**Enhancing Financial Cybersecurity through Cloud Engineering: A Systematic Review of Threats, Mitigation Strategies, and Regulatory Compliance**

**ABSTRACT**

**Aims**: In the digital economy, where financial transactions are conducted online, cybersecurity poses a significant threat. This review analyses the intersection of cloud engineering and cybersecurity in the financial sector, highlighting how advanced cloud technologies can improve defenses against cyber threats for safe evolution. The first aim is to examine modern methodologies, frameworks, and technologies that enhance financial cybersecurity through cloud-based solutions.

**Methodology:**  A comprehensive literature review methodology is employed to assess existing studies that explore prevalent trends and challenges based on peer-reviewed articles, technical reports, and industry case studies.

**Result and Discussion:** It thoroughly investigates the methods of evaluating risks related to data breaches, phishing attacks, and ransomware, utilising principles of cloud engineering, including scalability, elasticity, and automation. The assessment focuses on key cloud security tools, such as zero trust models, encryption techniques, and multi-cloud strategies, for their effectiveness in securing financial operations. While cloud adoption introduces new vulnerabilities, it also offers robust tools for proactive threat detection and response. Furthermore, the importance of adhering to established cloud security practices is discussed, along with compliance with common regulations like GDPR, PCI-DSS, and ISO/IEC.

**Conclusion:**  Finally, the review recommends that future research should focus on developing AI-driven security orchestration platforms, enhancing cloud governance models, and exploring socio-technical aspects of cybersecurity. Additionally, it advocates for an empirical investigation into the economic and operational impacts of device cloud-type transformations over time.

***Keywords****: Financial Cybersecurity, Cloud Engineering, Zero Trust Architecture, Risk Management, Secure Cloud Infrastructure*

**1.0 Introduction**

**1.1 Literature Review**

The financial cybersecurity challenges that arise from the use of cloud services by financial institutions are significant with the rate at which financial institutions are adopting cloud nature to improve their operations’ efficiency and flexibility. The studies indicate that organizations are prone to cybersecurity threats such as data breaches, insider threats, account hijacking and advanced persistent threats, to name a few, and more specifically in multi-tenant environments where technology shared vulnerabilities abound (Lampe et al., 2013). And because of the complexity of the outsourced infrastructures, it becomes harder to be visible and to control, thereby making it impossible to protect sensitive financial data (Yalamati, 2024). In addition, this further complicates the process of regulatory compliance because any financial institution has to adhere to vast legal structures and must enforce seamless security schemes (Nicoletti, 2013). Research shows often financial institutions are often the common targets of malicious actors such as disgruntled employees and state-sponsored hackers, especially larger organizations subjected to different threats than smaller community banks (Skelton, 2017). For example, if cyber-attacks are a reality, it is not just an issue of an individual company because the potential consequences of cyber-attacks are systemic, as shown in the rather dramatic projections of the costs of malicious cyber-attacks in the sector (Harvey, 2018).

Countermeasures in the technical space include encryption, identity and access management (IAM), intrusion detection systems (IDS), as well as secure APIs, all of which are important to protect cloud-deployed assets against such risks as data tampering and leakage (Alouffi et al., 2021), (Alotaibi et al., 2021). On the organizational front, the strategies for employee training, cybersecurity awareness programs and incident response planning are key items in a layer of defense which makes cloud environments more secure on a whole (Betcher, 2010; Latif et al., 2014). In addition, mitigating appropriate models in each security threat, which are specifically designed, are essential for efficient risk management across diverse cloud environments (Tanna et al., 2019). Blockchain, with its tamper-proof decentralized nature, addresses the vulnerabilities of traditional cloud storage in (Zheng et al., 2019), (Dong et al., 2018), which improves the whole security framework with the help of AI in enhancing operational efficiency and malicious behavior detection. For example, blockchain can be used to securely share cloud audit data by consensus mechanisms and smart contracts, however, the quality assurance and operational maintenance challenges remain (Dong et al., 2018; Baalamurugan et al., 2021). Additionally, combining AI with blockchain involves issues in ensuring privacy protection for users and having a strong authorization and access control scheme, which are the intricacies of using these technologies in actual circumstances (Li et al., 2023).

Infrastructure as code (IaC), DevSecOps and CI/CD are practices that are widely accepted in the industry as they are capable of streamlining cybersecurity resilience and automation of compliance in the financial sector. There are, however, challenges when it comes to implementing these practices as financial institutes have legacy systems, siloed teams, and little to no technical expertise (Mohammed, 2015; Rajapakse et al., 2022). According to research, although DevSecOps combines security into the software development lifecycle to be more compliant, ensuring compliance is still difficult without looking into more automated compliance methods (Ramaj et al., 2022; Chavan et al., 2022).

