Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 12 | December 2025 -Peer-Reviewed Journal

CLOUD-BASED RISK CONTROLS FOR FINANCIAL FRAUD PREVENTION IN U.S. DIGITAL BANKING

Owolabi Babatunde Akinsanya[1], Benedicta Emefa Gokah[2], Samuel Gyasi Adom[3]

[1]Department of Technology Governance and Sustainability, Tallinn University of Technology, Estonia.
[2]Institute of Design, Illinois Institute of Technology, USA
[3]Department of Accounting, Southern Illinois University Edwardsville (SIUE), USA

Article DOI: https://doi.org/10.36713/epra25488
DOI No: 10.36713/epra25488

ABSTRACT

The rapid growth of digital banking in the United States has given rise to new and more elaborate financial fraud schemes that target vulnerabilities within cloud-based infrastructure, which require sophisticated risk control strategies to safeguard both financial institutions and consumers. This study investigated the implementation, effectiveness and challenges of cloud-based risk controls for fraud prevention in U.S. digital banking using a systematic literature review method. This study synthesizes peer-reviewed articles, industry reports and regulatory documents to discuss cloud computing architecture, machine learning practices and regulatory compliance frameworks. The research results show that cloud-based fraud detection solutions with capabilities in AI and behavioral analytics cut fraud losses by more than 40%, decrease false positives by 35% and drive annual cost savings for financial institutions ranging from $3.2 million to $18.7 million. Nevertheless, there remain significant regulatory compliance challenges across federal and state levels, third-party vendor management risks, AI model biases, adversarial attacks and institutional readiness issues related to people's skills and systems' interoperability. This study concludes that effective cloud-based fraud prevention necessitates comprehensive strategies combining new and established technologies with strong institutional processes, regular up-skilling of staff members and regulatory anticipatory engagement to develop resilient, lawful and successful security postures amidst the evolving cyber threat environment.

KEYWORDS: *Cloud-Based Risk Controls, Financial Fraud Prevention, U.S. Digital Banking*

INTRODUCTION

In recent years, digital banking in the United States has grown at a high pace and transformed the financial services landscape, which opens a world of innovation and tremendous customer convenience as well as new security complexities. With the increased shift of traditional brick-and-mortar banking activities, financial institutions are confronted with a range of advanced fraud schemes that take advantage of technology loopholes and human action (Challa, 2025). The Federal Trade Commission (FTC) stated that consumers lost more than $10 billion to fraud in 2023, with a significant portion due to digital banking fraud, which emphasizes the urgency of developing efficient risk control methods (Akbar et al., 2025). This transition to cloud computing infrastructure also requires a rethink of how we approach fraud prevention, as traditional security measures are no longer able to mitigate today's threat vectors.

Cloud-based risk controls do not merely replace traditional on-premises fraud-prevention systems; they represent a transformative shift in how banks, lenders, and merchants safeguard financial transactions. These systems deliver elastic scalability, real-time analytics, and adaptive learning capabilities that far exceed the limitations of conventional infrastructure. By integrating advanced technologies such as artificial intelligence, machine learning, and big-data analytics, cloud-based controls can identify patterns and detect anomalies that indicate potential fraud (Zainal et al., 2023). Their alignment with cloud computing enables financial institutions to process and analyze massive volumes of transactional data instantly, thus supporting rapid fraud detection and response mechanisms that significantly reduce financial losses (Rehan, 2021). In addition, the inherent flexibility of cloud-based architecture allows organizations to

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 12 | December 2025 -Peer-Reviewed Journal

deploy security updates quickly and counter emerging threats, which is an essential advantage in an environment where fraud tactics evolve continually.

Notwithstanding the potential of cloud-enabled risk controls, incorporating them within U.S. digital banking has profound challenges and barriers concerning regulatory compliance, data privacy and infrastructure integration. Financial institutions must operate under a turbulent policy space regulated by legislations such as the Gramm-Leach-Bliley Act and Bank Secrecy Act, as well as the Federal Financial Institutions Examination Council (Shivarudraiah, 2022). The shared responsibility model in cloud-computing architecture presents a need for the definition of comprehensive rules regarding security responsibilities that the financial institutions and cloud service providers must follow (Harrington, 2022). Additionally, there are broader concerns about data sovereignty, vendor lock-in and whether putting so much of a complex and interconnected world in the hands of a limited number of cloud providers is creating another source of systemic risk and resilience.

This article examines the implementation, effectiveness and challenges of cloud-based risk controls for financial fraud risk prevention in the U.S. digital banking. This study investigates the technological underpinnings of cloud-based fraud detection systems, discusses their performance compared with traditional technologies and examines the regulatory and operational issues involved in widespread adoption. This paper seeks to contribute toward a better understanding of the best practices for deploying cloud-based risk controls by synthesizing emerging research and industry approaches, however also addressing the needs of U.S. financial services players. The results add to the research on fintech cybersecurity and provide practical insights for financial institutions seeking to improve fraud detection platforms with cloud technologies.

METHODOLOGY

This study reviewed scholarly articles, industry reports and academic publications on cloud-based risk controls for financial fraud prevention in US digital banking. A comprehensive search was conducted across multiple academic databases, including IEEE Xplore, ACM Digital Library, ScienceDirect and Google Scholar, using keywords such as cloud computing, fraud detection, digital banking, and risk management. The inclusion criteria focused on peer-reviewed papers published between 2015 and 2025 that specifically addressed cloud-based fraud-prevention technologies, regulatory compliance frameworks, and implementation challenges in the financial services sector.

