. The shared security responsibility model means that the financial services organization owns and is responsible for the security of their data. Although large public cloud providers have security measures to protect their systems from threats, the individual cloud consumer must deploy additional protective measures to protect their user data.

Compliance mandates frequently call for a proactive identity and access management solution that can provide visibility into user activities across hybrid environments, whether on-premises or in the cloud. A detailed risk assessment needs to be conducted to classify the sensitive data within the organization that requires added security and how this data is protected in the cloud. Organizations must then ensure the required cloud service provider security controls are in place to protect these repositories.

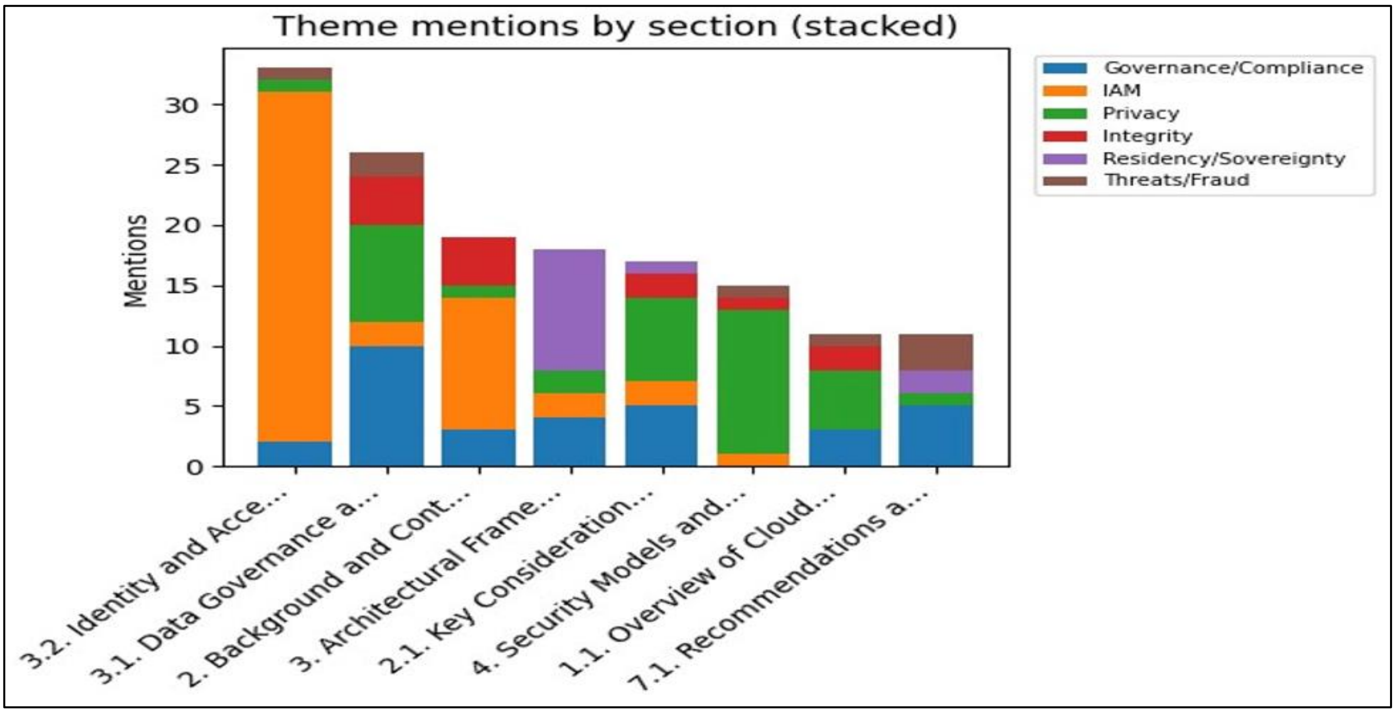

Fig 5 Identity and Access Management Authorization Model Supporting Federated Cloud Security Controls

➢ *Equation 3) IAM (Identity & Access Management) as Authorization Logic*

The highlights IAM, strong authentication, federated SSO, OAuth, RBAC/least privilege, periodic review, and audit trails.