In cloud-deployed environments, there are major challenges for banks to bridge the gap between regulatory expectations and actual security implementation. Most organizations can align their cloud security frameworks to other standards such as ISO/IEC 27001, NIST, and GDPR, but some keep falling behind due to vague guidelines and high compliance costs that hinder them from adopting the proper security measures (Mohammed, 2015; Pierotti, 2018). Often, cloud services are identified as serving as a weak link to the operational security of the services, which calls for new technologies to meet evolving regulatory trends (Herardian, 2019). However, research has shown that cloud computing affords these benefits not without security challenges, such as data breaches and compliance risks arising out of GDPR and PCI DSS, among others (Yalamati, 2024). Implementing such strategies as Continuous Integration and Continuous Deployment (CI/CD) pipelines automates security checks and reduces deployment time to join compliance with the minimum requirement while automating and reducing time to remediate. Also, techniques for advanced encryption and strong authentication are important to limit cyber threats and keep data private.

**1.2 Purpose of the Study**

Currently, there is a gap in regards to well-executed research that has focused on cloud engineering and cybersecurity separately, without consideration of their integration in the financial sector, and this manuscript takes on some of the issues on that. This is emphasized by the lack of tailored security frameworks for cloud environment management of financial data, which are sensitive to their threats. In addition, the study highlights the need for cloud native security model in a dynamic cloud environment, as standard models may not fit in the dynamic cloud environment. Additionally, there are very few empirical studies or use cases shown to validate the ability of cloud engineering to boost cybersecurity in financial institutions. This study synthesizes the current knowledge in these domains to inform financial institutions, cloud service providers, policymakers and researchers about what level of best practices and future directions can be pursued for improving cybersecurity resilience through cloud engineering.

**1.3 Objectives of the Study**

The objective of this study is to identify and classify the main cybersecurity threats that financial institutions are confronted with in cloud computing applications. There are external attacks, insider threats, data breaches, and vulnerabilities on your system, and they focus on what causes them and what their prevalence is within in the financial sector.

The evaluation will also cover the efficiency of current cloud-based mitigation techniques like encryption, access controls, artificial intelligence driven monitoring and adopted security frameworks in dealing with the particular cybersecurity challenges that are faced by the financial institutions.

Further, the exploration includes the adoption of the secure cloud engineering practices: DevSecOps, Infrastructure-as-Code (IaC) as well and continuous security integration. By assessing these practices, the assessment will determine how they help in building proactive, resilient, scalable security architectures in financial environments.

The work concludes by evaluating the level of alignment between the practices of current cloud security implementations in financial institutions and the national and international regulatory standards (such as GDPR, NIST, ISO/IEC 27001, etc.) and the gaps between policy requirements and existing practices.

**2.0 Methods**

**2.1 Literature Search Strategy**

This literature review was conducted systematically using the academic databases such as Scopus, Web of Science and Google Scholar. Other key words were: ‘cloud engineering in cybersecurity’, ‘financial cybersecurity frameworks’, ‘Increased threat detection facilitated by cloud computing’, ‘Improvements on data protection via cloud computing’. What was reviewed was peer reviewed article; technical reports; and case studies which discussed integration of cloud engineering in improving financial cybersecurity systems.

**2.2 Selection Criteria**

Articles were selected using the following inclusion and exclusion criteria:

**Inclusion criteria** **focused on studies that:**

1. Discussed the use of cloud engineering in financial or cybersecurity applications.
2. Provided empirical or case-based evidence of cloud-based security strategies.
3. Addressed the deployment of cloud services for threat detection, risk mitigation, or compliance in the financial sector.

**Exclusion criteria** **omitted studies that:**

1. Lacked empirical data or detailed methodological frameworks.
2. Focused purely on general cloud computing without reference to cybersecurity.
3. Did not include application in financial or similarly regulated environments.

From an initial pool of about 180 records, 16 papers and case studies were selected for their relevance and methodological robustness, while 164 were excluded according to the established criteria.

**Limitations of Methods:**

The present study is based on the literature and is of a qualitative nature. For broader applicability and generalizability of the findings, primary data collection or quantitative comparisons may be lacking. Nevertheless, the emphasis on the use of conceptual frameworks and applied case studies offers an depth understanding of the part of cloud engineering in enhancing financial cybersecurity.

**3.0 Results**

**3.1 Predominant Cybersecurity Threats in Cloud-Enabled Financial Systems**

Integration of the cloud technology with the financial sector created a complex landscape of cybersecurity threats present in both the human and technical vectors. About (Chintale et al., 2019) highlighted infrastructure misconfigurations and code vulnerabilities as factors in compromising financial cloud environments, especially within deployments of Infrastructure-as-a-Service (IaaS). In particular, these vulnerabilities become especially pressing when the environments have continuous deployment while lacking adequate oversight. Likewise, (Dopamu, 2024) performed a forensic analysis of the cybersecurity incidents in U.S. financial institutions and found that data breaches and credential theft are the most common threats. This highlights the lack of fit of static defense systems for quickly changing cloud contexts.