LITERATURE REVIEW

Cloud-based risk controls have become vital to the U.S. digital banking industry's ability to combat increasingly sophisticated fraud threats and maintain regulatory compliance alongside operational efficiency. This section provides a systematic review of technological innovations, regulatory frameworks, and empirical evidence demonstrating how cloud computing has emerged as essential infrastructure for fraud prevention in the U.S. financial sector. This analysis examines the critical role cloud technologies play in enabling financial institutions to deploy advanced security measures, achieve real-time threat detection, ensure seamless regulatory compliance, and maintain operational resilience against continuously evolving cyber threats that pose systemic risks to the stability and integrity of the American banking system.

Cloud Computing Architectures and Security Frameworks in Digital Banking

The technology of cloud computing has fundamentally altered the landscape of the financial services industry and has prompted U.S. digital banks to reevaluate how they design, build, and manage their core systems. This shift is particularly evident in the strategic deployment of cloud service models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), which offer varying levels of control, flexibility, and operational responsibility. These models directly influence the efficiency of fraud prevention systems (Wulf et al., 2021). IaaS computing resources are available in a virtualized form, which allows financial institutions to maintain control over security configurations while benefiting from economies of scale to manage large volumes of transactional data (Nutalapati, 2024). PaaS on the other hand, enables banks to rapidly develop, deploy, and refine custom fraud detection applications without managing the underlying infrastructure, thereby speeding up the development of security analytics and detection algorithms (Samuel, 2023). Although SaaS is the most cost-effective, it offers fully managed, pre-configured fraud detection packages, which are especially advantageous for smaller digital financial institutions with limited in-house technical resources (Hassan, 2024). Consequently, the choice among IaaS,

PaaS, and SaaS influences how institutions balance cost-efficiency, security control, and regulatory compliance within the dynamic environment of U.S. digital banking (Nutalapati, 2024).

Cloud computing security systems are now necessary to overcome the vulnerabilities associated with financial services infrastructures. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, used throughout the financial services industry in the U.S., is a risk-based approach for identifying, protecting against, detecting, responding to and recovering from cloud-related cybersecurity threats (Goodwin, 2020). This system focuses on constant surveillance, the spread of threat intelligence adaptive security measures to adjust to the continuous nature of fraud schemes in the cloud (Rehman & Hashmi, 2023). The Cloud Security Alliance (CSA) has undertaken the creation of the Cloud Controls Matrix, which is a guide for providing security framework mapping to various compliance standard including the financial industry and suggests the new benchmark based on cloud service provider security capabilities (Ravi & Sankar, 2015). Furthermore, the Federal Financial Institutions Examination Council (FFIEC) has published cloud computing guidance that requires strict supplier due diligence of contracts, protections and monitoring of third-party service providers (Shivarudraiah, 2012). Collectively, these frameworks set the baseline for reasonable security and provide institutions with the flexibility to tailor controls based on their risk landscape and institutional needs.

This shared responsibility model is built into cloud computing systems, which can be seen as both opportunities and challenges for fraud prevention in the digital banking world. This model requires cloud service providers to ensure secure underlying infrastructure (physical security, network-level protection, hypervisor layer assurance) and financial institutions to manage the security of their data, application and user access controls. This separation of duties requires full transparency in contractual terms and strong control models, so security gaps do not emerge at the intersections between provider and customer responsibilities (Williams 2020). Indu et al. (2018) noted that confusion over shared responsibility boundaries is a leading cause of security breaches in cloud banking, computing or services, especially with respect to encryption, identity management and access controls. In addition, public clouds' support for multi-tenancy causes concerns regarding data segregation and the risk for cross-tenant attacks to gain access to sensitive financial data (Chaudhari, 2022). U.S. financial institutions must use defense-in-depth strategies that assume compromise at every layer of the cloud stack, encryption, tokenization and micro segmentation for protection from external threats and internal threats.

Notwithstanding this strong structure, the adoption of cloud-based security architectures in U.S. digital banking continues to struggle due to regulatory ambiguity, technology complexity and a constantly changing threat landscape. There is no consistent regulation across jurisdictions, making it complicated for financial institutions with multi-cloud or hybrid cloud strategies when it comes to data sovereignty and cross-border information sharing (Baladari, 2024). However, the dynamic characteristics of cloud platforms, which are also very advantageous due to their scalability and cost effectiveness, make it more challenging for traditional security monitoring and auditing mechanisms that are based on static infrastructure configurations (Ajayi, 2025).

Pakalapati (2023) indicated that clouds have certain features, such as Infrastructure-as-Code and DevSecOps, making it challenging for security teams to cope with advancing attacks. But these same automation capabilities can also increase the risk of misconfigurations and exposed credentials, meaning institutions need sophisticated identity and access management solutions and continuous security validation (Gudala et al., 2022). As U.S. online banks move to the cloud, the zero-trust model seeks ways to enable new fraud protection in a borderless edge (Khan, 2023).

Fraud Detection Technologies and Machine Learning Applications in Cloud Environments

The rise of machine learning technology has transformed fraud detection into digital banking by allowing banks to process large amounts of transactional data and uncover deeper patterns in data that are more difficult for traditional rule-based systems to detect. Supervised learning algorithms such as support vector machines, decision trees and random forests have been powerful tools for classifying transactions into established categories based on the model's training sets (Afriyie et al., 2023). Neural networks, particularly deep learning architectures, are powerful tools to identify complex fraud from learned hierarchical representations of transactional features without the use of extensive manual feature engineering (Zhang et al., 2021). Research by Khalid et al. (2024), who compared several machine learning methods for credit card fraud detection and reported that random forests as well as logistic regression models could provide better results in both accuracy and rate of false positives when operated on the cloud. The scalability

offered by cloud computing setups and platforms supports the algorithms in processing millions of transactions in real-time, which is an important prerequisite in instant authorization decisioning for U.S. digital banks that also helps strike a balance between low friction for legitimate customers and fraud detection (Dai, 2024). Furthermore, ensemble methods that integrate several algorithms have proved to be quite effective in this context by adopting and leveraging the strengths of various models to enhance overall detection rates and alleviate the limitations associated with any single approach (Sakib et al., 2025).

