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: 9 | September 2025 -Peer-Reviewed Journal

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR FRAUD DETECTION IN THE U.S. BANKING INDUSTRY: REGULATORY FRAMEWORKS, IMPLEMENTATION, AND CHALLENGES

David Amoako[1], Cynthia Omowonuola Boboye[2], Victor Boateng[3]
Jehu Emefa Nii-Laryea Laryea[4]
[1]School of Business, San Francisco Bay University, U.S.A.
[2]Darden School of Business, University of Virginia, U.S.A.
[3]College of Business and Technology, East Tennessee State University, U.S.A.
[4]Department of Business Administration, University of Professional Studies Accra, Ghana.

Article DOI: https://doi.org/10.36713/epra23647
DOI No: 10.36713/epra23647

ABSTRACT
This paper investigates the impact of Artificial Intelligence (AI) and Machine Learning (ML) for enhanced fraud detection in the U.S. banking industry. As electronic transactions increase, rule-based approaches are less effective in identifying sophisticated cyber threats. This research investigates how artificial intelligence and machine learning technologies are enhancing fraud prevention, real-time monitoring, behavioral analysis, and anomaly detection in banking systems. The study also examines these implementations within strict federal regulatory frameworks, including the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), and Federal Financial Institutions Examination Council (FFIEC) guidelines. The research addresses significant implementation challenges that financial institutions encounter when deploying AI/ML systems. These challenges include data privacy concerns, algorithmic bias mitigation, and the critical requirement for model explainability to satisfy regulatory requirements and maintain stakeholder confidence. The paper examines machine learning models such as supervised, unsupervised, and ensemble learning, and their role in fraud detection, insider threat, and systemic risks. Thus, the analysis provides a comprehensive operational and regulatory template to help banks in the United States respond to the adoption of AI/ML-based fraud detection systems and to strike a balance between technological progress and legal and financial system soundness.

KEYWORDS: *Artificial Intelligence, Machine Learning, Fraud Detection, U.S. Banking, Cybersecurity, Regulatory Compliance*

INTRODUCTION
U.S. banks have increasingly come to depend on digital technology, and the methods they use to identify and prevent fraudulent financial activity have been fundamentally altered in the process, which raises new issues about how banks can and should use Artificial Intelligence (AI) and machine learning (ML) in the future (Agbeve et al., 2025; Amoako et al., 2025). The application of AI/ML in fraud detection is currently deemed very important for the banking industry in meeting the cybersecurity needs and managing risks more efficiently across the banking sector in the U.S. (Adebayo et al., 2025). There are now complex regulatory constraints that banks have to operate under that necessitate the bank being innovative in their security defences but also have to navigate strict compliance rules, so that banks can offer a complete process to detect cyber threats, a mechanism to stop fraud and increase the overall cyber security having to stay within federal banking laws (Ng & Kwok, 2017).

The regulations that govern the use of AI and machine learning within U.S. banks were formulated using the pre-existing cybersecurity guidelines available in other sectors regulated by the U.S. government, such as hospitals and universities that adhere to U.S. regulations (Khader et al., 2021). This guidance emphasizes key areas in which banks

should excel, including maintaining secure systems, operating and maintaining technology in a sound and prudent manner, overseeing and managing operations, protecting against threats, and responding when systems fail, to create reports and conduct analysis to ensure that cybersecurity fulfills the expectations set by federal banking law (Agbeve et al., 2025). Studies of these regulations have also indicated that banks must educate employees and customers on cybersecurity risks as part of the comprehensive fraud prevention mandates U.S. banking regulators require (Amoako et al., 2025; Onunka et al., 2023).

The federal cybersecurity standards and regulatory frameworks offer important guidance to the U.S. banking industry to develop cybersecurity practices, balancing federal banking regulations with industry requirements (Adebayo et al., 2025). The NIST Cybersecurity Framework, which has been customized specifically for financial services, is now recognized by regulators as the best way to address cybersecurity risks in the U.S. for financial institutions because it covers a consistent approach that fulfills federal standards demands (Agbeve et al., 2025). Banks are subject to regulatory agencies that mandate the use of cost-benefit analysis principles in their decision-making in selecting security measures that correspond to risk levels and are consistent with the federal capital requirements (Lee, 2020). Federal regulators now understand the importance of technological investment, financial resources, and personnel training required by some banks to enhance their cybersecurity capabilities (Agbadamasi et al., 2025; Adelakun et al., 2023). According to recent studies, compliance with cybersecurity is one of the determining factors regarding the competitive performance of banks (Hasani et al., 2023), which reaffirms that cybersecurity should be incorporated into banking strategic planning and risk management frameworks (Adebayo et al., 2025). Further regulatory assessments demonstrate that bank performance and compliance ratings dramatically increase when AI and machine learning cybersecurity solutions are used by banks (Adebayo et al., 2025; Agbeve et al., 2025).

This comprehensive analysis adds to regulatory literature by considering how U.S. banks face practical difficulties in the implementation and control of fraud detection systems based on machine learning and blockchain technologies. The research evaluates how banks can leverage advanced AI and machine learning technologies under federal banking regulations and provides an operational framework by which U.S. banks can better identify illicit financial transactions while ensuring full compliance with government supervision mandates, further enhancing the cybersecurity of American financial institutions within current regulatory confines.

In an age of digital banking, banks form the bedrock of the US economy by processing transactions, making investments, and enabling the flow of money, all under the watch of strict federal rules and regulations (Agbeve et al., 2025; Firoozi & Mohsni, 2023). Banks are particularly vulnerable with their heavy dependence on digital technology, and to comply with highly complex government requirements, they are exposed to a myriad of cyberthreats, including data theft and more advanced hacking attacks, which challenge computer security measures as well as the capabilities of the government to both supervise and control them (Shah, 2021). Cybersecurity at U.S. banks isn't just a matter of protecting customers' personal information; rather, it is a critical component of federal regulators' obligation to ensure the entire U.S. financial system is safe, trusted, and stable.