According to (Farayola, 2024), hybrid cloud deployments bring in new levels of complexity in terms of the control of malware propagation and unauthorized access. Traditional perimeter-based security models, as per his framework review, do not deliver in a hybrid setup. Identification of challenging threats of transforming banking ecosystems is done in conceptual work by (Farayola, 2024), namely fraud, data breaches and system intrusions. In testing AI/ML systems for banking, he points to numerous instances of fraud and data theft in live data streams that are processed in the cloud-hosted environment, as demonstrated in (Johora et al., 2024), and only in machine learning workflows.

The technical analysis by (Jabir et al., 2016) shows that similarly classic attacks such as SQL injections, Denial-of-Service (DoS), as well as spoofing were observed in such general-purpose cloud settings, where contextual security layering was not provided. Research from (Katari & Ankam, 2022) includes data leakage, vendor lock in, and interoperability problems in multi-cloud financial environments that tend to create vulnerability to service provider lock in and imbalance of locus of control. Similarly, in financial fraud detection systems (Kokogho et al., 2025) identified phishing, insider threats and fraud as recurring attack vectors, and the matter is further complicated by hybrid environments.

For example, (Madasamy, 2022) established that model drift in AI applications for banking and insurance can lead to poor governance that can be exploited to circumvent security measures or to employ biased decision-making. In (Masud et al., 2024), ML models are targeted or circumvented in systems that incurred data breaches or financial fraud. (Nagarajan, 2024) flagged other issues regarding data confidentiality and insider risks associated with SaaS and IaaS deployments, primarily the lack of visibility and control over cloud layers.

According to (Orelaja et al., 2024), which studies African banks, they see a high number of external hacks and fraud cases in the SaaS private cloud hybrid space that point to regional issues of underfunded security and lack of compliance efforts that spread across borders. Supply chain threats exposed by poorly secured CI/CD pipelines in the PaaS environment—including exploiting attack visas in dependencies—are shown to exist (Owoade et al., 2024). Payment fraud and insider threats were defined as pressing threats in hybrid cloud banking systems, exacerbated by complexity in the regulation and variation in the practices for governance of data (Sharma, 2021). Specifically, (Vadisetty, 2024) looked at data analytics breaches in large data models in hybrid architecture, where big datasets in a multi architecture increase the possibility of misuse of data, (Wang et al., 2024) discussed privacy issues and data leakage in financial cloud computing models and linked them to systemic concentration risks and uneven implementation of predictive technologies.

**Table 1: Case studies showing different cloud models and cyber security threats addressed**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Reference** | **Case Study** | **Study Methodology** | **Cybersecurity Threats Addressed** | **Cloud Model Focus** | **Mitigation Strategy Type** | **Secure Cloud Engineering Practice** | **Regulatory/Compliance Relevance.** | **Technology Stack** |
| **Owoade et al., 2024** | Fintech CI/CD pipelines | Applied systems case | Supply chain threats | PaaS | DevSecOps, automation | IaC, CI/CD | GDPR referenced |

|  |
| --- |
|  |

|  |
| --- |
| CI/CD tools |

 |
| **Chintale et al., 2019** | Financial cloud management | Technical implementation, DevOps adoption | Infrastructure misconfigurations, code vulnerabilities | IaaS | IaC, automated policy enforcement | Infrastructure as Code (IaC) | ISO 27001 (mentioned) | Terraform, Jenkins, AWS |
| **Dopamu, 2024** | US Financial Institutions | Forensic analysis of incidents | Data breaches, credential theft | Public Cloud | Forensic techniques, behavioral analysis | Microservices architecture | NIST | Log analysis tools |
| **Ejiofor, 2023** | US banking cybersecurity | Framework development, literature review | Malware, unauthorized access | Hybrid Cloud | Zero-trust framework, encryption | DevSecOps |