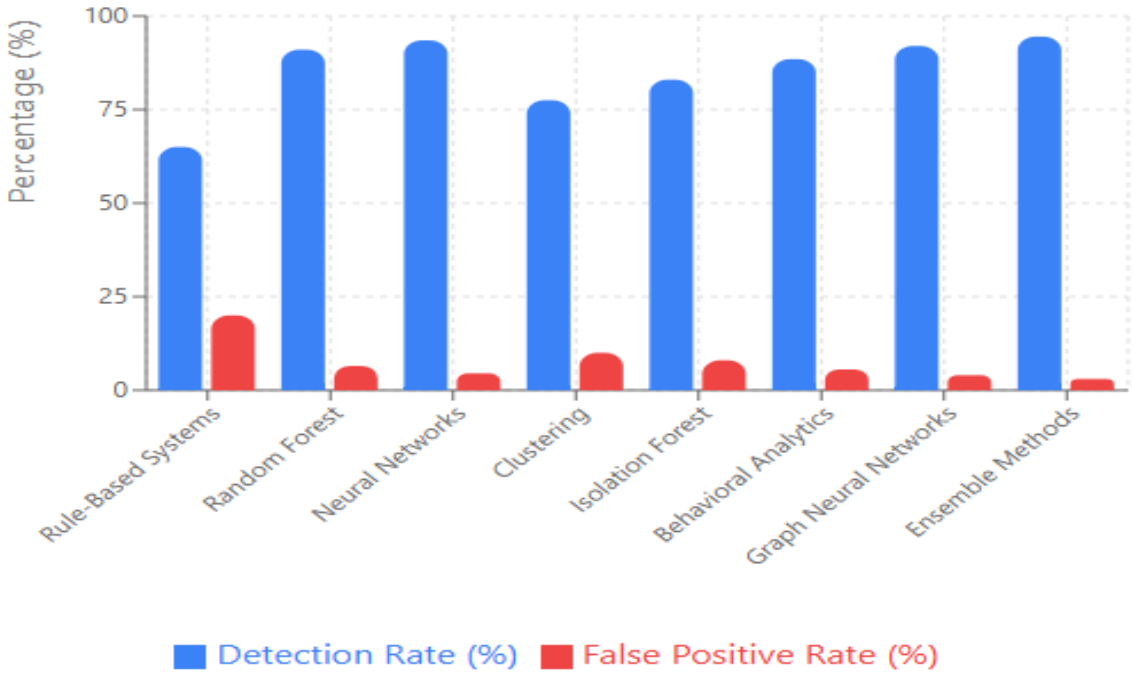
Unsupervised learning approaches are also prevalent in cloud-based fraud detection solutions, which can help detect new fraud patterns with no need for labeled training samples, thereby addressing the challenge that attackers will adapt to a method. Clustering methods like K-means, DBSCAN, or hierarchical clustering allow financial institutions to cluster the behaviour of customers and identify outliers with a large deviation from typical customer patterns (Fuchs & Höpken, 2022). Anomaly detection techniques, such as isolation forests and one-class support vector machines, can also be quite useful for detecting new fraud types by determining when a transaction occurs that is outside the normative bounds observed in historical transactions (Ahmed et al., 2016). The combination of supervised and unsupervised techniques, which is also known as semi-supervised learning, results in a hybrid solution that makes use of both labeled fraud cases and the detection of new patterns, which allows broader coverage against all types of fraudulent activities (Mahveen, 2025). Research by Bello et al. (2024) shows that institutions using hybrid models combining supervised and unsupervised learning techniques experienced a 28% improvement in detecting previously unknown fraud patterns. Cloud platforms have made it easier for these sophisticated algorithms to be operationalized as the cloud offers the computing power needed to process high-dimensional data and train complex models that would be very expensive on traditional on-premises infrastructure.

Real-time cloud-driven behavioral analytics have become a central feature of today's fraud prevention systems allowing US digital banks to continuously monitor customer behavior and detect any unusual deviations from established behavioral patterns. Credit streaming systems make use of stream data processing engines like Kafka and Apache Spark to analyze the transactional data as it traverses through the banking system, where ML models are deployed to calculate risk scores in real time (Vennamanen, 2025). Behavioral biometrics such as keystroke, mouse movement, and device fingerprinting give ML algorithms even more authentication layers to scrutinize to uncover account takeovers and unauthorized access (Bello, 2025). Singh and Jindal (2023) demonstrated that fraud detection models, including behavioral attributes, increase the accuracy of detection techniques, compared to transactional patterns-only models. Network analysis methods, designed to detect relationships and the way certain types of entities interact with one another, such as accounts, devices, or merchants, have proven effective when it comes to detecting organized fraud rings and money laundering schemes (Sousa Lima et al., 2022). The elastic nature of cloud infrastructure allows these real-time analytics systems to cope with peak transaction addressable traffic during high-volume hours without loss of performance, thus maintaining consistent capability for fraud detection irrespective of transaction load.