Cyberattacks against banks in the U.S. can induce broad regulatory reactions and possess wide-reaching implications at the national level, with implications beyond individual clients to regional economies or pan-national financial stability (Pomerleau and Lowery, 2020). Deviations in U.S. banking networks could lead to loss of enormous money, legal penalties, loss of public confidence, and the disruption of essential bank services under the federal coverage and protection (Adebayo et al., 2025; Pomerleau and Lowery, 2020). The growing U.S. banking services digitization, accompanied by the widespread availability of online transactions and mobile banking systems functioning under federal consumer protection laws, enlarged the range of regulatory attack surface that federal regulators need to guard and monitor against cyberattacks (Amoako et al., 2025). As U.S. banking adopts new technologies, including the cloud, blockchain, and Internet of Things (IoT) devices, the banks must manage new compliance requirements and address emerging vulnerabilities and new security issues that need a regulatory response (Agbadamasi et al., 2025; Umoren et al., 2025). As a result, protecting U.S. banking systems from significant cyberthreats has become a central regulatory activity for federal banking regulators, policymakers, and market participants working within the American financial regulatory ecosystem.

The impact of cyberattacks on U.S. banking institutions is profound, in that they can lead to a direct, regulatory-level response and even affect regional economies and federal financial stability mechanisms, rather than just affecting

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: 9 | September 2025 -Peer-Reviewed Journal

individual customers (Pomerleau and Lowery, 2020). Banking breaches in the U.S. may be costly in terms of money, regulation, consumer confidence, and the operation of essential services that fall under federal regulation and protection (Pomerleau & Lowery, 2020). And like in a globally linked economy whose banking industry is subject to international banking regulations, a cyber event at any one U.S. bank can result in a cascade reaction of regulation and systemic risk assessments across federal and state jurisdictions (Amoako et al., 2025). The growing digitalization of the banking sector in the U.S. and widespread online activity and mobile banking platforms that are federally regulated under consumer protection laws have widened the opportunities for cyberattacks, and federal agencies need to guard the sector against these threats (Amoako et al., 2025; Agbeve et al., 2025). While U.S. banks are embracing technological innovations like cloud computing, blockchain, and Internet of Things (IoT) devices under evolving regulatory frameworks, banks have to develop new policies and processes in the face of complex cybersecurity threats (Adebayo et al., 2025). As a result, U.S. federal banking regulators, along with U.S. policymakers and industry participants, now have a heightened regulatory focus on protecting U.S. banks from cybersecurity risks.

Financial Cybersecurity

The US financial industry faces evolving fraud threats, and it is therefore necessary to take advantage of AI technology and machine learning solutions to protect the integrity and stability of the U.S. financial system (Dupont, 2019). These threats come from targeted and well-organized cybercriminals as well as opportunistic fraudsters' attacks attempting to profit from fraudulent transactions, and as such, banks need advanced analytics capabilities that are beyond the traditional systems in order to respond to these dynamic, escalating challenges (Amoako et al., 2025).

Complex attacks on U.S. banking systems are becoming increasingly popular among recent fraud scams, undermining the conventional means of defense against such schemes. The use of malware, especially ransomware, also poses continuous threats to financial institutions, locking the crucial fraud detection information and disrupting AI and machine learning processes until ransom is paid (Angelopoulos et al., 2019). But these ransomware attacks have progressed to target entire fraud detection networks and machine learning infrastructure systems, and therefore, the banks need AI algorithms that can detect patterns that are strange and indicate ongoing fraud.

Moreover, the U.S. Banking industry is confronted with the threat of phishing attacks, which is an explicit example of imitating valid financial institutions in which a cybercriminal disguises itself as a legitimate financial institution to get the username/password of authentication in a fraudulent way (Amoako et al., 2025; Alkhalil et al., 2021). Social engineering techniques, such as pretexting and baiting, which involve manipulating customers to initiate unauthorized transactions that circumvent typical detection logic, are also on the rise. Machine learning solutions provide the ability to analyze behavior, such as subtle signals about social engineering attempts like strange communication patterns, abnormal timing of transactions, or transactions that deviate from established customer profiles.

Hidden threats are a significant threat to financial service managers who have privileged access to sensitive transaction processing systems. Such threats may encompass deliberate malicious activity such as theft of data, forged transactions, or creating an unauthorized account, careless behavior, or human errors resulting in an unintended misapplication (Firoozi & Mohsni,2023; Agbeve, 2025). AI models are good at uncovering insider fraud through analysis of user behavior, access logs, and transaction anomalies that suggest illicit actions on the part of internal staff.

Financial institutions are often hit by Distributed Denial of Service (DDoS) attacks, which overload fraud detection systems with malicious traffic (Sharafaldin et al., 2019). Such attacks cause downtime in the fraud detection system, which leads to time windows for the fraudsters to operate while the defense mechanisms are not in place. This downtime incurs a heavy financial toll in lost time, having a dramatic impact on the organisation's ability to prevent financial fraud.

The interconnectivity of the financial ecosystem makes institutions prone to a supply chain risk regarding AI/ML fraud detection infrastructure (Amoako et al., 2025). Companies that provide these fraud detection systems may create vulnerabilities in these AI/ML systems that are not properly secured as a result of tainted training data or flawed algorithmic implementations that fraudsters can then exploit to evade detection or access sensitive financial data.

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: 9 | September 2025 -Peer-Reviewed Journal

Fraud is one of the most important and critical events for financial institutions, and it affects companies, clients, partners, and the entire U.S. economy (Bouchama and Kamal, 2021). Such events lead to direct monetary losses, stolen funds, malicious transactions, and ransom payments (Stanikzai and Shah, 2021). Incident response, remediation, and regulatory fines add to financial loss, and as a result, it is prudent for companies to deploy advanced AI/ML capabilities to achieve higher detection rates while reducing false positives and mitigating losses by quickly detecting and preventing fraud because the cost of not doing so far outweighs the cost of these systems (Amoako et al., 2025).

Fraud undermines trust and confidence in financial institutions, affecting their reputation and brand. Customers lose confidence in the institution's ability to safeguard personal and financial information, which ultimately leads to a loss of customers and revenue. Emerging AI/ML fraud detection systems not only act as shields but also show stakeholders that the bank is using the most advanced tech available to ensure the security of deposits (Adebayo et al., 2025; Atisu et al., 2024).