|  |
| --- |
|  |

|  |
| --- |
| NIST, ISO 27001 |

 | Encryption standards, firewalls |
| **Farayola, 2024** | Secure banking transformation | Conceptual integration framework | Fraud, data breaches, system intrusions | Hybrid Cloud | AI-based detection, blockchain verification | Microservices | GDPR, ISO 27001 referenced | AI, blockchain, BI tools |
| **Jabir et al., 2016** | Not a case study | Technical analysis | SQL injection, DoS attacks, spoofing, malware | General Cloud | Preventive controls (firewalls, encryption) | Access control, encryption | No direct regulatory references | Firewalls, intrusion detection, encryption |
| **Johora et al., 2024** | Banking/Fintech | Applied AI/ML system testing | Fraud, data breaches | Cloud-hosted AI system | AI-based fraud detection | Secure data ingestion, real-time analysis | GDPR, PCI DSS (implied from financial context) | Python, AI/ML stack |
| **Katari & Ankam, 2022** | Multi-cloud governance in finance | Case study & solution modeling | Data leakage, vendor lock-in, interoperability issues | Multi-Cloud | Governance framework | Microservices, data federation | ISO 27001, SOC 2 | API gateways, containerization |
| **Kokogho et al., 2025** | Cybersecurity fraud detection in finance | Framework development | Financial fraud, phishing, insider threats | Hybrid Cloud | AI-based detection, microservices for modular defense | Microservices, secure APIs | Compliance implied but not detailed | AI, microservices, API security |
| **Madasamy, 2022** | Banking and insurance security | Architectural modeling | Data breaches, model drift in AI | Hybrid Cloud | Secure architecture design | Secure SDLC, DevSecOps | General mention of GDPR | AI/ML platforms, cloud-native services |
| **Masud et al., 2024** | Fraud detection via ML & blockchain | Technical evaluation | Financial fraud, data breaches | Public Cloud | ML and blockchain integration | Smart contracts, containerization | GDPR and national laws |

|  |
| --- |
|  |

|  |
| --- |
| Blockchain, ML, containerization |

 |
| **Nagarajan, 2024** | Banking data confidentiality | Framework analysis | Data breaches, insider risks | SaaS, IaaS | Confidentiality-enhancing frameworks | Data encryption, access control | ISO 27001 mentioned | Data masking tools, access control platforms |
| **Orelaja et al., 2024** | African banks | Case study (tech deployment) | Fraud, external hacks | SaaS + Private Cloud | Multi-layer security | API security, DevSecOps | African financial standards | APIs |
| **Sharma, 2021** | Banking systems | Case examples | Payment fraud, insider threats | Hybrid Cloud | Technical controls and audits | Identity management, encryption | PCI DSS, RBI guidelines | Banking APIs, cloud encryption |
| **Vadisetty, 2024)** | Data architecture in finance | Technical modeling | Data risk, analytics breaches | Hybrid Cloud | Big data analytics security | Federated models | Implied standards | Big data platforms |
| **Wang et al., 2024** | Financial institutions | Analysis of cloud computing models in financial information processing | Data breaches, privacy concerns | Cloud computing in the financial sector | Intelligent prediction and assessment technologies | Enhancement of data processing efficiency and accuracy | Policy recommendations to mitigate concentration risks | Not specified |

**3.1.2** **Effectiveness of Mitigation Strategies and Threat Response Models**

The financial cloud cybersecurity poses considerable diversity of mitigation strategies, reactive forensic approach as well as proactive, architecture driven ones. (Chintale et al., 2019) presented a DevOps framework coupled with Infrastructure as Code (IaC) and automated policy enforcement against the configurations and updates of policies as fast as needed. An example of automation against low-level infrastructure threats was seen through the use of Terraform and Jenkins. However, (Dopamu, 2024) employed forensic techniques and behavioral analysis to help respond to post-incident data breaches to work through attacker behavior and strengthen pre and retroactive defense techniques. His research is to enable people to use the log analysis tools for the sake of visibility within large-scale public cloud environment.

In a hybrid cloud environment, (Ejiofor, 2023) suggested the use of zero trust framework attached with encryption techniques as a proactive defense technique. The paper underscores that trust validation is necessary for every access request as a potential threat and that every single one of them may be scrutinized. In (Farayola, 2024), an AI-based threat detection and verification using blockchain was proposed to create provable forensic evidence that’s available for offline using the blockchain and that contributes to the induction and analysis of blockchain sophistication by eliminating the use of probabilistic models, emphasizing the necessity of proactive fraud detection and increased auditability. This is particularly true in environments where transaction volumes are heavy, and immutable records play a very important role in these. (Johora et al., 2024) also looked into real-time AI and machine learning driven fraud detection systems and it was found how a predictive analysis can detect small events in a financial pattern before enormous harm is done.

(Jabir et al., 2016) stressed that apart from those traditional preventive measures, such as firewalls, intrusion detection systems, and data encryption, which will continue to be required in a cloud environment with little automation, predictive systems are not as feasible. Moreover, (Katari & Ankam, 2022) proposed a governance framework to handle the multi-cloud architecture through centralizing control and data federation to cope with the interoperability as well as the data leakage. AI and secure APIs integrated with a modular microservices framework that enhances defense adaptability against dynamic threats (i.e., phishing and fraud) have been introduced by (Kokogho et al., 2025).

A secure architectural model to mitigate model drift and to guarantee consistency of AI behavior over time is proposed by (Madasamy, 2022). This architecture was based on the Secure SDLC and DevSecOps principles, which meant it had inherent resilience. In an integrated solution utilizing blockchain smart contracts and machine learning, which (Masud et al., 2024) had assessed, smart contracts enforce non-repudiation, and machine learning predicts fraudulent activity. To guard against insider risks in financial SaaS and IaaS applications, (Nagarajan, 2024) recommended a confidentiality enhancing framework, which includes data encryption and access control to make data secure for insiders.