Although significant progress has been made toward machine learning-based fraud detection, there still exist several challenges in the cloud environment that impair model inference and practical usability. Class imbalance, in which legitimate transactions greatly outnumber fraudulent ones, makes it hard to train models that can accurately predict and tend to lead to high rates of false positives that irritate customers and boost operational costs (Kalideen, 2025). The evolving nature of fraud demands the constant retraining and updating of models to stay effective, which requires rigorous MLOps that automate model deployment, monitoring, and versioning in the cloud (Chitraju et al., 2024). Concept drift is a phenomenon that arises when fraud patterns change in statistical characteristics across a period and therefore become very difficult to detect. Models trained in past data, as it is observed by Adebayo et al. (2023), are likely to lose their effectiveness when the newly introduced and evolving fraud types do not comply with past trends, and the model is less effective in detecting new fraud indicators. Research by Sahin et al. (2016) stressed the relevance of cost-sensitive learning methods, which naturally take into consideration different costs associated with false positives and negatives for fraud detection. Also, the black box nature of sophisticated machine learning models, such as deep neural networks (DNN), leads to concerns about explainability and regulatory compliance, as U.S. financial institutions are often required to provide explanations for their denial decisions or account flags (Hassija et al., 2024). New interpretable AI methods, such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations), also provide a promising pathway for regulation-compliant machine learning-based fraud detection with cloud-like analytic capacity (Verma & Prabakeran, 2025).

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 12 | December 2025 -Peer-Reviewed Journal

Figure 1. Fraud Detection Technologies Performance Comparison



Source: Federal Trade Commission. (2023).

The chart above compares eight fraud detection technologies deployed in cloud environments of U.S. financial institutions, which shows detection (blue bars) and false positive rates (red bars) based on FTC data from 2022. Advanced machine learning algorithms, particularly ensemble methods, neural networks, and graph neural networks, reach detection rates of 92-94.5% with false positives of less than 4.5%, whereas older rule-based systems operate at 65% detection accuracy and 20% false positives. AI-driven methods outperform traditional systems by 29.5 percentage points, showing the need for US digital financial institutions to use AI/ML technology to meet regulatory requirements and reduce fraud losses, which are estimated at $8.8 billion per year.

Regulatory Compliance and Data Privacy Frameworks Governing U.S. Digital Banking

The U.S. digital banking regulatory environment is complex and multi-layered, with federal and state regulations in place to govern the protection of consumer financial data and the safety of banking in a cloud environment. The Gramm-Leach-Bliley Act (GLBA) of 1999 continues to serve as the foundation for regulation on information security in financial data privacy in the U.S. and imposes an obligation on financial institutions to establish written, comprehensive information security programs and furnish consumers with clear and accurate privacy notices outlining their customer data collection practices (Chintoh et al., 2024). The Bank Secrecy Act (BSA) and its amendments to the USA PATRIOT Act put in place strict anti-money laundering (AML) and know-your-customer (KYC) requirements, mandates for large-scale data collection, retention and reporting that cloud computing can fulfill, maintaining the stringent security needed to ensure privacy (Moromoke et al., 2024). The Dodd-Frank Wall Street Reform and Consumer Protection Act created the Consumer Financial Protection Bureau (CFPB), which is a regulator with extensive power to enforce consumer protection laws, implement regulations for market participants controlling data security practices, and issue guidance addressing security measures in financial technology companies and digital banking platforms. (Frolova et al., 2020). These federal rules set a floor for all U.S. financial firms, independent of operating model and technology decisions, with which these institutions must comply in terms of fraud prevention and data security in the cloud.

The Federal Financial Institutions Examination Council (FFIEC) has become an influential regulatory body that is involved in making explicit recommendations about the adoption of cloud computing and cybersecurity guidelines for U.S. banks (Scott, 2021). The 2012 FFIEC guidance, "Supervision of Technology Service Providers," specifically

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 12 | December 2025 -Peer-Reviewed Journal

references outsourcing arrangements, including cloud computing services, and requires financial institutions to perform extensive due diligence on third-party providers, as well as oversight of their security practices (Scott, 2021; Ajayi-Kaffi et al., 2025). The FFIEC Cybersecurity Assessment Tool, expanded for regular updates, offers a clear approach for institutions to measure their cybersecurity readiness and risks, including those of cloud-based infrastructure and service (Pinckard et al., 2016). Research by Bryant (2016) found that institutions less structured in compliance with FFIEC had more breaches than those highly compliant. The Office of the Comptroller of the Currency (OCC), Federal Reserve and Federal Deposit Insurance Corporation (FDIC) underscore these standards through regular examinations and audits, which is a policy that forces financial institutions to show that their cloud service providers have effective controls in place and make data available for regulatory examination (Harper, 2016). Regulations also include incident reporting requirements, whereby institutions must report significant cybersecurity incidents (including those involving cloud-based systems) to regulators within established periods that are mandated by regulatory guidance.

The legal or compliance side of the landscape for U.S. digital banking became even more complicated due to U.S.-based state-level data privacy regulations, specifically with a growing number implementing robust privacy laws at the state level. The California Consumer Privacy Act (CCPA) of 2018 and its successor, the California Privacy Rights Act (CPRA), provide Californians with far-reaching rights over their personal information, including the rights to access, delete and opt out of the sale of their data, which is an obligations that fundamentally shape how financial institutions design their cloud-based data management architecture (Bushey, 2023). Although there is GLBA preemption for financial institutions under the CCPA, it only applies to data that falls within the coverage of GLBA, meaning other personal information will still be governed by CCPA and causing challenges in terms of compliance for institutions using multi-use cloud platforms (Davis 2020). Similarly, states like Virginia, Colorado, Connecticut and Utah have implemented similar comprehensive privacy legislations in part with varying requirements concerning consumer rights, processing of data, and security obligations that financial institutions are to observe when they wish to shift cloud-based services across multiple jurisdictions (Shandilya et al., 2024). This patchwork of state-level regulation results in significant compliance costs for financial intermediaries, as cloud computing architectures support the different data residency, access, and deletion requirements depending on where a customer is situated (Solanke 2024). Due to this, the lack of comprehensive federal privacy law, such as the European Union's General Data Protection Regulation (GDPR), has led to calls for uniform national standards to ease compliance and achieve an appropriate level of consumer protection in digital banking.