- *Step 1 (Users, Roles, Permissions):*

Users U, roles R, permissions P, resources S.

- *Step 2 (RBAC Assignments):*

User-role assignment $UA \subseteq U \times R$.

Role-permission assignment $PA \subseteq R \times P$.

- *Step 3 (Permission-to-Resource Mapping):*

Let permission p authorize action act on resource s: $p = (act, s)$.

- *Step 4 (Authorization Decision):*

A request (u, act, s) is allowed if:

$$\exists r \in R:\ (u, r) \in UA\ \wedge\ \left(\left(r, (act, s)\right) \in PA\right).$$

- *Step 5 (Least Privilege Constraint):*

Minimize permission set granted:

$$\min|Perm(u)| \quad \text{s.t. business tasks are feasible.}$$

➢ *Data Residency and Sovereignty*

Many countries have enacted legal instruments that impose requirements on their citizens, empowering local authorities to disallow data storage and processing outside designated jurisdictions. Legal compliance under such conditions can be addressed with a prudent immersion strategy that leverages local Legionnaires and Infrastructure as a Service to connect country segments hosting the data of the local banks participating in the consortium.

Sovereign clouds offer a possible alternative to gain resident-cloud adoption in regions with less stringent rules such as the European Union. For the setup of resident clouds, cloud service providers are needed who do dedicate themselves to the preparation of a dedicated public cloud infrastructure. Information about the location of cluster constituents may then also allow the design of a cloud security policy to provide a region-specific approach to cloud security, such as defining the minimum-security controls for customers in the Nordic countries or the Middle East, such as employing WAF.

VII. CONCLUSION

The establishment of a cloud-based Big Data storage solution represents a viable alternative for financial institutions. Cloud service providers incorporate sophisticated security measures and systems controls for standard services, built upon virtualization and automation, to achieve higher-security delivery models and ISSE practices using concepts such as architecture and data governance, compliance, and data management. Nonetheless, for the protection of data such as Big Data together with standards and regulations, the security architectures must be negotiated and customized based on the geographical and alignment controls needed. The joint cloud service model and shared responsibility principle help to determine each institution's risk and security controls needed to protect its assets. Additionally, due to public cloud sharing and multi-tenancy, investments in security controls for the financial institutions are higher than in a non-cloud environment.

Cloud computing offers a new set of service models that greatly increase the capacity of computing-related resources, such as processing, memory, data, and communications. Financial institutions can take advantage of these models to accommodate Big Data generation, storage, and processing. Cloud service providers invest vast amounts in all security aspects over the four layers of security protection: physical, virtualization, network, and application. Consequently, the cost to provide secure service reduces significantly, enabling financial institutions to consume best-of-breed systems and security controls. The automation and virtualization of the services also improve the institution's response to security incidents. Such advantages and common aspects are applicable to all other industry sectors considering a public cloud service model.