(Orelaja et al., 2024) provides the strategies of multi-layered security deployments of DevSecOps and API security of African banks that are adapted to address the lack of resources and different regional threats, as well as establishes how these pervade into the way the data is viewed and how data can be stored. As (Owoade et al., 2024) summarized, automating, and in conjunction with DevSecOps, there is a need for this in CI/CD pipelines to provide a shield against supply chain threats in a PaaS environment. Technical controls such as identity management systems, which helped provide user authentication and accountability, were further provided for in (Sharma, 2021). The data security models using the Federated Analytics model to limit exposure of data during its distributed processing were proposed by (Vadisetty, 2024). Moreover, (Wang et al., 2024) introduced a policy-oriented model for predictive assessment technologies applicable to early risk identification, predominately through a data-intensive setting in financial operations.

**3.1.3 Adoption and Impact of Secure Cloud Engineering Practices**

The cloud engineering in the financial domain is being driven more and more by the secure by design principles, i.e., automation, modularity, and visibility. Early on, Infrastructure as Code (IaC) and DevOps streams were used by (Chintale et al., 2019), to carry out configurations across AWS crutches seamlessly and consistently. Modern engineering practices, which are applicable to maintain secure IaaS environments, are embodied on their side through their deployment tools, e.g. Terraform, Jenkins. Using engineering strategies such as (Dopamu, 2024) microservices and behavioral analytics systems, (Dopamu, 2024) increased the modularity (incidence of incident response), while at the same time forensic workflows could be conducted without interfering with core banking features. According to (Ejiofor, 2023), a DevSecOps model was implemented over a zero-trust architecture for continuous security validation in all stages of the development lifecycle. In secure banking, microservices were highlighted (Farayola, 2024) as a modularity and scalable way to bring AI, blockchain and engineering pipelines together to decentralize and guard data flow. Among others, Johora et al. (2024) employed cloud-hosted AI systems under actual workloads conditions, minimizing secure data ingestion in real time and improving runtime fraud detection for achieving a low latency in high-volume transactions.

Engineering controls, such as access control layers or encryption modules, are promoted in a more traditional approach where they provide the fundamentals of securing a system architecture laid out by (Jabir et al., 2016). API gateways and containerizing were used by Katari & Ankam (2022) to engineer interoperability and vendor-agnostic systems in a multi-cloud governance framework. The emphasis on the modular directions is in line with the contemporary paradigms of the cloud-native. (Kokogho et al. (2025) followed a similar idea of secure APIs in microservices to detect fraud while allowing the normal performance of the core systems. (Madasamy (2022) offered a security analysis in cloud-based environments for the security of financial models through the integration of DevSecOps and SDLC principles to secure AI architecture. In (Masud et al., 2024), smart contracts and machine learning components were integrated into the containerized environment to bring both assessability and scalability. (Nagarajan, 2024) investigated platforms for access control and data-masking tools aimed at obfuscating sensitive information even when access is authorized.

As mentioned in (Orelaja et al. (2024), they implemented DevSecOps pipelines and secure API layers designed for African banks, showing how secure engineering works for local problems. As Owoade et al., 2024) pointed out, Security posture is preserved throughout the software delivery process with CI/CD toolchains, supported by Infrastructure as Code (IaC) practices to deliver infrastructure reproducibility. Identity management systems and data encryption stacks, as per the RBI and PCI DSS mandate, were presented by Sharma (2021). (Vadisetty (2024) integrated federated architectures for secure big data analytics and thought of distributing the processing tasks to limit the losses incurred in case of a potential breach. Intelligent prediction tools, if incorporated in the financial data pipeline, can not only improve the engineering performance but also lead to higher security (Wang et al., 2024).

**3.1.4 Regulatory and Compliance Integration in Financial Cloud Security**

No financial cloud operation could take place without proper compliance with data protection and cybersecurity regulations. Early efforts to formalize compliance using ISO 27001 were made by (Chintale et al., 2019) through their use of ISO 27001 within a DevOps cloud infrastructure. (Dopamu, 2024) adapted his forensic framework to the NIST guidelines since the U.S. financial sector relies on federal protocols on incident response and data integrity. In their proposed frameworks, (Ejiofor, 2023) and (Farayola, 2024) referenced NIST, GDPR and ISO 27001. In (Ejiofor, 2023), this is for structured compliance layers in hybrid environments, and in (Farayola, 2024), this is for compliance about AI and blockchain architectures. For instance, (Johora et al., 2024) suggested to adhere to GDPR and PCI DSS in applications of AI in data-sensitive applications in the banking sector, and (Jabir et al., 2016), even though he did not directly refer to certain standards, posed the basis for controls to be implemented following these frameworks.