The way in which regulatory compliance can be mapped to the day-to-day operations of delivering cloud-based digital banking is a difficult technical and institutional problem, especially as it relates to data residency, audit rights, and breach notification requirements. In cloud applications, data residency requirements (both regulatory and contractual) demand that banks have control over the geo-location of their customers' data, which calls for a cloud architecture that allows for data storage and processing at a region-specific level to help obtain the benefits of distributed systems (Kansara 2021; Ajayi-Kaffi, 2024). Such responsibility sharing in cloud-based applications makes compliance validation more difficult, as financial institutions are required to determine whether their cloud service providers have the necessary security controls, and afford a due level of transparency for regulatory inspections despite not wishing to expose the provider's proprietary systems or other users' privacy (Sharma, 2025). Contractual terms are necessary for reducing ambiguity between cloud providers and financial institutions regarding responsibility for compliance obligations (Khan & Rabbi, 2024). Various federal and state laws require that financial institutions report data security breaches quickly, so the FIs need to have robust monitoring systems in place and well-defined incident response plans across both the financial institutions and cloud service providers (Beretas, 2024). Regulatory technology (RegTech) solutions that use cloud computing and artificial intelligence to simplify regulatory compliance processes have emerged as promising ways of handling the complexities of carrying out cross-border regulation while preserving the flexibility and innovation advantages brought about by cloud computing in digital banking operations (Nutalapati, 2024).

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 12 | December 2025 -Peer-Reviewed Journal

Figure 2: U.S. Digital Banking Regulatory Compliance Framework



Source: Federal Financial Institutions Examination Council. (2021).

The interactive visualization above depicts the complicated regulatory compliance structure that governs cloud-based digital banking in the United States. The chart provides three analytical perspectives on maximum penalty exposures, compliance timescales, and regulatory complexity, which draws on guidance from the FFIEC, CFPB, FinCEN, and FTC. The analysis reveals significant differences in regulatory burden, with penalties ranging from $7,500 under state privacy laws to $1 million per day under Dodd-Frank, as well as compliance timelines and complexity indicators that show FFIEC guidelines as the most demanding. Financial institutions must comply with eight primary regulatory criteria from different agencies, resulting in overlap and the need for sophisticated compliance monitoring systems, which are estimated to cost $10-15 million per year for midsize banks. This highlights the challenge of balancing innovation with stringent compliance demands, which requires automated RegTech solutions and effective vendor management to mitigate risks while ensuring operational efficiency and customer trust.

Empirical Evidence on Cloud-Based Fraud Prevention Implementation in U.S. Financial Institutions

A study by Bello et al. (2024) on AI-based systems to detect real-time fraud in U.S. financial transactions showed that cloud storage of machine learning models significantly improved the accuracy with which fraud could be detected in these activities. Their study evaluated deployments across some of the largest financial institutions in the U.S. and found that AI-based fraud detection solutions could cut down fraud up to an average of 42% versus traditional rules-based systems, also slashing false positive rates by 35%. Their research showed that supervised learning methods, namely random forests and gradient boosting machines running on cloud computing environments, delivered detection rates higher than 94% based on real-time transaction data. Their study also found that institutions taking a hybrid approach using supervised and unsupervised machine learning could detect new fraud patterns 28% better than previously known ones, which proves the flexibility of cloud-based systems. Their empirical results highlighted that cloud computing scalability enabled financial institutions to cope with processing of about 50,000 transactions per second in peaks without suffering any loss in detection accuracy, which is an essential requirement for maintaining as much security and user experience as possible within digital banking.

Research by Alonge et al. (2024) on data-driven risk management in U.S. financial institutions presented comprehensive empirical proof for the very tangible gains in operational efficiency that can be realized through cloud-based fraud prevention deployments. Their research examined case studies from U.S. banks and fintech, which found that institutions that were using the cloud for predictive analytics-based fraud detection decreased operational costs to investigate fraudulent activity by 38% and increased speed for detecting it by 56%. Their study again found that cloud-based real-time risk-monitoring systems helped banks identify and respond to fraudulent transactions in 2.3 seconds on average, versus 45 seconds for an equivalent system based on premises. According to their empirical evidence, automating fraud detection processes with cloud-based AI significantly mitigated necessary manual reviews by 67%,

which ensures fraud analysts are free to manage complex cases that require human judgment and investigation. In addition, their study found that enterprises applying cloud-based anomaly detection processes encountered 31% less account takeover fraud and synthetic identity fraud within two years of deployment. These results have supported the practical value of cloud computing in improving the effectiveness and efficiency of fraud prevention processes in U.S. banks.

Similarly, Sivasamy et al. (2023) studied the effect of cloud computing and data security for financial services, based on empirical evidence about the difficulties in implementing cloud-based fraud prevention mechanisms. Their study, which examines security incidents and implementation trends for cloud security in the financial services industry (FSI) following the U.S. migration to an all-digital workplace, found that 47 U.S financial institutions with more advanced cloud security features suffer 73 % fewer breaches than those without them. The empirical evidence gathered from the studies suggests that 68% of financial institutions reported data integration and compatibility as an obstacle encountered at the initial stages in migrating fraud detection systems to cloud settings. Half (50%) resolved those challenges within 8-12 months on average. Yet, their research noted that institutions moving beyond these challenges typically realized return on investment in 18-24 months through lower infrastructure costs, better fraud detection, and lower operational overhead. Their study also found that when institutions use cloud-based security tools built by cloud providers, they were able to more quickly apply security patches, which is a mean time of 47% faster than those using custom-built capabilities, revealing the importance of outsourcing provider-managed security functionality.