Financial cyberattacks not only directly disrupt critical banking operations such as payment processing, account management, and trading but also have ripple effects on the wider U.S. economy, affecting businesses, consumers, and financial markets (Adelakun et al., 2024). High-availability, fault-tolerance, and transparent integration are essential for AI/ML fraud detection systems to operate while maintaining normal banking business workflows. Kopp et al. (2017) posit that cyberattacks, in rare but extreme cases, such as systemic risk, can result in widespread effects that can impact the stability of a financial system, which may result in system failure and market chaos. The connected nature of financial networks has the unfortunate effect that the fraud incidents within an institution can have a cascading effect throughout the entire financial industry, making industrywide coordination in AI/ML approaches to fraud detection and collaborative development of machine learning models very important (Amoako et al., 2025; Adebayo et al., 2025).

Evolution of Fraud Detection Systems in the U.S.

The traditional fraud detection systems employed by the U.S. banking institutions were predominantly operational within predetermined criteria that have been formed according to the rules set by the regulatory authorities and are used for detecting dubious activities for regulatory reporting purposes (Ali et al., 2019). While these systems perform well under existing regulatory requirements, they produce several implementation issues that are counterproductive to evolving regulatory demands for enhanced capacity for detecting more elaborate fraud. These systems of fraud detection were reactive, as security systems are dependent on precedent and can only detect attacks that are already known and are properly regulated, not so much new threats or new patterns in behavior. Moreover, such rules-based approaches that were enforced by the rules-based systems owing to strict regulatory compliance requirements also tend to cause false positives where valid transactions are flagged as fraudulent, leading to customer dissatisfaction, operational inefficiencies, and, potentially, adding unnecessary regulatory scrutiny (Amoako et al., 2025). Moreover, due to the highly complex nature of cybercrimes that increasingly rely on technological insecurities and the limits of the existing regulation, rule-based detection may become obsolete when attackers find loopholes to exploit in the regulation or simply create new ways of committing cybercrimes.

The high volumes and complexity of financial transactions in U.S. banks present an enormous challenge for the traditional fraud detection systems, because they cannot operate and process the high banking transaction volume and speed of today's bank operations (Al-Mansoori and Salem, 2023). The manual review processes needed for compliance are slow and costly, making it difficult for banks to be compliant and up to speed with the needs of competitive banking today. As a result, regulators are increasingly realizing that banks require more advanced, data-enabled fraud detection capabilities that can analyze large volumes of data in real time, which also adhere to privacy and data protection laws and can adapt rapidly to new types of fraud threats, while still remaining within the scope of existing regulations.

In its approach to addressing the regulatory requirements and operational hurdles of the current state of the banking sector, this paper explores how U.S. banks can enhance their cybersecurity by incorporating machine learning and artificial intelligence technology in their fraud detection system strategically, keeping in mind the current regulatory limitations and compliance obligations. Integration of ML and AI into existing regulatory frameworks, U.S. banks can enhance their cybersecurity defense systems while adhering strictly to the regulations and enable them to also preempt

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: 9 | September 2025 -Peer-Reviewed Journal

fraudulent activities in a more accurate, faster manner, and tackle complex social engineering fraud schemes (Firoozi & Mohsni, 2023). It does so, showing how banks can comply with regulations while also outpacing cyberthreats, earning customer trust with smarter security, and safeguarding the integrity of the U.S. banking system. This study involves a detailed review of data-driven insights, including advanced analytics and regulatory limitations. It therefore offers a full spectrum examination of the regulatory issues and implementation strategies that are vital in combating fraud in the digital banking era.

The application of machine learning and AI in fraud detection systems in U.S. banks presents both opportunities and challenges in enhancing financial cybersecurity. Drawing upon the cybersecurity frameworks and related technology, as well as emphasizing on required investment in cybersecurity and regulatory awareness programs, this detailed analysis aims to assess and ascertain the regulatory frameworks, implementation challenges, and compliance mandates that govern how U.S. banks can adopt AI and machine learning to bolster their cybersecurity defenses. The objective is to get a sense of the regulatory requirements, the real-world challenges in adopting these systems, and the compliance obligations that inform how U.S. banks can enhance their cyber-defense capabilities by using AI and machine-learning systems.

Regulatory Frameworks in Financial Cyberthreats

U.S. financial services work in a diverse regulatory environment in deploying AI/ML fraud detection systems. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to ensure the privacy of customer information, which includes securing systems so unauthorized parties cannot access sensitive data (Agbeve et al., 2025; Firoozi & Mohsni,2023). Thus, in the use of AI/ML fraud detection systems, U.S. financial institutions are required to deploy AI/ML algorithms that enforce customers' privacy, such as data anonymization, differential privacy, secure multi-party computation, while ensuring that the architecture is implemented efficiently.

Moreover, the Sarbanes-Oxley Act mandates that publicly traded companies maintain internal controls over financial reporting, including the cybersecurity controls that protect against fraud and unauthorized access to financial systems, a regulation that financial institutions must comply with (Agbeve et al., 2025; Adebayo et al., 2025). AI/ML fraud detection deployments need to meet Sarbanes-Oxley Act requirements by having strong model governance that includes version control, model review process, performance monitoring, and documentation of algorithmic decision-making that affects finance reporting and fraud detection.

Furthermore, the Federal Financial Institutions Examination Council (FFIEC) offers guidelines and standards for the examination and supervision of financial institutions, including cybersecurity risk management practices, incident response planning, and business continuity planning (Pinckard et al., 2016). These guidelines are increasingly focused on specific risks related to AI/ML deployments, such as model risk management, testing for algorithmic bias, managing AI/ML services delivered by third parties, and the expertise needed to assess fraud detection systems based on AI/ML.

Several states have passed data breach notification legislation that obliges financial institutions to inform affected customers and regulators after their personal or financial data has been impacted through cybersecurity breaches (Chaudhry et al., 2023). These include laws that specifically affect AI/ML systems of fraud detection with respect to the identification and reporting of training data breaches, and unauthorized access to the AI/ML infrastructure that may affect the ability of fraud to be detected.