This is in agreement with (Katari & Ankam, 2022) which explicitly mentioned ISO 27001 and SOC 2, showing the relevance of compliance in multi-cloud governance. However, the alignments with regulatory standards (Kokogho et al., 2025) did not specify which regional frameworks, suggesting that there might be a difference between regional regulatory enforcement or reporting. For example, (Madasamy, 2022) acknowledged GDPR and stated that the design of the architecture has to be arranged to comply with these principles of secure processing, especially in AI workflows; (Masud et al., 2024) advanced the discourse by developing and incorporating both GDPR and national data protection laws in their hybrid machine learning and blockchain solution, demonstrating awareness of the complex compliance environment. In (Nagarajan, 2024), ISO 27001 was taken into account in the design of confidentiality-enhancing systems, stressing that access should be secure and minimal data is needed. According to (Orelaja et al., 2024), however, regional frameworks are becoming more structured and, as such, they are worthy of global comparison.

As an example, their continuous integration and continuous delivery (CI/CD) security enhancements were cited (Owoade et al., 2024) as being guided by GDPR as the foundational standard. In the Indian banking sector, (Sharma, 2021) satisfied PCI DSS and the guidelines of the Reserve Bank of India. However, (Vadisetty, 2024) found adherence to standard-based design in his big data systems but does not mention specific frameworks, which may reflect an early stage of implementation. Aligning with the ever-growing regulatory thought leadership (Wang et al., 2024), proposed policy recommendations would reduce systemic concentration risk, a compliance issue at the macro level.

**3.2 Discussion**

Through analysis of case studies and technical evaluations, a wide range of cybersecurity threats for which the cloud enabled financial systems are exposed are underlined, all consistent with critical thematic concerns. They include a broad spectrum of cyberattacks as well as misconfigurations of traditional infrastructure as well as more complex, evolving threats such as hybrid cloud, AI and ML, and regulatory gaps. However, financial systems operating on the cloud platforms and the use of the Infrastructure as a Service (IaaS) or hybrid models are structurally prone, and this is a problem. (Chintale et al., 2019) noted that poor configurations and insufficient code control can lead to compromise of DevOps environments and (Masud et al., 2024) pointed out that DevOps environments were also a vulnerability for attackers who targeted machine learning models integrated with blockchain for fraud detection. Like (Dopamu, 2024), (Nagarajan, 2024), they also pointed out the continuous difficulty maintaining the data confidentiality and dealing with the insider risk, observing how the problems with visibility and access control remain in both the public cloud and Software as a Service (SaaS).

Across many studies, we find that fraud, phishing, and credential theft have been reported (Farayola, 2024); (Johora et al., 2024); (Kokogho et al., 2025); (Orelaja et al., 2024). They (Farayola, 2024) developed a conceptual framework to link these threats to system-wide interconnection, and (Kokogho et al., 2025) indicated that phishing and insider threats would undermine fraud detection systems, particularly in a hybrid cloud environment. By demonstrating that the AI/ML systems themselves are susceptible to fraud vectors during real-time data processing, (Johora et al., 2024) takes a unique stance as to provide a potential backdoor for biased or manipulated decision-making, elaborated upon by (Madasamy, 2022), who discovered model drift as a way to exploit a backdoor. Intelligence insights show that AI can sweep both detection and new-to-detect vulnerability areas.

As indicated by (Jabir et al., 2016), legacy threats (such as SQL injection, DoS attacks and spoofing) are still present in cloud environments, requiring adaptation of fundamental security measures such as firewalls and encryption to a cloud native environment. In particular, (Katari & Ankam, 2022) investigated interoperability and overcoming the challenge of vendor lock in while using multi cloud financial frameworks. In particular, it can reduce the effectiveness of governance or lack of data federation protocols combined with the weak governance causes these integration issues to open up the attack surface. As a consequence of the growing complexity of hybrid and multi cloud models, both (Ejiofor, 2023) and (Sharma, 2021) have argued that more context aware constructs are needed, in line with Sharma’s preoccupation with audits, encryption, and identity management, particularly when most banking models are hybrid in nature, (Ejiofor, 2023)’s opening up to zero trust and encryption along with the view he put forward for ensuring that encryption is tied to identity and modeled as a trust indicator of a user is very much in line with (Sharma, 2021)’s approach. This is also backed by (Owoade et al., 2024), who demonstrated that supply chain threats can pose significant problems on poorly governed CI/CD pipelines in PaaS architectures in the almost fast-evolving fintech landscape.