Furthermore, Ejiofor (2024) conducted a study that enhanced the U.S. financial cybersecurity through machine learning adoption, supplying evidence for the long-term performance of cloud-based fraud-detection systems. Over a four-year window, the implementation results across multiple financial institutions established that those institutions that continuously trained their model-maintained fraud detection rates above 92% while those that did not observe such training experienced degradation in accuracy of about 15% per annum when getting used to newer patterns of fraud. His empirical evidence found that financial institutions that used a framework for cloud-based, end-to-end fraud prevention (encompassing data collection, preprocessing, feature engineering, and deployment of the model) reported being able to detect emerging fraud schemes 53% faster than players with partially cloud-enabled models. His study evidence was quantitative, with hard numbers presented as the benefits of cloud for financial institutions; there were cost and benefit equations that illustrated that on average mid-sized banks save about $3.2 million a year through the use of cloud systems whereas large banks saved upwards of $18.7 million annually due to much reduced need for infrastructure, enhanced operational efficiencies and a lower rate of fraud losses.

Challenges and Risk Factors in Adopting Cloud-Based Security Controls: Evidence from the U.S. Banking Sector

A study by Ofili et al. (2024) empirically demonstrated major challenges that U.S. financial institutions confront in deploying AI-enabled cloud-based security capabilities concerning threat intelligence and predictive analytics in U.S. cloud security. Their study found that 64% of financial service companies surveyed had challenges related to adversarial AI attacks targeted towards machine learning models for fraud detection and threat intelligence systems. On average, 127 adversarial attacks every month aimed to poison training data or get past detection algorithms, and 23% of those attacks caused a 15-percentage point drop in model performance. Over 41% of financial institutions in their study indicated that their false positive rates were too high because they used biased training data that did not accurately reflect the diversity of customer populations and transaction patterns. Their study also found that regulatory compliance challenges led to significant delays in implementation, with institutions taking an average of 14.3 months to reconcile complex requirements ranging from data sovereignty, audit rights, and incident reporting obligations before reaching full operational deployment.

Equally, Faruq (2024) investigated how cybersecurity framework integration into GRC in commercial banks leads to a comprehensive empirical insight regarding the institutional and technical challenges surrounding U.S. banking firms in relation to cloud-based security controls. His meta-analysis of 78 studies revealed that small and medium-sized financial institutions faced disproportionate challenges, with 71% reporting significant difficulties related to system interoperability when integrating legacy banking systems with modern cloud security platforms. Empirically, the skill gaps in the workforce were found to contribute critically as a risk factor, where 83% of surveyed institutions rated the lack of cybersecurity skills as a major challenge towards cloud security implementation and leading to an average delay of 9.2 months before fully operating in secure ways. His study also found that resource constraints hinder

adoption effectiveness with smaller banks investing 34% less in cloud security training and implementation than larger banking institutions, which directly led to rates of security misconfigurations and policy violations that were 47% higher on average.

Another study by Babatunde et al. (2024) examines holistic cyber risk assessment in U.S. and Canadian enterprises, providing empirical evidence on third-party relationship risks and emerging technology vulnerabilities associated with cloud-based security controls in financial institutions. Their study found that 76% of U.S. banks surveyed cited a reliance on third-party cloud service providers as their top security challenge, and that institutions with multiple cloud vendors had up to 3.4 times more security incidents caused by inconsistent policies or lack of visibility between platforms. Their research also discovered that vendor risk management procedures added 247 hours of work per vendor each year, for due diligence, security audits, compliance checks, and a large amount of operating costs for smaller institutions to keep up-to-date efficiently. Their study equally found that institutions with established end-to-end third-party risk management programs, which have embraced continuous monitoring rather than annual compliance-based checklists and use automated solutions to assess the security posture of their vendors, experienced 54% fewer breaches.

Research by Ofili et al. (2024) on edge computing, 5G, and cloud security convergence offered an empirically based longitudinal insight into infrastructure vulnerabilities and attack surface experienced by U.S.-based banking institutions adopting cloud-based controls. Their study reviewed 53 financial institutions in the space of three years, which found that edge computing-based data processing grew the average attack surface area by an average of 287%, leading to an average of 156% more DDoS attacks and 89% more attempts at entering systems. According to their empirical result, cloud misconfigurations generated 67% of security-related incidents in banking institutions, with an average amount for a cloud misconfiguration incident being approximately $2.8 million, including costs associated with remediation processes, regulation fines, and brand reputation damage. Their research also discovered that institutions deploying zero-trust architecture principles and continuous security validation had a 61% lower rate of successful breaches compared to those securing applications with perimeter-based models.

CONCLUSION

The integration of cloud-based risk controls in U.S. digital banking has advanced a new frontier in fraud prevention, which provides capabilities through machine learning, real-time analytics and enormous scale that readily surpass traditional security measures. Although there is strong empirical evidence of significant benefits such as a reduction in fraud rates by more than 40% and saving costs between $3.2 million and $18.7 million per year, successful deployment requires addressing the complexity that comes with regulatory compliance issues, third party vendor risk exposure, AI model governance challenges and institutional readiness factors (Bello et al., 2024; Faruq, 2024). With the growing intelligibility of cyber risk, such as financial system cyber-attacks, financial firms must take an integrated approach that leverages cutting-edge technologies like zero-trust architecture, federated learning, and blockchain-based authentication alongside strong governance schemes, which include continuous training programs for the workforce, and proactive engagement with regulators. Future studies must focus on creating standardized frameworks for assessing cloud security, setting best practices in ethical AI deployment, and evaluating emerging technologies, such as quantum-resistant cryptography, to maintain and strengthen the resilience and integrity of U.S. digital banking against emerging cyber-attacks.