Invariably, adherence to regulatory and legal requirements is critical for financial institutions to avoid legal and regulatory liability, protect sensitive information, and maintain faith in the financial system (Amoako et al., 2025; Umoren et al., 2025). Yet, implementing an AI/ML fraud detection system raises new compliance challenges not experienced with traditional rule-based systems. This regulation presents a significant challenge, considering the complexity and number of layers in recent machine learning algorithms, which leads institutions to cope with a compromise where the highest detection rate should also be explained and justified in terms of fraud outcomes. Those fintech companies can incur liability under local and international regulatory frameworks, such as fines, penalties, and reputational harm, thereby demonstrating the significance of strong cybersecurity governance and compliance programs at financial institutions that are underpinned by AI/ML-driven fraud prevention systems.

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: 9 | September 2025 -Peer-Reviewed Journal

Machine Learning Approaches to Fraud Detection and Prevention in Banking Systems in the U.S.

Increased complex fraud in the U.S. financial industry has urged the application of a higher-order machine learning method to deal with the complexity of fraudulent transactions. The U.S. banking sector faces a wide variety of fraud threats and must have a sophisticated approach to detecting and preventing fraud if it is to preserve the legitimacy and reliability of financial institutions (Amoako et al., 2025; Dupont, 2019). The fraudulent activities extend from complex, planned attacks executed by well-resourced organized crime elements to opportunistic attacks by miscreants to make illicit money through the exploitation of banking systems.

Several key categories of fraud must be addressed when machine learning is used for fraud detection. According to Angelopoulos et al. (2019), automated fraud, such as advanced malware-derived financial theft, is an ongoing struggle that demands real-time interfacing to view and block unauthorized money flow before damage is done. Machine learning evasion of advanced persistent threats for banking infrastructure is an evolving reality, requiring ML techniques that can keep pace with new attack vectors and evasions (Amoako et al., 2025). Social engineering-related fraudulent attacks, where bank customers and employees are tricked by cybercriminals to disclose authentication passwords or authenticate unauthorized actions, need behavioral analysis algorithms to detect abnormal interaction patterns (Amoako et al., 2025). ML models need to integrate methods in Natural Language Processing (NLP) and behavior pattern recognition to filter deceptive communication attempts and suspicious access attempts.

Insider fraud detection is a particularly difficult area for machine learning because insiders, such as bank employees, contract staff, and third-party service providers, have legitimate system access, which can hide fraudulent behavior. ML algorithms have to be able to differentiate between authorized and unauthorized environment insiders through examining access patterns, transaction behaviors, and data-handling practices (Babu, 2024). Advanced anomaly detection techniques are necessary to detect small variations from normal insider behavior while keeping the number of false positives affecting genuine bank staff behavior low.

Personal takeover and denial of service attacks on banking infrastructure involve real-time analysis of traffic and classification of threats, which demands an AI module. These attacks congest financial networks, such as bank networks and payment systems, impeding the performance of legal transactions while supporting the illicit activity. To ensure availability and prevent fraud when systems are stressed, machine learning models need to quickly differentiate between volumes of normal transactions and volumes of malicious traffic.

The interconnectedness of today's banking environment means that one bank's loss through fraud is another bank's loss through life cycle events and by third-party suppliers, payment processors, and correspondent banking relationships (Babu, 2024). ML systems need to have the capability to assess supply chain risks in order to identify the potential fraud risks within partner organizations and the transaction processing chains. Higher-level graph neural networks and relationship investigation techniques are required for identifying fraud patterns across multiple institutions and service providers.

As such, fraud in U.S. banking systems costs enormous financial losses to the U.S. banking industry; they are not only based on the direct losses, but also relate to operational interruptions, risks of regulation, and erosion in customer trust (Bouchama and Kamal, 2021). Fraud detection systems based on machine learning systems face the challenge of quantifying and reducing these multi-faceted costs, while ensuring that detection accuracy is acceptable and the false positive rate is low. The financial loss from the unaddressed fraud is evident by direct monetary theft, illicit transaction processing, and ransomware incidents that take advantage of loopholes in the payment mechanisms (Stanikzai and Shah, 2021). Cost-sensitive learning techniques need to be integrated into machine learning models to optimise the performance of detection using the financial losses hierarchical profiling of fraud.

Trust and reputation are important to customers, as their personal and financial data with the banks needs to be protected by a fraud detection system that accurately and timely identifies threats (Amoako et al., 2025). Sophisticated ML algorithms have to weigh fraud detection sensitivity with customer experience, not to impede smooth transactions from genuine customers while spotting nefarious activities. Fraud incidents impact the reputation of banks and can lead to loss of customer trust and lack of confidence in the U.S. financial system, so prevention-based machine learning algorithms are crucial to stabilize banking over time.

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: 9 | September 2025 -Peer-Reviewed Journal

U.S. banks that use machine learning for fraud detection and prevention must follow strict regulatory guidelines, as such systems must meet certain data quality and reporting standards (Amoako et al., 2025). Post-fraud regulatory inquiries and enforcement can place an institution at risk of fines and constraints on operation, highlighting the need for a proactive ML approach to fraud prevention. To comply with regulations and investigate incidents, machine-learning systems must include an audit trail and explainable AI.

Networked gaming systems can be highly vulnerable to fraudulent activity, leading to cascading operational interruptions throughout interlinked banking systems and payment processing and account management, and trading systems that are critical to the functioning of the U.S. economy (Firoozi & Mohsni,2023; Adelakun et al., 2024). ML algorithms need to address systemic risk assessment to detect fraud patterns. Given the real-time nature of the operations in a banking ecosystem today, for optimum prevention and response against emerging and quickly evolving threats, ML systems are required that help in faster threat detection such that service disruptions are minimized and customers' smooth access to his/her financial services is ensured.