Various authors have examined regulatory and compliance dimensions, but there was an inconsistency between different case studies. (Farayola, 2024) and (Johora et al., 2024) refer to GDPR, (Dopamu, 2024) and (Sharma, 2021) refer to PCI DSS and the national regulatory frameworks such as the Reserve Bank of India (RBI). Indeed, (Wang et al., 2024) noted that systemic concentration risk and varying enforcement are heightened as parties increasingly rely on centralized vendor cloud providers that don’t provide as good an integration of predictive technology. Their appeal for policy standardization is in line with the (Katari & Ankam, 2022) and (Orelaja et al., 2024) calls for policy standardization in light of their challenges that redrafted the fragmented compliance landscape in African banks. It was shown that variability also existed in the integration of secure cloud engineering practices. (Owoade et al., 2024) and (Chintale et al., 2019) focused on using cloud native tools, e.g. Terraform, Jenkins, and CI/CD pipelines as verified by (Owoade et al., 2024) to reduce manual errors and increase response time. (Masud et al., 2024) also looked into the feasibility of using smart contracts and containerization to strengthen the machine learning systems. Despite these advanced data architectures, as noted in (Vadisetty, 2024), even these federated models and access controls need to be faithfully managed to avoid vulnerabilities in hybrid systems.

**4.0 Conclusion and recommendation**

**4.1 Conclusions**

Amid the financial sector’s cloud transformation, it is crucial that the cloud engineering is strong enough to ensure robust cybersecurity. Understanding cloud native technologies, such as micro services, container orchestration, and DevSecOps pipeline, this review shows that there is a huge enhancement of scalability and resilience, and also more responsive and automated security. This is achieved when these innovations are integrated with an encrypted and real-time intrusion detection and access-controlled layered defence strategy.

Whereas cloud migration introduces unique challenges, there are complex regulatory environments that the financial institutions must navigate, which include PCI DSS, GDPR, to name a few, further the shared responsibility model that the financial institutions must adhere to and finally implement robust identity and access management (IAM). Interestingly enough, the cloud architecture itself is not the most important part of security, rather, it must be built within the organization’s strategic governance and culture.

The continuous monitoring, AI enhanced threat detection and secure by design cloud engineering practices are needed to solve real world application.

**4.2** **Limitations of the Study**

However, limitations in this review should be acknowledged, as this review provides a wide overview of how cloud engineering is employed to strengthen financial cybersecurity. First, the study largely utilizes secondary data sources and prior literature, which may suffer from publication bias and be missing observations of the most recent or unpublished new ideas in the field. However, some emerging trends or vulnerabilities of cloud computing and cyber threats may not have surfaced yet, or the evolution is so rapid that some may be overlooked. Second, this review is conceptual and is not empirically validated, nor is it quantitative. The findings are not generalizable to all financial institutions, and it is difficult to assess the efficacy of particular cloud-based security implementations, especially in real-world financial institutions. Overall, the study does not have any direct input from stakeholders, including IT professionals or cybersecurity experts in the financial sector. Adding their perspectives would have been valuable to make us perhaps more practical and give us some on the ground experiences.

**4.3 Recommendations for future research**

Further research can involve the integration of AI-driven threat detection in the cloud financial environment. Major current studies on cloud engineering demonstrate the potential of improving cybersecurity, but more empirical evidence is required for estimating the long-term effectiveness and resilience of these systems when confronting ever-evolving cyber threats. Comparing the deployment models of the hybrid, public and private cloud infrastructures concerning financial data security will offer some interesting insights in choosing the best deployment model. Additionally, the area of human factor is not well explored; the research on how employee behavior and organizational cybersecurity culture tie in with cloud based protections may unveil critical holes.

**COMPETING INTERESTS DISCLAIMER:**

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

**References**

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access, 9, 57792–57807.

Alotaibi, A. F., AlZain, M. A., Masud, M., & Jhanjhi, N. Z. (2021). A comprehensive survey on security threats and countermeasures of cloud computing environment. Turkish Journal of Computer and Mathematics Education, 12(9), 1978–1990.

Baalamurugan, K. M., Kumar, S. R., Kumar, A., Kumar, V., & Padmanaban, S. (Eds.). (2021). Blockchain security in cloud computing. Springer Nature.

Betcher, T. J. (2010). Cloud computing: Key IT-related risks and mitigation strategies for consideration by IT security practitioners.

Bhatnagar, S., & Mahant, R. (2024). Strengthening financial services through secure computing: Challenges, solutions, and future directions. International Journal of Advanced Research in Science Communication and Technology, 4(1), 449–458.

Chavan, N., Bharambe, N., Deshmukh, S., Ahire, D., & Jain, A. R. (2022, May). Implementing DEVSECOPS pipeline for an enterprise organization. International Journal of Advanced Research in Science Communication and Technology, 46–72.

Chintale, P., Korada, L., Ranjan, P., & Malviya, R. K. (2019). Adopting Infrastructure as Code (IaC) for efficient financial cloud management. ISSN: 2096-3246, 51(04).