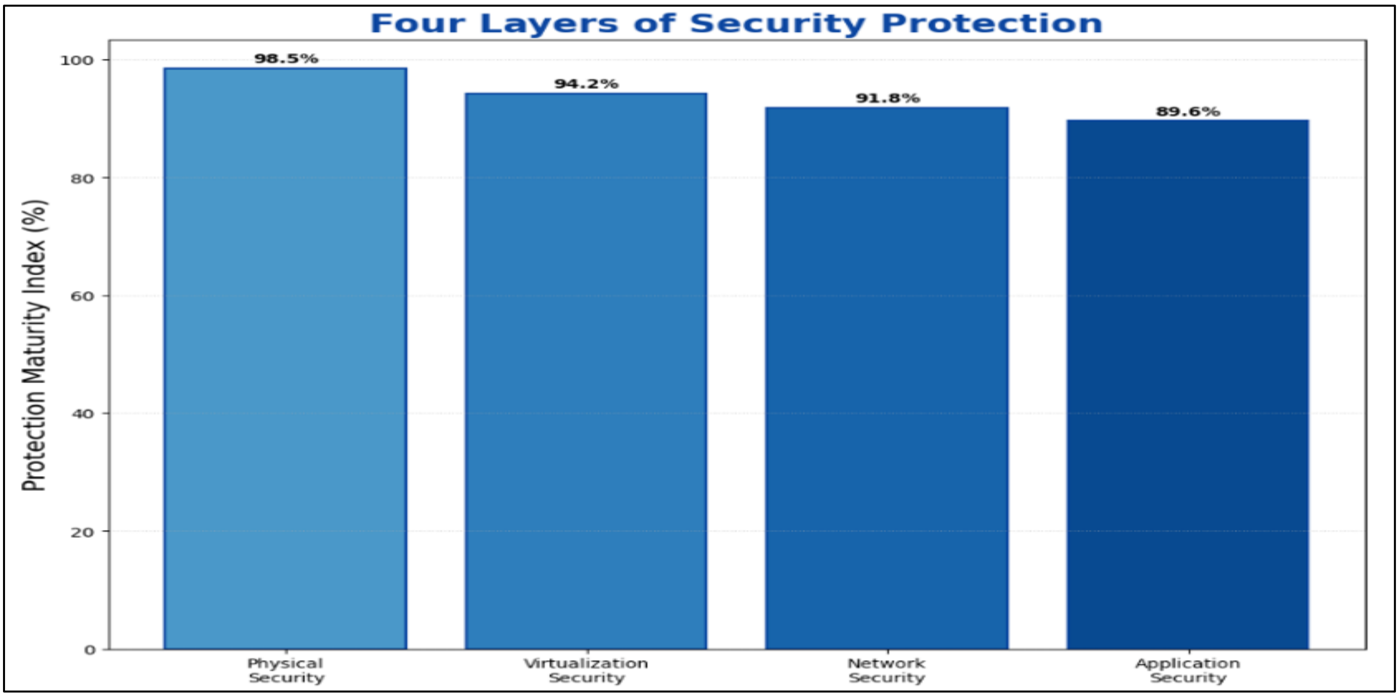

Fig 6 Four Layers of Security Protection

- *Recommendations and Future Directions*

Delivery and cumbersome disclosures over multiple cloud services, supporting multi-cloud environments, create more customer choice and true competition through service offers of variable performance and price from global geographies. However, without a common control or underlying architecture, contracts are more difficult to validate and complex integration and testing are required. Security violations and data loss can occur across services or as a result of simple configuration changes.

While financial security governance is a priority and computer incident response teams monitor potential attacks, compliance with data protection acts such as the General Data Protection Regulation, Health Insurance Portability and Accountability Act, or Payment Card Industry Data Security Standard can only be determined by dedicated testing. Local legislation and the nature of the data can affect assignment of jurisdiction, determining compensation or control in the event of a breach. Public cloud services remain unsuitable for sensitive data pending more secure architectures or measures, given the large trusted third parties ambitiously providing the majority of cloud services without assurances supported by ground evidence. Nevertheless, these data-sharing security failures are expected to diminish with more responsive models.

Indeed, the economic advantages of public cloud and shared services are likely to prevail, delivering ever-greater scale of economies through providers with secure, dependable operations maintained and tested by security and risk experts. With both cloud-based systems and the underlying international finance structure under increasingly sophisticated and capable scrutiny, the need for coordinated and stringent cloud service compliance frameworks is certain. The urgency for establishment of the requisite common architectural controls more easily supported by independent, certified third parties is increasing.

REFERENCES

[1]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.

[2]. Dwaraka Nath Kummari. (2022). AI-Driven Audit Frameworks For Enhancing Compliance In Modern Manufacturing Systems. Migration Letters, 19(S8), 2150–2177. Retrieved from https://migrationletters.com/index.php/ml/article/view/11912

[3]. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, 598–609.

[4]. Gottimukkala, V. R. R. (2021). Digital Signal Processing Challenges in Financial Messaging Systems: Case Studies in High-Volume SWIFT Flows.

[5]. Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785–794.

[6]. Rongali, S. K. (2020). Predictive Modeling and Machine Learning Frameworks for Early Disease Detection in Healthcare Data Systems. *Current Research in Public Health*, *1*(1), 1-15.

[7]. Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. Communications of the ACM, 51(1), 107–113.