Complex fraud schemes that are focused on a range of institutions at the same time expose the U.S. to systemic risk in the financial system and can unleash a series of defaults and market disruptions (Agbeve et al., 2025; Adebayo et al., 2025). Cross-institution data sharing and collaborative threat detection are key additions to machine learning systems to track coordinated fraud campaigns spanning several banking organizations. In these networks where institutions are interlinked, there is a need for ML algorithms that can detect systemic fraud threats by analyzing how transactions flow and how relationships pattern across organizational boundaries.

SOX requires U.S. publicly traded financial institutions to have stringent monetary controls and effective fraud detection procedures capable of detecting unauthorised access and transaction tampering. Machine learning systems need to support an auditable decision process and logging that are necessary to satisfy the SOX requirements. Advanced interpretable AI methods are necessary for regulatory auditors to explain the trustworthiness and correctness of fraud decisions made by ML.

Moreover, the Payment Card Industry Data Security Standard (PCI DSS) requires the implementation of certain security controls when processing payment card transactions, necessitating that a machine learning Fraud Detection System operate in an encrypted environment and still be able to analyze data in real-time (Bhutta et al., 2022; Amoako et al., 2025). The ML algorithms need to take into account the tokenization and encryption to be able to analyze the patterns of payments without revealing the cardholder's sensitive information involved in the detection process.

Federal Financial Institutions Examination Council (FFIEC) guidelines outline detailed standards for cybersecurity risk management and incident response preparedness, and expect machine learning fraud detection systems to integrate with the institution's security framework (Pinckard et al., 2016). ML models need to integrate threat intelligence feeds and external risk indicators to improve detection accuracy and foster coordinated incident response efforts across various banking functions.

Adherence to these sweeping regulatory requirements is crucial for U.S. banks deploying machine learning fraud detection solutions, as regulatory non-compliance can lead to hefty fines, limits on activities, and reputational harm. Continuous compliance monitoring and validation are key, as fraud is becoming complex by the day. New model development requires a continuous process of validation to comply with regulatory requirements, which can change at any time. Incorporating regulation-compliant functions into the ML fraud detection system is a key success factor for long-term viability in the overregulated banking world.

Types of Machine Learning Techniques

Machine learning technologies are playing an indispensable role in combating sophisticated fraud rings targeting U.S. banks. The development of fraudulent behavior necessitates sophisticated algorithmic strategies that are flexible in the recognition of patterns in real-time and in reacting to threats (Dupont, 2019). Such methods need to handle large volumes of transactional data while ensuring an extremely high level of accuracy and low false positives that might interfere with valid banking activities.

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: 9 | September 2025 -Peer-Reviewed Journal

Supervised learning techniques are widely used as the underlying mechanism of most fraud detection systems, which use labeled historical data sets to train models capable of detecting previously identified fraudulent patterns (Amoako et al, 2025). Decision trees and random forest-type algorithms are well suited to the mixed nature of the data that is typical in banking transactions that utilise numerical amounts, categorical merchant codes, and temporal patterns (Angelopoulos et al., 2019). The ensemble methods have an interpretable nature, which is ideal to satisfy regulatory compliance needs with strong generalization ability to various types of fraudulent activities.

Support vector machine (SVM) has been proven to be a powerful tool for high-dimensional fraud detection, in particular when the number of fraud incidents is rare compared to total activities. The SVM classifier successfully explores the non-linear decision plane, which is used to separate the normal and anomalous behavioral activities that could not be observed by normal statistical methods (Mensah et al., 2025). SVM implementations learn and encapsulate non-linear associations within transformed transaction data using the kernel trick without the need for explicit feature engineering (Alkhalil et al., 2021).

The use of neural network architectures has greatly increased the efficacy of fraud detection models by allowing the model to automatically learn from the raw transaction data more complex feature representations. Complex fraud patterns, invisible to rule-based fraud systems, can be detected by deep learning models. Such networks are shown to be effective in sequential transaction data processing for detecting temporal patterns of fraud activities (Babu, 2024). Recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are especially useful for the analysis of sequences of transactions and finding patterns of fraud that develop over time (Mensah et al., 2025). Such architectures might persist through transactional trails, which, in turn, may be used for the detection of advanced fraud trends that stretch over long periods. RNNs are ideally suited to analyzing customer-behavior sequences as they accommodate variable-length sequences and can thus be used to identify sudden 'change points' that indicate account takeovers or insider fraud (Mensah et al., 2025).

Unsupervised learning is heavily involved when it comes to fraud detection and can uncover new fraud patterns that were previously hidden and unknown, even if they haven't been previously labeled in the data. Methods, like k-means and hierarchical clustering, allow for grouping transaction data into behavioural clusters and indicate unusual patterns which should be investigated (Kaur Chahal et al., 2019). These methods are useful, especially for new fraud patterns that have no history from which to learn.

Among anomaly detection methods, methods such as Isolation Forests and One-class Support Vector Machines (OCSVM) work well when it comes to finding out the anomalies in transaction data that might indicate fraud behavior. These approaches develop baselines of normal behaviour and detect transactions that differ substantially from the expected pattern (Mensah et al., 2025). These methods are unsupervised and are particularly efficient in detecting Zero-Day fraud attacks and emergent threat vectors, which could be otherwise missed by the supervised models.

Ensemble techniques can combine various machine learning models to enhance the overall fraud detection and overcome the weaknesses of each model. Methods such as bagging, boosting, and stacking help in building strong detection systems by combining the decision results of various algorithms. Both gradient boosting machines and extreme gradient boosting have outperformed most of the classifiers in fraud-detection competitions and real case studies (Bouchama and Kamal, 2021).

In machine learning-based fraud detection, feature engineering and selection methods are important to ensure the best possible classifier performance. Advanced features can be generated to detect significant patterns in transaction data, such as velocity features, network features, and behavioural features. Strategies for dimensionality reduction address the high dimensionality aspect of banking data while maintaining the discriminatory information (Stanikzai and Shah, 2021).

Real-time processing is essential to machine learning fraud detection systems, where algorithms need to be able to process transactions in the millisecond range to stop an attack before it happens. With a stream processing framework and online learning algorithms in place, the model can be updated continuously as new transaction arrives, helping fraud detection systems to keep pace with the changing fraud patterns (Amoako et al., 2025). Fraud detection

processing is performed closer to where the transactions originate with edge computing deployments; thus, latency is dropped, and response times are increased.