Dopamu, O. M. (2024). Cloud-based ransomware attack on US financial institutions: An in-depth analysis of tactics and countermeasures. International Journal of Science and Research (IJSR), 13(2), 1872–1881.

Dong, G., Wang, X., Cheng, H., Xiang, Z., Li, D., & Liu, B. (2018). Dynamic secure sharing of cloud audit data based on blockchain technology. In International Conference on Computational Science and Engineering (ICCSE 2018) (pp. 202–207).

Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: Integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology, 11(6), 62–83.

Farayola, O. A. (2024). Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. Finance & Accounting Research Journal, 6(4), 501–514.

Harvey, J. T. (2018). The financial sector’s vulnerabilities, villains, and options for defense. Military Cyber Affairs, 3(2), 8.

Herardian, R. (2019). The soft underbelly of cloud security. IEEE Security & Privacy, 17(3), 90–93.

Jabir, R. M., Khanji, S. I. R., Ahmad, L. A., Alfandi, O., & Said, H. (2016, January). Analysis of cloud computing attacks and countermeasures. In 2016 18th International Conference on Advanced Communication Technology (ICACT) (pp. 117–123). IEEE.

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. The American Journal of Management and Economics Innovations, 6(06), 8–22.

Katari, A., & Ankam, M. (2022). Data governance in multi-cloud environments for financial services: Challenges and solutions. Educational Research (IJMCER), 4(1), 339–353.

Kokogho, E., Odio, P. E., Ogunsola, O. Y., & Nwaozomudoh, M. O. (2025). A cybersecurity framework for fraud detection in financial systems using AI and microservices. Gulf Journal of Advance Business Research, 3(2), 410–424.

Lampe, U., Wenge, O., Müller, A., & Schaarschmidt, R. (2013, August). On the relevance of security risks for cloud adoption in the financial industry. In AMCIS.

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: A systematic literature review. Future Information Technology: FutureTech 2013, 285–295.

Li, Z., Kong, D., Niu, Y., Peng, H., Li, X., & Li, W. (2023). An overview of AI and blockchain integration for privacy-preserving. arXiv preprint arXiv:2305.03928.

Madasamy, S. (2022). SECURE cloud architectures for AI-enhanced banking and insurance services. International Research Journal of Modernization in Engineering Technology and Science, 4, 6345–6353.

Masud, S. B., Rana, M. M., Sohag, H. J., Shikder, F., Faraji, M. R., & Hasan, M. M. (2024). Understanding the financial transaction security through blockchain and machine learning for fraud detection in data privacy and security. Available at SSRN 5164958.

Mohammed, D. (2015). Cybersecurity compliance in the financial sector. Journal of Internet Banking and Commerce, 20(1), 1–11.

Nagarajan, H. (2024). Assessing security and confidentiality in cloud computing for banking and financial accounting. International Journal of HRM and Organizational Behavior, 12(3), 389–409.

Nicoletti, B. (2013). Cloud computing in financial services. Springer.

Orelaja, A., Nasimbwa, R., & Omoyin, D. D. (2024). Enhancing cybersecurity infrastructure: A case study on safeguarding financial transactions. Australian Journal of Wireless Technologies, Mobility and Security, 1(1).

Owoade, S. J., Uzoka, A., Akerele, J. I., & Ojukwu, P. U. (2024). Cloud-based compliance and data security solutions in financial applications using CI/CD pipelines. World Journal of Engineering and Technology Research, 8(2), 152–169.

Pierotti, W. (2018). Cyber Babel: Finding the lingua franca in cybersecurity regulation. Fordham Law Review, 87, 405.

Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. Information and Software Technology, 141, 106700.

Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S., & Colomo-Palacios, R. (2022). Holding on to compliance while adopting DevSecOps: An SLR. Electronics, 11(22), 3707.

Sharma, V. (2021). Securing payments and banking systems from cybersecurity threats. Journal of Economics & Management Research, SRC/JESMR-274(2), 207, 2–4.

Skelton, A. (2017). Analyzing cyber threats affecting the financial industry.

Tanna, M., Sridaran, R., & Dobariya, A. (2019, March). A study on security mitigation models in cloud computing. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 446–450). IEEE.

Vadisetty, R. (2024, November). Efficient large-scale data based on cloud framework using critical influences on financial landscape. In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC) (pp. 1–6). IEEE.

Wang, Y., Zhu, M., Yuan, J., Wang, G., & Zhou, H. (2024). The intelligent prediction and assessment of financial information risk in the cloud computing model. arXiv preprint arXiv:2404.09322.

Yalamati, S. (2024). Data privacy, compliance, and security in cloud computing for finance. In Practical Applications of Data Processing, Algorithms, and Modeling (pp. 127–144). IGI Global.

Zheng, Z., Dai, H. N., & Wu, J. (2019). Blockchain intelligence: When blockchain meets artificial intelligence. arXiv preprint arXiv:1912.06485.