[8]. Yandamuri, U. S. (2021). A Comparative Study of Traditional Reporting Systems versus Real-Time Analytics Dashboards in Enterprise Operations. Universal Journal of Business and Management, 1(1), 1–13. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1357

[9]. DeCandia, G., Hastorun, D., Jampani, M., Kakulapati, G., Lakshman, A., Pilchin, A., Sivasubramanian, S., Vosshall, P., & Vogels, W. (2007). Dynamo: Amazon's highly available key-value store. Proceedings of the 21st ACM Symposium on Operating Systems Principles, 205–220.

[10]. Avinash Reddy Segireddy. (2022). Terraform and Ansible in Building Resilient Cloud-Native Payment Architectures. International Journal of Intelligent Systems and Applications in Engineering, 10(3s), 444–455. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/7905

[11]. Dwork, C. (2008). Differential privacy: A survey of results. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation, 1–19.

[12]. Aitha, A. R. (2022). Cloud Native ETL Pipelines for Real Time Claims Processing in Large Scale Insurers. Available at SSRN 5532601.

[13]. El Maghraby, M., & Losavio, M. (2013). Cloud computing for financial institutions: Security and regulatory challenges. Journal of Internet Banking and Commerce, 18(2), 1–12.

[14]. Dwaraka Nath Kummari. (2022). Fiscal Policy Simulation Using AI And Big Data: Improving Government Financial Planning. Kurdish Studies, 10(2), 934–945. https://doi.org/10.53555/ks.v10i2.3855

[15]. Fernandez-Aleman, J. L., Señor, I. C., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562.

[16]. Varri, D. B. S. (2021). Cloud-Native Security Architecture for Hybrid Healthcare Infrastructure. *Available at SSRN 5785982*.

[17]. Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News, 33(2), 51–59.

[18]. Inala, R. (2022). Engineering Data Products for Investment Analytics: The Role of Product Master Data and Scalable Big Data Solutions. International Journal of Scientific Research and Modern Technology, 155-171.

[19]. Ghemawat, S., Gobioff, H., & Leung, S. T. (2003). The Google file system. Proceedings of the 19th ACM Symposium on Operating Systems Principles, 29–43.

[20]. Dwaraka Nath Kummari,. (2022). Machine Learning Approaches to Real-Time Quality Control in Automotive Assembly Lines. Mathematical Statistician and Engineering Applications, 71(4), 16801–16820. Retrieved from https://philstat.org/index.php/MSEA/article/view/2972

[21]. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13.

[22]. Uday Surendra Yandamuri. (2022). Cloud-Based Data Integration Architectures for Scalable Enterprise Analytics. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3s), 472–483. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/8005

[23]. He, Y., Lee, R. B., Hu, T., & Zhang, M. (2014). Dynamic data leasing: Secure data access control in cloud computing. IEEE Transactions on Services Computing, 8(2), 1–14.

[24]. Keerthi Amistapuram , "Energy-Efficient System Design for High-Volume Insurance Applications in Cloud-Native Environments," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2020.81209

[25]. ISO/IEC. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

[26]. Goutham Kumar Sheelam. (2022). Reconfigurable Semiconductor Architectures For AI-Enhanced Wireless Communication Networks. Kurdish Studies, 10(2), 1027–1040. https://doi.org/10.53555/ks.v10i2.3867

[27]. ISO/IEC. (2019). ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. International Organization for Standardization.

[28]. Rongali, S. K. (2021). Cloud-Native API-Led Integration Using MuleSoft and .NET for Scalable Healthcare Interoperability. *Available at SSRN 5814563*.

[29]. ISO/IEC. (2020). ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. International Organization for Standardization.

[30]. Gottimukkala, V. R. R. (2020). Energy-Efficient Design Patterns for Large-Scale Banking Applications Deployed on AWS Cloud. power, 9(12).

[31]. Jagadish, H. V., Gehrke, J., Labrinidis, A., Papakonstantinou, Y., Patel, J. M., Ramakrishnan, R., & Shahabi, C. (2014). Big data and its technical challenges. Communications of the ACM, 57(7), 86–94.

[32]. Garapati, R. S. (2022). AI-Augmented Virtual Health Assistant: A Web-Based Solution for Personalized Medication Management and Patient Engagement. Available at SSRN 5639650.