Network-based machine learning algorithms became popular for fraud detection in banking networks. Graph neural networks can be used to understand intricate relationships across accounts, merchants, and transactions to detect fraud rings and coordinated attack schemes (Mensah et al., 2025). These methods are particularly good at identifying money laundering patterns and organized fraud networks that connect various accounts and institutions (Amoako et al., 2025).

They have already been applied to adaptive fraud detection systems, which can learn the optimal exploitation strategy by interacting with evolving fraudster behaviour. These methods allow fraud detection systems to trade detection performance for operational cost and dynamically adapt detection thresholds to catch new fraud patterns and meet changing business demands. It's possible that something like a multi-armed bandit can be a way to optimize a strategy for detecting fraud by constantly trying new things and figuring out what's working, and that could be turned into a general optimization.

Explainable AI methods are of great significance for fraud detection systems in regulated banking that can function to avoid fraud risk. Local Interpretable Model-agnostic Explanations (LIME), and SHapley Additive exPlanations (SHAP) to explain machine learning (ML) models for compliance and audit reasons (Kumarakulasinghe et al., 2020; Zafar & Khan, 2021). These methods give fraud analysts insight into which transactions were marked suspicious to aid in the investigation process and lower the falsely identified transaction rate (Cains et al., 2022).

Federated learning and omniset architecture enable a fraud detection model to be concurrently trained by multiple banks without sharing any sensitive customer data. These methods allow the development of stronger fraud detection systems through the use of collective knowledge, but at the same time do not violate privacy and regulatory requirements. Differential privacy guarantees that personalized transaction data is safe, while they do not prevent shared model building.

The state of the art in fraud detection systems is the combination of different machine learning methods via ensemble methods and hybrid designs. These integrated systems leverage the best attributes of different algorithmic families to deliver a comprehensive and robust fraud detection appliance that is designed to adapt to new threats, while remaining efficient and compliant (Ramakrishna, 2015).

Integration of AI and ML in Fraud Detection in the U.S.

The adoption of AI and machine learning tech in U.S. banks' fraud detection systems is a crucial development in financial security infrastructure. AI methods, including machine learning algorithms, natural language processing, and complex pattern recognition, have been increasingly integrated into the U.S. banking infrastructure to improve the effectiveness as well as the efficiency of fraud detection tools (Agbeve et al., 2025; Bhutta et al., 2022; Hassan et al., 2023). This revolution in technology is a response to increasingly sophisticated fraudulent activity that includes attempts to defraud U.S. financial institutions, and is also necessary because of the need to comply with regulatory requirements for fraud prevention systems.

From a U.S. banking perspective, transaction monitoring systems powered by AI are the core systems serving as the cornerstone of today's transactional fraud detection architecture. These systems analyze streams of transactional data as it is transmitted and completed, searching for suspicious patterns or anomalies that might suggest fraudulent activities within the banking industry (Adebayo et al., 2025). The ability to identify those deviations from common customer behavior, such as unusually high transaction amounts, strange spending behavior, and geographic discrepancies not pertaining to standard customer profiles, allows U.S. banks the ability to create real-time alerts to be investigated (Amoako et al., 2025). While real-time monitoring capability is especially important when compliance freezing is mandated under laws such as the Bank Secrecy Act and USA PATRIOT Act, to enable transaction monitoring and suspicious activity reporting (Amoako et al., 2025).

Behavioral biometrics is another key use case for AI in U.S. banking fraud prevention systems. These innovative AI methodologies scrutinize user behavior patterns and possession or intrinsic identifiers, such as mouse movement

patterns, or voice recognition signature, to authenticate the rightful users and also to detect an unauthorized access attempt or for identity theft (Firoozi & Mohsni,2023; Sharma and Elmiligi, 2022). For U.S. banks subjected to stringent regulation, behavioral biometrics offer an added layer of security as a complement to existing traditional authentication methods.

U.S. banks are increasingly deploying AI algorithms and systems at the back-end to safeguard customer accounts from fraud and cybercrimes. By examining user account data holistically, including account creation patterns, log-in behavioral analytics, and historical transaction analysis information, such AI-supported systems can detect account activities that stray from the norm and that could suggest fraudulent account creation or unauthorized account access (Hassan et al., 2023). This functionality is especially critical for U.S. banks as a result of regulatory demands such as customer identification programs and the management of money laundering activities as required by federal banking regulations (Amoako et al., 2025).

These kinds of advanced optimisation algorithms are being used in U.S. Banking to improve feature selection in fraud detection algorithms. Such optimization methods decide which data characteristics have the most influence and impact on the correct detection and categorization of fraud in banks. After the feature selection process, datasets are used to train and evaluate several classification models, and U.S. banks can implement the best fraud detection algorithms to be compliant with model validation and performance monitoring regulations.

ML/AI in cybersecurity: Pros and Cons

The adoption of machine learning (ML) and artificial intelligence (AI) in fraud detection and prevention by U.S. banks offers great promise as well as significant challenges that should be weighed in the broader regulatory and operational context within which they shape the business. The ability of ML/AI algorithms to sift through large amounts of transactional data to uncover subtle patterns or anomalies associated with fraudulent activities that could escape the reach of traditional rule-based detection models is a great step forward in fighting financial crime (Okoli et al., 2024). This ability is especially important in the U.S. banking industry as the large number of daily transactions from various channels introduces complexity that is beyond the traditional fraud detection methods.

ML/AI-based systems offer real-time tracking and monitoring of flows of transactions, customer activity patterns, and account-related activities, which help in quickly identifying fraudulent incidents as they surface in banking networks (Agbeve et al., 2025; Umoren et al., 2025). These systems are incredibly flexible, acquiring knowledge of new methods of fraud and adapting to the highly technical methods used by financial criminals, and they are well suited to the rapidly changing and more complex fraudulent environment confronting U.S. financial institutions. With the scalability of the technologies, banking systems can manage huge datasets that include various information sources, such as transaction histories and customer profiles, as well as threat intelligence feeds to be sourced from outside to form an overall fraud prevention ecosystem.