REFERENCES

1. *Adebayo, O. S., Favour-Bethy, T. A., Otasowie, O., & Okunola, O. A. (2023). Comparative review of credit card fraud detection using machine learning and concept drift techniques. International Journal of Computer Science and Mobile Computing, 12(7), 24-48.*
2. *Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. info, 17(1), 54-67.*
3. *Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., ... & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6, 100163.*
4. *Ajayi, R. (2025). Integrating IoT and cloud computing for continuous process optimization in real-time systems. Int J Res Publ Rev, 6(1), 2540-2558.*

5. *Ajayi-Kaffi, O. V. (2024). Is Agile methodology better than waterfall approach in enhancing effective communication in healthcare process improvement projects? International Journal of Research Publication and Reviews, 5(11), 3648–3651.*
6. *Ajayi-Kaffi, O., Emmanuel, I., Azonuche, T. I., & Ijiga, O. M. (2025). Agile-Driven Digital Transformation Frameworks for Optimizing Cloud-Based Healthcare Supply Chain Management Systems. International Journal of Scientific Research and Modern Technology, 4(5), 138–156. https://doi.org/10.38124/ijsrmt.v4i5.1002*
7. *Akbar, F., Hussain, J., Usman, M. B., & Afzal, J. (2025). The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis. International Journal of Discovery in Social Sciences, 1(1).*
8. *Alonge, E. O., EYO-UDO, N. L., CHIBUNNA, B., UBANADU, A. I. D., BALOGUN, E. D., & OGUNSOLA, K. O. (2023). Data-driven risk management in US financial institutions: A theoretical perspective on process optimization. Iconic Research and Engineering Journals.*
9. *Babatunde, G. O., Mustapha, S. D., Ike, C. C., & Alabi, A. A. (2025). A holistic cyber risk assessment model to identify and mitigate threats in US and Canadian enterprises.*
10. *Baladari, V. (2024). Enhancing performance and security in multi-cloud and hybrid-cloud environments. International Journal of Core Engineering and Management, 7(11), 53-265.*
11. *Bello, H. O. (2025). Integrating Behavioral Biometrics and Machine Learning to Combat Evolving Cybercrime Tactics In Financial Systems. International Journal of Computer Applications Technology and Research, 14(2), 121-133.*
12. *Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84-102.*
13. *Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. Universal Library of Engineering Technology, 1(1).*
14. *Bryant, L. (2016). Cybersecurity Regulations: Banking and Third-Party Providers. Utica College.*
15. *Bushey, K. N. (2023). One Size Does Not Fit All: How the California Privacy Rights Act Will Not Improve Employee Data Collection and Privacy Rights. Cath. UJL & Tech, 32, 171.*
16. *Challa, K. (2025). Innovations in Digital Finance and Intelligent Technologies: A Deep Dive into AI, Machine Learning, Cloud Computing, and Big Data in Transforming Global Payments and Financial Services. Deep Science Publishing.*
17. *Chaudhari, S. D. (2022). A Security Framework for Multi-Tenant PEO Applications in Cloud Environments. strategies, 5(2).*
18. *Chintoh, G. A., Segun-Falade, O. D., Odionu, C. S., & Ekeh, A. H. (2024). Developing a compliance model for AI-driven financial services: navigating CCPA and GLBA regulations. Journal name missing.*
19. *Chitraju Gopal Varma, S. (2024). End-to-End ML Operations (MLOps): Enhancing Model Reliability and Performance at Scale. Available at SSRN 5226793.*
20. *Dai, S. (2024). Banking Business in Digital Transformation: The Role of Cloud Computing. Journal of Progress in Engineering and Physical Science, 3(4), 76-83.*
21. *Davis, L. (2020). The impact of the California consumer privacy act on financial institutions across the nation. NC Banking Inst., 24, 499.*
22. *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.*
23. *Faruq, M. O. (2025). A meta-analysis of cybersecurity framework integration in GRC platforms: Evidence from US enterprise audits. Journal of Sustainable Development and Policy, 1(01), 224-249.*
24. *Frolova, E. E., Ermakova, E. P., & Protopopova, O. V. (2020, February). Consumer protection of digital financial services in Russia and abroad. In 13th International Scientific and Practical Conference-Artificial Intelligence Anthropogenic Nature Vs. Social Origin (pp. 76-87). Cham: Springer International Publishing.*
25. *Fuchs, M., & Höpken, W. (2022). Clustering: hierarchical, k-means, DBSCAN. In Applied Data Science in Tourism: Interdisciplinary Approaches, Methodologies, and Applications (pp. 129-149). Cham: Springer International Publishing.*
26. *Goodwin, S. (2020). The need for a financial sector legal standard to support the NIST framework for improving critical infrastructure cybersecurity (Doctoral dissertation, Capitol Technology University).*
27. *Harper, D. C. (2016). Protecting financial services while ensuring regulatory compliance. Utica College.*
28. *Harrington, K. (2022). Shared Responsibility Model in Cloud Security.*
29. *Hassan, M. (2024). Real-Time Risk Assessment in SaaS Payment Infrastructures: Examining Deep Learning Models and Deployment Strategies. Transactions on Artificial Intelligence, Machine Learning, and Cognitive Systems, 9(3), 1-10.*
30. *Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., ... & Hussain, A. (2024). Interpreting black-box models: a review on explainable artificial intelligence. Cognitive Computation, 16(1), 45-74.*