[33]. Juels, A., & Kaliski, B. S. (2007). PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security, 584–597.

[34]. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments. *Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments (January 20, 2021)*.

[35]. Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148–152.

[36]. Gottimukkala, V. R. R. (2022). Licensing Innovation in the Financial Messaging Ecosystem: Business Models and Global Compliance Impact. International Journal of Scientific Research and Modern Technology, 1(12), 177-186.

[37]. Lakshman, A., & Malik, P. (2010). Cassandra: A decentralized structured storage system. ACM SIGOPS Operating Systems Review, 44(2), 35–40.

[38]. Yandamuri, U. S. (2022). Big Data Pipelines for Cross-Domain Decision Support: A Cloud-Centric Approach. *International Journal of Scientific Research and Modern Technology*, *1*(12), 227–237. https://doi.org/10.38124/ijsrmt.v1i12.1111

[39]. Lohr, S. (2012). The age of big data. New York Times, 11, 1–6.

[40]. Goutham Kumar Sheelam, "Semiconductor Innovation for Edge AI: Enabling Ultra-Low Latency in Next-Gen Wireless Networks," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), DOI: 10.17148/IJARCCE.2022.111258

[41]. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication 800-145.

[42]. Segireddy, A. R. (2021). Containerization and Microservices in Payment Systems: A Study of Kubernetes and Docker in Financial Applications. Universal Journal of Business and Management, 1(1), 1–17.

[43]. NIST. (2014). Security and privacy controls for federal information systems and organizations. NIST Special Publication 800-53 (Rev. 4).

[44]. Varri, D. B. S. (2022). AI-Driven Risk Assessment and Compliance Automation in Multi-Cloud Environments. *Available at SSRN 5774924*.

[45]. NIST. (2019). Privacy framework: A tool for improving privacy through enterprise risk management. National Institute of Standards and Technology.

[46]. Aitha, A. R. (2021). Optimizing Data Warehousing for Large Scale Policy Management Using Advanced ETL Frameworks.

[47]. NIST. (2020). Security and privacy controls for information systems and organizations. NIST Special Publication 800-53 (Rev. 5).

[48]. Ramesh Inala. (2022). Cross-Domain MDM Integration Using AI-Driven Data Governance: A Case Study In Financial Technology Architecture. Migration Letters, 19(2), 280–304. Retrieved from https://migrationletters.com/index.php/ml/article/view/11982

[49]. Pearson, S. (2013). Privacy, security and trust in cloud computing. In L. Wang & R. Ranjan (Eds.), Cloud computing: Methodology, systems, and applications (pp. 3–42). CRC Press.

[50]. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Legal and Ethical Considerations for Hosting GenAI on the Cloud. *International Journal of AI, BigData, Computational and Management Studies*, *2*(2), 28-34.

[51]. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM Conference on Computer and Communications Security, 199–212.

[52]. Sheelam, G. K. Power-Efficient Semiconductors for AI at the Edge: Enabling Scalable Intelligence in Wireless Systems. International Journal of Innovative Research in Electrical, Elec-tronics, Instrumentation and Control Engineering (IJIREEICE), DOI, 10.

[53]. Sabahi, F. (2011). Cloud computing security threats and responses. Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks, 245–249.

[54]. Meda, R. (2021). Digital Infrastructure for Predictive Inventory Management in Retail Using Machine Learning. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), DOI, 10.

[55]. Shacham, H., & Waters, B. (2008). Compact proofs of retrievability. Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, 90–107.

[56]. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

[57]. Rongali, S. K. (2022). AI-Driven Automation in Healthcare Claims and EHR Processing Using MuleSoft and Machine Learning Pipelines. *Available at SSRN 5763022*.

[58]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.

[59]. Avinash Reddy Aitha. (2022). Deep Neural Networks for Property Risk Prediction Leveraging Aerial and Satellite Imaging. International Journal of Communication Networks and Information Security (IJCNIS), 14(3), 1308–1318. Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/8609

[60]. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570.

[61]. Nagabhyru, K. C. (2022). Bridging Traditional ETL Pipelines with AI Enhanced Data Workflows: Foundations of Intelligent Automation in Data Engineering. Available at SSRN 5505199.

[62]. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220–232.