Also, ML/AI will allow for automation of the routine tasks of fraud detection, such as transaction monitoring, pattern identification, and initial incident response, potentially allowing the human analysts to concentrate on more complex investigatory work and strategic fraud prevention (Santos et al., 2024). This automation capability is critical for U.S. banks under heavy regulatory pressures to maximize efficiency and accuracy in fraud detection.

Despite all the positives, the use of ML/AI in fraud for banking in the US is fraught with a number of serious limitations and challenges that affect not only effectiveness but also regulatory compliance. ML/AI models exhibit strong reliance on the quality and representativeness of training data, which may be an issue, especially for fraud detection, because historical fraud data may not adequately reflect emerging fraud patterns (Adebayo et al., 2025). Bias or errors in the training data can feed into biased or error-prone fraudulent predictions and may generate fair lending and consumer protection implications, as well as possibly introduce new deficiencies in fraud monitoring capabilities.

The fact that AI/ML models are vulnerable to adversarial attacks is a major concern for fraud detection platforms, as fraudsters could intentionally tamper with transaction data or take advantage of model vulnerabilities to escape detection methods (Agbeve et al., 2025; Umoren et al., 2025). These adverse attacks pose a fundamental threat to the reliability and efficacy of ML/AI-based fraud prevention defenses, which results in considerable operational and regulatory risk for banks. The difficulty in explaining or interpreting the decisions of ML/AI again makes the use of

these kinds of algorithms more challenging in fraud detection, as regulatory restrictions, especially in the financial domain, may force banks to explain why certain decisions have been made (Amoako et al., 2025).

Non-interpretability of ML/AI-based fraud detection systems may adversely affect trust among stakeholders, increase challenges for audits, and make it difficult to comply with rules and regulations demanding transparency of the systems applied to customer accounts and transactions (Agbadamasi et al., 2025; Adebayo et al., 2025). Although there is little doubt that ML/AI techniques can boost the detection of fraudulent activities in the U.S. banking industry, the overarching effectiveness of these technologies in the context of financial crime prevention, in general, should not be overstated as having the ability to address fraud. Nonetheless, human expertise and oversight are expected to remain necessary for interpreting algorithmic output, validating fraud investigations, decision-making in strategic fraud prevention efforts, and complying with a changing regulatory environment (Adebayo et al., 2025).

Adoption of ML/AI technologies for fraud detection and prevention in U.S. banking should take these benefits, limitations, and their implications for regulatory compliance and operational effectiveness into account. Although these approaches offer great potential for enhancing fraud detection and preventing banks and their customers from falling prey to emerging threats, their effective use requires careful strategies for deployment that maximize benefits, minimize threats, and ensure compliance with rules and regulations that apply to financial services within the U.S.

CONCLUSION

The researchers, therefore, conclude that the paradigmatic shift toward digital banking infrastructure within the United States financial sector has precipitated a fundamental reconceptualization of fraud detection methodologies, which positions artificial intelligence and machine learning technologies as transformative catalysts in contemporary cybersecurity frameworks. The inadequacies of legacy rule-based detection systems in addressing the exponentially evolving threat landscape have compelled financial institutions to embrace AI/ML paradigms that deliver sophisticated, real-time, adaptive detection capabilities through advanced predictive analytics architectures. These computational frameworks demonstrate unprecedented efficacy in fraud identification through their capacity to discern complex latent patterns within high-dimensional transactional datasets, conduct thorough behavioral biometric analysis, and execute comprehensive anomaly detection across heterogeneous data streams with remarkable precision and temporal efficiency. Notwithstanding these demonstrable advantages, the operationalization of AI/ML solutions within fraud detection ecosystems encounters substantial impediments encompassing stringent regulatory compliance requirements, evolving data privacy mandates and the imperative for algorithmic interpretability and explainability that satisfies both supervisory scrutiny and stakeholder transparency demands. Consequently, U.S. banking institutions must orchestrate a delicate equilibrium between technological innovation and regulatory conformity, necessitating the development of transparent, auditable and resilient AI/ML architectures that integrate federated learning methodologies, explainable AI frameworks and collaborative industry-wide data sharing initiatives. Given the trajectory of increasingly sophisticated cyber threats, the future viability of fraud prevention within the U.S. banking sector is intrinsically dependent upon the strategic deployment of advanced AI/ML systems within a comprehensively regulated, ethically governed and dynamically responsive cybersecurity ecosystem that maintains adaptive capacity for emerging threats, however ensuring unwavering regulatory compliance and operational integrity.

REFERNCES

1. *Adebayo, O., Attionu, G. T., Singh, D., Mensah, N., Adukpo, T. K. (2025). Impact of Digital Transformation on Liquidity Management Among U.S. Multinational Corporations. International Journal of Multidisciplinary Research, 7(2), 1-13.*
2. *Adebayo, O., Mensah, N., Adukpo, T. K. (2025). Beyond Cash Flow Management: How Machine Learning and Scenario Planning Drive Financial Resilience. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 81-89. https://doi.org/10.36713/epra20503*
3. *Adebayo, O., Mensah, N., Adukpo, T. K. (2025). Navigating Liquidity Management Challenges in the Era of Digital Banking in the United States. World Journal of Advanced Research and Reviews, 25(2), 2711-2719.*
4. *Adelakun, B.O., 2023. How Technology Can Aid Tax Compliance in the US Economy. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(2), pp.491-499.*
5. *Adelakun, B.O., Nembe, J.K., Oguejiofor, B.B., Akpuokwe, C.U. and Bakare, S.S., 2024. Legal frameworks and tax compliance in the digital economy: a finance perspective. Engineering Science & Technology Journal, 5(3), pp.844-853.*
6. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). The Role of Business Intelligence in AI Ethics: Empowering U.S. Companies to Achieve Transparent and Responsible AI. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 8-14. https://doi.org/10.36713/epra2031*

7. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). Artificial Intelligence Governance in U.S. Corporations: Legal and Ethical Implications for Business Intelligence and Regulatory Compliance. International Journal of Research Publication and Reviews, 6(3), 3083-3089.*
8. *Agbadamasi, T. O., Opoku, L. K., Adukpo, T. K., Mensah, N. (2025). Navigating the Intersection of U.S. Regulatory Frameworks and Artificial Intelligence: Strategies for Ethical Compliance. World Journal of Advanced Research and Reviews, 25(3), 969-979. https://doi.org/10.30574/wjarr.2025.25.3.0814*
9. *Agbeve, V., Adukpo, T. K., Mensah, N., Appiah, D., Atisu, J. C. (2025). Comparative Analysis of Digital Banking and Financial Inclusion in the United States: Opportunities, Challenges and Policy Implications. Asian Journal of Economics, Business and Accounting, 25(3), 452-467.*
10. *Ali, S. M., Augusto, J. C., & Windridge, D. (2019). A survey of user-centred approaches for smart home transfer learning and new user home automation adaptation. Applied Artificial Intelligence, 33(8), 747-774.*
11. *Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.*
12. *Al-Mansoori, S., & Salem, M. B. (2023). The role of artificial intelligence and machine learning in shaping the future of cybersecurity: trends, applications, and ethical considerations. International Journal of Social Analytics, 8(9), 1-16.*
13. *Amoako, E.K.W., Boateng, V., Ajay, O., Adukpo, T.K., Mensah, N. (2025). Exploring the Role of Machine Learning and Deep Learning in Anti-Money Laundering (AML) Strategies within U.S. Financial Industry: A Systematic Review of Implementation, Effectiveness, and Challenges. Finance & Accounting Research Journal, 7(1). https://doi.org/10.51594/farj.v7i1.1808*
14. *Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A., Voliotis, S., & Zahariadis, T. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 20(1), 109.*
15. *Atisu, J. C., Mensah N., Alipoe, S. A., Rahman, S. A. (2024). The Effect of Non-Performing Loans on the Financial Performance of Commercial Banks in Ghana. Iosr Journal of Economics and Finance, 15(5), 42-48. https://doi.org/10.9790/5933-1505054248*
16. *Babu, C. S. (2024). Adaptive AI for Dynamic Cybersecurity Systems: Enhancing Protection in a Rapidly Evolving Digital Landscap. In Principles and Applications of Adaptive Artificial Intelligence (pp. 52-72). IGI Global.*
17. *Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal, 5(3), 528-543.*
18. *Bhutta, M. N. M., Bhattia, S., Alojail, M. A., Nisar, K., Cao, Y., Chaudhry, S. A., & Sun, Z. (2022). Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). Wireless communications and mobile computing, 2022(1), 9942270.*
19. *Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.*
20. *Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.*
21. *Chaudhry, M., Shafi, I., Mahnoor, M., Vargas, D. L. R., Thompson, E. B., & Ashraf, I. (2023). A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. Symmetry, 15(9), 1679.*
22. *Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity, 5(1), tyz013.*
23. *Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: a comparative study. International Journal of Disclosure and Governance, 20(4), 451-477.*
24. *Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. Sn Business & Economics, 3(5). https://doi.org/10.1007/s43546-02300477-6*
25. *Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.*
26. *https://doi.org/10.9734/ajeba/2025/v25i31722*
27. *Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. Journal of Economics, Finance and Accounting Studies, 6(1), 67-77.*
28. *Kanagaraj, P. (2020). EDUCATIONAL SECTOR. In National Level Virtual Conference On (p. 29).*
29. *Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: a threat or challenge. New Review of Information Networking, 24(1), 31-103.*
30. *Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), 417. https://doi.org/10.3390/info12100417*
31. *Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund.*

32. *Kumarakulasinghe, N. B., Blomberg, T., Liu, J., Leao, A. S., & Papapetrou, P. (2020, July). Evaluating local interpretable model-agnostic explanations on clinical machine learning classification models. In 2020 IEEE 33rd international symposium on computer-based medical systems (CBMS) (pp. 7-12). IEEE*
33. *Lee, I. (2020). Internet of things (iot) cybersecurity: literature review and iot cyber risk management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157*
34. *Ng, A. and Kwok, B. (2017). Emergence of fintech and cybersecurity in a global financial centre. Journal of Financial Regulation and Compliance, 25(4), 422-434. https://doi.org/10.1108/jfrc-01-2017-0013*
35. *Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms.*
36. *Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T., & Daraojimba, C. (2023). Cybersecurity in US and Nigeria banking and financial institutions: review and assessing risks and economic impacts. Advances in Management, 1(2).*
37. *Pinckard, J., Rattigan, M., & Vrtis, R. (2016). Mapping of the Federal Financial Institutions Examination Council (FFIEC) cybersecurity assessment tool (CAT) to the cyber resilience review (CRR).*
38. *Pomerleau, P. L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer.*
39. *Ramakrishna, S. (2015). Enterprise compliance risk management: an essential toolkit for banks and financial services. John Wiley & Sons.*
40. *Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.*
41. *Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019, October). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In 2019 international carnahan conference on security technology (ICCST) (pp. 1-8). IEEE.*
42. *Sharma, M., & Elmiligi, H. (2022). Behavioral biometrics: past, present and future. Recent Advances in Biometrics, 69.*
43. *Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of cyber security threats in banking systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-4). IEEE.*
44. *Umoren, J., Adukpo, T. K., & Mensah, N. (2025). Leveraging Artificial Intelligence in Healthcare Supply Chains: Strengthening Resilience and Minimizing Waste. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(2), 190-196. https://doi.org/10.36713/epra20385*
45. *Umoren, J., Adukpo, T. K., Mensah, N. (2015). Exploring factors, outcomes, and benefits in supply chain finance: Insights and future directions for the U.S. healthcare system. World Journal of Advanced Research and Reviews, 25(02), 060-071. https://doi.org/10.30574/wjarr.2025.25.2.0345*
46. *Umoren, J., Korang, A., Utomi, E., Adukpo, T. K., Mensah, N. (2025). The Importance of Utilizing Big Data Analytics in U.S. Healthcare Supply Chain Management. EPRA International Journal of Multidisciplinary Research, 11(3), 411-421. https://doi.org/10.36713/epra20572*