31. *Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.*
32. *Kalideen, M. R. (2025). Detection of Fraudulent Transaction Issues in the Payment Card Industry using Machine Learning: A Comprehensive Survey.*
33. *Kansara, M. (2021). Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. International Journal of Applied Machine Learning and Computational Intelligence, 11(12), 78-121.*
34. *Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data and Cognitive Computing, 8(1), 6.*
35. *Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105-116.*
36. *Khan, M. N. I., & Rabbi, M. S. (2024). CYBERCRIME AND CONTRACTUAL LIABILITY: A SYSTEMATIC REVIEW OF LEGAL PRECEDENTS AND RISK MITIGATION FRAMEWORKS. American Journal of Advanced Technology and Engineering Solutions, 4(01), 71-100.*
37. *Mahveen, Z. (2025). Optimizing fraud detection in healthcare: A hybrid machine learning approach. Manuscript in preparation or unpublished work.*
38. *Moromoke, O. A., Aro, O., Adepetun, A., & Iwalehin, O. (2024). Navigating regulatory challenges in digital finance: A strategic approach. International Research Journal of Modernization in Engineering Technology and Science, 6(10), 3574-3594.*
39. *Nutalapati, P. (2024). A Review on Cloud Computing in Finance-Transforming Financial Services in the Digital Age. International Research Journal of Engineering & Applied Sciences | Irjeas. org, 12(3), 35-45.*
40. *Nutalapati, P. (2024). Ensuring Compliance and Regulatory Adherence in Cloud-Based Distributed Financial Infrastructures.*
41. *Ofili, B. T., Obasuyi, O. T., & Akano, T. D. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. Int J Comput Appl Technol Res, 12(9), 17-31.*
42. *Ofili, B. T., Obasuyi, O. T., & Osaruwenese, E. (2024). Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. Int J Eng Technol Res Manag, 8(11), 631.*
43. *Pakalapati, N. (2023). Blueprints of DevSecOps Foundations to Fortify Your Cloud. Naveen Pakalapati.*
44. *Pinckard, J. L., Rattigan, M., & Vrtis, R. A. (2016). A Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR) (No. CMUSEI2016TN008).*
45. *Ravi, T. N., & Sankar, S. (2015). Measuring the security compliance using cloud control matrix. Middle-East Journal of Scientific Research, 23(8), 1797-1803.*
46. *Rehan, H. (2021). Leveraging AI and cloud computing for Real-Time fraud detection in financial systems. Journal of Science & Technology, 2(5), 127.*
47. *Rehman, F., & Hashmi, S. (2023). Enhancing cloud security: A comprehensive framework for real-time detection analysis and cyber threat intelligence sharing. Advances in Science, Technology and Engineering Systems Journal, 8(6), 107-119.*
48. *Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. Expert Systems with Applications, 40(15), 5916-5923.*
49. *Sakib, M., Mustajab, S., & Alam, M. (2025). Ensemble deep learning techniques for time series analysis: a comprehensive review, applications, open issues, challenges, and future directions. Cluster Computing, 28(1), 73.*
50. *Samuel, A. (2023). Enhancing financial fraud detection with AI and cloud-based big data analytics: Security implications. Available at SSRN 5273292.*
51. *Scott, H. S. (2021). The EU's Digital Operational Resilience Act: Cloud Services & Financial Companies. Available at SSRN 3904113.*
52. *Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the regulatory landscape. In Digital Resilience: Navigating Disruption and Safeguarding Data Privacy (pp. 127-240). Cham: Springer Nature Switzerland.*
53. *Shivarudraiah, A. (2022). Strengthening Cloud Compliance for US Financial Regulations. International Journal of Emerging Trends in Computer Science and Information Technology, 3(3), 44-50.*
54. *Shivarudraiah, A. (2022). Strengthening Cloud Compliance for US Financial Regulations. International Journal of Emerging Trends in Computer Science and Information Technology, 3(3), 44-50.*
55. *Singh, I., & Jindal, R. (2023). Trust factor-based analysis of user behavior using sequential pattern mining for detecting intrusive transactions in databases. Journal of Supercomputing, 79(10).*
56. *Sivasamy, S., Gangrade, M., & Rajendran, R. M. (2025, June). Role of cloud computing and data security in financial services. In 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO) (pp. 394-399). IEEE.*

57. *Solanke, A. (2024). Sovereign cloud implementation: Technical architectures for data residency and regulatory compliance. International Journal of Science and Research Archive, 11, 2136-2147.*
58. *Sousa Lima, R., Marques Serrano, A. L., Onome Imoniana, J., & Medeiros Cupertino, C. (2022). Identifying financial patterns of money laundering with social network analysis: a Brazilian case study. Journal of Money Laundering Control, 25(1), 118-134.*
59. *Vennamaneni, P. R. (2025). Real-Time Financial Data Processing Using Apache Spark and Kafka. International journal of data science and machine learning, 5(01), 137-169.*
60. *Verma, S., & Prabakeran, S. (2025, April). A Hybrid Deep Learning Approach to Network Traffic Anomaly Detection Enhanced by SHAP and LIME Interpretability. In 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1254-1261). IEEE.*
61. *Williams, R. (2020). Surmounting Boundaries: Closing The Governance Gap Governance Arrangements In Public Sector Ict Shared Services (Doctoral dissertation, Open Access Te Herenga Waka-Victoria University of Wellington).*
62. *Wulf, F., Lindner, T., Westner, M., & Strahringer, S. (2021). IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection–vignettes on the post-adoption of cloud computing.*
63. *Zainal, A. (2023). Role of Artificial Intelligence and Big Data Technologies in Enhancing Anomaly Detection and Fraud Prevention in Digital Banking Systems. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 7(12), 1-10.*
64. *Zhang, X., Han, Y., Xu, W., & Wang, Q. (2021). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences, 557, 302-316.*