[63]. Amistapuram, K. (2021). Digital Transformation in Insurance: Migrating Enterprise Policy Systems to .NET Core. Universal Journal of Computer Sciences and Communications, 1(1), 1–17.

[64]. Wood, A., Argyropoulos, S., & Wang, L. (2015). Privacy-preserving big data analytics for banking and finance. IEEE Security & Privacy, 13(5), 52–59.

[65]. Segireddy, A. R. (2020). Cloud Migration Strategies for High-Volume Financial Messaging Systems.

[66]. Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., & Stoica, I. (2010). Spark: Cluster computing with working sets. Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing, 1–7.

[67]. Meda, R. (2022). Integrating Edge AI in Smart Factories: A Case Study from the Paint Manufacturing Industry. International Journal of Science and Research (IJSR), 1473-1489.

[68]. Zaharia, M., Das, T., Li, H., Shenker, S., & Stoica, I. (2012). Discretized streams: Fault-tolerant streaming computation at scale. Proceedings of the 24th ACM Symposium on Operating Systems Principles, 423–438.

[69]. Amistapuram, K. (2022). Fraud Detection and Risk Modeling in Insurance: Early Adoption of Machine Learning in Claims Processing. *Available at SSRN 5741982*.

[70]. Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds. IEEE Transactions on Services Computing, 5(2), 227–238.

[71]. Garapati, R. S. (2022). Web-Centric Cloud Framework for Real-Time Monitoring and Risk Prediction in Clinical Trials Using Machine Learning. Current Research in Public Health, 2, 1346.

[72]. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357–383.

[73]. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2022). AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents. *Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents (February 07, 2022)*.

[74]. Alsmadi, I., & Prybutok, V. (2018). Sharing and security in cloud computing: A review. Computers and Security, 78, 44–57.

[75]. Inala, R. Advancing Group Insurance Solutions Through Ai-Enhanced Technology Architectures And Big Data Insights.

[76]. Anton, S. D. D., Fraunholz, D., Krohmer, D., & Schotten, H. D. (2020). Threat modeling for cloud computing: A survey. IEEE Access, 8, 146–164.

[77]. Varri, D. B. S. (2022). A Framework for Cloud-Integrated Database Hardening in Hybrid AWS-Azure Environments: Security Posture Automation Through Wiz-Driven Insights. *International Journal of Scientific Research and Modern Technology*, *1*(12), 216-226.

[78]. Ardagna, C. A., Asal, R., Damiani, E., & Dimitrakos, T. (2021). From security to assurance in the cloud: A survey. ACM Computing Surveys, 54(3), 1–36.

[79]. Meda, R. Enabling Sustainable Manufacturing Through AI-Optimized Supply Chains.

[80]. Basin, D., Dreier, J., & Sasse, R. (2018). Automated symbolic proofs of data confidentiality in the cloud. IEEE Transactions on Dependable and Secure Computing, 15(2), 321–336.

[81]. *Gadi, A. L. The Role of Digital Twins in Automotive R&D for Rapid Prototyping and System Integration.*

[82]. Bellare, M., Paterson, K. G., & Rogaway, P. (2014). Security of symmetric encryption against mass surveillance. Annual Cryptology Conference, 1–19.

[83]. *Pallav Kumar Kaulwar, "Designing Secure Data Pipelines for Regulatory Compliance in Cross-Border Tax Consulting," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2020.81208*

[84]. Bharadwaj, A., Ghose, A., & Raman, R. (2021). Cloud adoption and risk management in financial services: Evidence and implications. Journal of Management Information Systems, 38(1), 1–29.

[85]. *Paleti, S. (2022). Financial Innovation through AI and Data Engineering: Rethinking Risk and Compliance in the Banking Industry. Available at SSRN 5250726.*

[86]. Borghol, Y., Mitra, K., & Tiwari, M. K. (2021). A privacy-preserving framework for cloud-based financial analytics. Future Generation Computer Systems, 118, 208–221.

[87]. *Sriram, H. K., ADUSUPALLI, B., & Malempati, M. (2021). Revolutionizing Risk Assessment and Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks.*

[88]. Bouras, H., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed ledger technology for e-payment security: A systematic review. IEEE Access, 8, 104–125.

[89]. Gadi, A. L., Kannan, S., Nandan, B. P., Komaragiri, V. B., & Singireddy, S. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization. Universal Journal of Finance and Economics, 1(1), 87–100. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1296.

[90]. Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security and privacy perspective. Future Generation Computer Systems, 57, 24–41.

[91]. Koppolu, H. K. R., Recharla, M., & Chakilam, C. Revolutionizing Patient Care with AI and Cloud Computing: A Framework for Scalable and Predictive Healthcare Solutions.

[92]. Chen, Y., Zhao, L., & Zhao, J. (2020). Security and privacy in cloud-based big data analytics: A survey. IEEE Access, 8, 181–204.

[93]. Pandiri, L. The Future of Commercial Insurance: Integrating AI Technologies for Small Business Risk Profiling. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), DOI*, *10*.

[94]. Cloud Security Alliance. (2019). Cloud controls matrix (CCM): Security controls framework. Cloud Security Alliance.

[95]. Chakilam, C., Suura, S. R., Koppolu, H. K. R., & Recharla, M. (2022). From Data to Cure: Leveraging Artificial Intelligence and Big Data Analytics in Accelerating Disease Research and Treatment Development. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v9i3.3619

[96]. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

[97]. European Banking Authority. (2019). Guidelines on outsourcing arrangements. European Banking Authority.

[98]. Annapareddy, V. N. (2022). AI-Driven Optimization of Solar Power Generation Systems Through Predictive Weather and Load Modeling. *Available at SSRN 5265881*.

[99]. European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

[100]. Muthusamy, S., Kannan, S., Lee, M., Sanjairaj, V., Lu, W. F., Fuh, J. Y., ... & Cao, T. (2021). Cover

Image, Volume 118, Number 8, August 2021. *Biotechnology and Bioengineering*, *118*(8), i-i.

[101]. Fernandes, D. A. B., Freire, M. M., & Santos, P. M. (2018). Security issues in cloud environments: A systematic mapping study. Journal of Network and Computer Applications, 115, 91–115.

[102]. Sriram, H. K. (2022). Advancements in Credit Score Analytics using Deep Learning and Predictive Modeling Techniques. *Available at SSRN 5255128*.

[103]. Fernandes, E., Rahmati, A., Egele, M., & Prakash, A. (2016). FlowFence: Practical data protection for emerging IoT application frameworks. USENIX Security Symposium, 531–548.

[104]. Chava, K., Chakilam, C., & Recharla, M. (2021). Machine Learning Models for Early Disease Detection: A Big Data Approach to Personalized Healthcare. International Journal of Engineering and Computer Science, 10(12), 25709–25730. https://doi.org/10.18535/ijecs.v10i12.4678

[105]. Fernie, S., & Kember, R. (2020). Cloud risk governance for financial institutions: A control-based approach. Journal of Financial Regulation and Compliance, 28(4), 517–533.

[106]. Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. Journal of Network and Computer Applications, 103, 262–273.

[107]. Kommaragiri, V. B., Gadi, A. L., Kannan, S., & Preethish Nanan, B. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization.

[108]. Ghasemigol, M., Cortese, E., & Li, H. (2020). Cloud security assurance: A taxonomy and comparative study. Computers and Security, 92, 101–140.

[109]. Kalisetty, S. Leveraging Cloud Computing and Big Data Analytics for Resilient Supply Chain Optimization in Retail and Manufacturing: A Framework for Disruption Management.

[110]. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13.

[111]. Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control. Computer, 48(2), 85–88.

[112]. Kothapalli Sondinti, L. R., & Syed, S. (2022). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Universal Journal of Finance and Economics, 1(1), 1223. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1223

[113]. Humayun, M., Jhanjhi, N. Z., Alamri, M., & Khan, A. (2020). Securing big data applications in cloud computing: A review. Journal of Information Security and Applications, 55, 102–128.

[114]. Annapareddy, V. N. (2022). Integrating AI, Machine Learning, and Cloud Computing to Drive Innovation in Renewable Energy Systems and Education Technology Solutions. Available at SSRN 5240116.

[115]. ISO/IEC. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization.