**AI- Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity**

**Abstract**

*This study investigates the limitations of traditional fraud detection techniques in digital banking and explores the applicability of AI-powered behavioral biometrics as a next-generation solution for enhancing cybersecurity. Utilizing the PaySim Financial Transactions Dataset, Credit Card Fraud Detection Dataset, and HMOG Dataset, this research applies machine learning models including Random Forest, Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), and Gradient Boosting Machines. Quantitative metrics such as Accuracy, Precision, Recall, F1 Score, and AUC-ROC were evaluated. The LSTM network achieved 97.9% accuracy, 95.6% precision, and 93.4% recall, outperforming other models. Results reveal that deep learning frameworks significantly enhance fraud detection efficiency, minimize false positives, and improve prediction accuracy. Recommendations include integrating deep learning models, developing ethical guidelines, upgrading infrastructure, and advancing predictive algorithms to address evolving threats and improve operational efficiency in digital banking security.*

**Keywords: Behavioral Biometrics, LSTM Network, Fraud Detection, Deep Learning, Digital Banking**

**1. Introduction**

The rapid digitization of banking has significantly transformed the financial services industry, offering enhanced accessibility, efficiency, and convenience. However, this transformation has simultaneously intensified the issues of threat, as increasingly complex cybersecurity risks and fraud mechanisms continue to undermine digital banking integrity. Cybercriminals now deploy sophisticated techniques, including phishing, social engineering, remote access abuse, synthetic identity fraud, and deepfake technology, rendering traditional rule-based fraud detection systems largely inadequate (Shamoo, 2024). Consequently, there is a critical need for adaptive, intelligent, and user-centered fraud prevention frameworks.

According to Awad et al. (2024), one of the most promising innovations in contemporary cybersecurity is the integration of AI-powered behavioral biometrics. This method shifts the paradigm from static identifiers—such as passwords, tokens, or even facial and fingerprint recognition—to real-time analysis of user behavior. Behavioral biometrics captures dynamic interaction patterns, including keystroke dynamics, mouse movement, touchscreen input, and device handling. In mobile contexts, this extends to gait and voice characteristics. Akhtar and Rawol (2024) argues that this continuous form of authentication enables security systems to assess user legitimacy without disrupting the digital experience, thereby offering a balance between usability and protection.

Artificial intelligence and machine learning are central to the effectiveness of behavioral biometrics. These technologies establish individualized behavioral baselines by processing extensive datasets drawn from user-device interaction. Once this baseline is set, even minor deviations—such as irregular typing speed, abnormal cursor movement, or inconsistent screen swipes—may trigger alerts or preventative actions. Piugie (2023) posits that this method addresses key limitations of traditional systems, particularly the high incidence of false positives and the failure to detect sophisticated threats that fall outside standard transactional parameters.

Rather than merely validating what a user does, behavioral biometrics assesses how they do it. This distinction offers a more precise and context-aware evaluation of authenticity, reducing risks related to account takeovers and identity theft—even in cases where login credentials have been compromised. In the view of Bardin (2024), this behavior-based approach constitutes a vital enhancement to digital security protocols, particularly as cybercriminals grow increasingly adept at circumventing conventional safeguards.

Recent data substantiates the need for these advanced systems. In 2023, global digital payment fraud losses totaled $485.6 billion (Kessler, 2025). In the U.S., every dollar lost to fraud translates into $4.23 in secondary costs, including investigation and operational disruption (LexisNexis, 2022). Elad (2025) observes that over one-third of financial institutions faced more than 1,000 fraud attempts annually, with roughly 10 percent confronting over 10,000. These statistics demonstrate the ineffectiveness of static tools and highlight the urgency for behaviorally adaptive solutions.

Real-world applications further affirm the viability of behavioral biometrics. Noonan and Smith (2024) note that a U.S.-based fintech firm prevented nearly $5.8 million in monthly fraud losses through behavioral analytics. Similarly, a major Latin American bank recorded a 67 percent reduction in social engineering attacks (Okunytė, 2024), while an Australian financial firm disrupted over 90 percent of mule account operations by combining behavioral and device-based intelligence (Crozier, 2024). These case studies reflect the broad applicability and measurable impact of such technologies across diverse financial settings.

Academic and commercial research alike have documented the high accuracy of behavioral biometrics. According to Preciado Martínez et al. (2025), the use of Random Forest and deep learning classifiers reported a fraud detection accuracy of 96.3 percent. Furthermore, Koprowski (2025) states that providers such as Outseer have incorporated behavioral biometrics into their fraud prevention ecosystems, including 3D Secure authentication protocols, resulting in a 54 percent reduction in false positives and improved user satisfaction.

Market dynamics reveal an accelerating investment in behavioral security. The global behavioral biometrics market, valued at $1.66 billion in 2023, is projected to reach $14 billion by 2032, growing at a compound annual rate of 26.77 percent (GrandViewResearch, 2022). This expansion is fueled not only by heightened cyber threats and fraud-related losses but also by increasing regulatory demands and evolving consumer expectations. For instance, Visa has committed $12 billion to AI and data initiatives, while the Commonwealth Bank integrates behavioral analytics through platforms like Truyu to enhance user verification (Bloomberg Intelligence, 2024).

Despite these advancements, significant implementation challenges persist. North-Samardzic (2019) avers that behavioral biometric systems raise substantial ethical and regulatory concerns, especially regarding data privacy. The continuous collection and analysis of behavioral patterns demand robust data governance and transparent consent practices. Moreover, the reliability of behavioral models can be compromised by legitimate changes in user behavior—due to stress, illness, or unfamiliar devices—potentially resulting in both false positives and negatives.

Technical integration also presents substantial obstacles. Many legacy infrastructures are incompatible with behavioral intelligence systems, necessitating costly upgrades and redesigns. According to Peters (2024), 79 percent of banks expressed high confidence in behavioral biometrics, but only 22 percent had implemented the technology—primarily due to concerns over integration complexity and regulatory compliance.

Additionally, as fraud tactics evolve, behavioral systems must continuously adapt to emerging threats. For example, French (2024) notes that deepfake-enabled fraud surged by 704 percent in 2023, while synthetic identity fraud remains a persistent vulnerability within digital onboarding and verification systems. These developments underscore the need for continuous refinement of AI-driven security mechanisms.

The surge in mobile banking has further intensified the urgency for advanced fraud prevention. Between 2022 and 2023, U.S. mobile banking usage grew from 54 percent to 73 percent, paralleled by an increase in mobile-originated fraud from 47 percent to 61 percent (MX, 2024). Behavioral biometrics offers a key advantage in this environment by supporting non-intrusive, continuous authentication across platforms and devices.

Industry collaborations are accelerating these integrations. The partnership between Feedzai and Mastercard is a model of how behavioral intelligence can be merged with transactional monitoring to create holistic fraud prevention frameworks (Harris, 2025). Similarly, Sopra Steria’s AI-based solution for Iberpay reflects an emerging consensus that layered, AI-enhanced strategies are essential in addressing the complex cybersecurity challenges confronting the financial sector (SopraSteria, 2025). This research aims to examine the effectiveness and applicability of AI-powered behavioural biometrics as an advanced fraud detection mechanism in digital banking and to evaluate its potential as a next-generation solution for strengthening financial cybersecurity by achieving the following objectives:

1. Investigates the limitations of traditional fraud detection techniques in digital banking and highlights the need for more adaptive, intelligent systems.
2. Explores how AI and machine learning algorithms are applied in behavioral biometrics to detect anomalies and prevent fraudulent activities in real-time.
3. Assesses the impact of behavioral biometric technologies on fraud detection efficiency, customer experience, and false positive reduction through relevant case studies and industry reports.
4. Examines the future prospects, potential challenges, and ethical implications of implementing AI-powered behavioral biometrics in digital banking platforms.

## **2. Literature Review**

Conventional fraud detection systems in digital banking have primarily depended on rule-based mechanisms, multi-factor authentication (MFA), transactional anomaly detection, and device fingerprinting (Malinka et al., 2022). Rule-based systems function by applying predefined thresholds and geographic parameters to flag potentially fraudulent activity (do Nascimento et al., 2024). Although Olushola and Mart (2024) assert that these systems are straightforward to deploy and effective in identifying established fraud typologies, their static configuration makes them ineffective against rapidly evolving threats. Fraudsters routinely adapt their methods to circumvent known rules, and the rigidity of these systems often results in elevated false positive rates, disrupting legitimate transactions and imposing unnecessary operational burdens (Vorobyev & Krivitskaya, 2022; Ajayi et al., 2025).

Multi-factor authentication introduced an additional layer of protection by combining credentials such as passwords with biometric data, tokens, or one-time passcodes. However, the reliability of MFA has diminished due to the proliferation of phishing tactics, SIM-swapping schemes, and social engineering exploits (Burton, 2024; Balogun, 2025). Alkhalil et al. (2021) posit that attackers increasingly manipulate users into divulging both primary and secondary credentials, thereby neutralizing the protective intent of MFA. The vulnerability is exacerbated by the widespread accessibility of personal data, much of which is sourced through data breaches or shared on social platforms, rendering knowledge-based authentication particularly susceptible to compromise (Suleski et al., 2023; Kolade et al., 2025).

Transactional anomaly detection, designed to identify deviations from established user transaction histories, offers some defense against fraud. However, its reliance on financial metrics alone renders it ineffective in scenarios involving contextual deception, such as coercion or remote access tool abuse (Palakurti, 2024; Obioha-Val, 2025). It also lacks the ability to account for behavioral cues that might indicate unauthorized access. Device fingerprinting, while valuable in identifying and tracking user devices, is similarly constrained. It is vulnerable to spoofing technologies, remote desktop tools, and user behavior that involves switching devices or employing privacy-enhancing tools (Bezawada et al., 2019; Olutimehin, 2025).

The emergence of advanced threats—including synthetic identities, deepfake impersonations, and adaptive social engineering- has further exposed the limitations of traditional detection methods. Chawki (2025) argues that these threats exploit the inherent inflexibility of legacy systems, which lack cognitive and contextual processing capabilities. The absence of behavioral intelligence prolongs the time between threat inception and detection, expanding the window for exploitation (Bhardwaj et al., 2022; Balogun et al., 2025). Additionally, excessive verification procedures associated with these legacy methods contribute to user fatigue, potentially deterring customers and prompting migration toward platforms that may prioritize convenience over security (Dakić et al., 2025; Obioha-Val et al., 2025). Consequently, the imperative for behavior-aware, AI-augmented fraud detection mechanisms has intensified.

**Conceptual Framework and Evolution of Behavioural Biometrics**

Behavioral biometrics refers to the analysis of distinct patterns in how individuals interact with digital systems, offering an adaptive and continuous form of authentication that extends beyond static credentials or physiological identifiers (Ayeswarya & Singh, 2024; Balogun et al., 2025). This method captures traits such as keystroke dynamics, touchscreen gestures, mouse movement, gait, and voice modulation. According to Salice and Salice (2024), these characteristics are shaped by an individual’s physical, psychological, and contextual states, making them inherently difficult to replicate or steal.

Unlike traditional biometrics that rely on fixed traits for one-time authentication—such as fingerprint or facial recognition—behavioral biometrics enable passive, ongoing verification throughout a session (Thomas & Preetha Mathew, 2023; Obioha-Val et al., 2025). In the view of Piugie (2023), this approach reduces user friction while enhancing the system’s ability to detect unauthorized access or session hijacking after the initial login, a limitation common in conventional methods.

The conceptual foundation of behavioral biometrics emerged in the 1990s with research into keystroke dynamics. Kadena et al. (2022) identify Monrose and Rubin as early proponents who demonstrated the viability of typing patterns for user identification. The development of sensor-rich mobile devices expanded the behavioral data available, leading to new dimensions of analysis, such as swipe dynamics and gait recognition (Teng et al., 2024; Olutimehin, 2025). The 2010s marked a shift from academic research to practical application, as cybersecurity firms like BioCatch and TypingDNA adapted behavioral techniques into fraud prevention tools for financial institutions (Sharma & Elmiligi, 2022; Obioha-Val et al., 2025).

Artificial intelligence has significantly advanced this field. Ranjan and Kumar (2021) posit that deep learning algorithms now enable the construction of behavioral profiles that evolve alongside legitimate user behavior, allowing systems to distinguish between normal variability and suspicious activity. This adaptability improves both the accuracy and resilience of fraud detection, particularly in confronting sophisticated attack vectors such as synthetic identity fraud or remote access tool misuse.

Despite ongoing concerns regarding data privacy and ethical use, behavioral biometrics has transitioned from a theoretical construct to a critical component of digital security infrastructure. According to Kumar et al. (2025), its integration into cybersecurity frameworks offers real-time, behavior-based protection that aligns with the increasing complexity of threats in digital banking environments. The evolution of this technology underscores its growing relevance and necessity in safeguarding both user identity and institutional integrity.

**AI and Machine Learning Integration in Behavioural Biometrics**

Artificial intelligence and machine learning form the technological backbone of behavioral biometrics in fraud detection, providing enhanced capabilities in accuracy, scalability, and adaptability (Ahmad, 2023; Olutimehin, 2025). These systems process vast datasets derived from user interactions—including keystrokes, swipe gestures, mouse dynamics, and device orientation—beginning with a critical phase of data pre-processing. This stage involves cleansing, normalization, and feature extraction, ensuring that raw behavioral signals are properly structured for computational analysis. The precision and reliability of this preparatory phase directly determine the model’s effectiveness in differentiating between legitimate and fraudulent behaviors (Chhabra Roy & Prabhakaran, 2022; Alao et al., 2024).

Following preprocessing, both supervised and unsupervised machine learning algorithms are employed to build classification models (Albahra et al., 2023; Olutimehin et al., 2025). Traditional classifiers such as Random Forests and Support Vector Machines have demonstrated high performance when applied to structured behavioral datasets (Mohd Ali et al., 2022; Balogun et al., 2025). However, in recent years, advanced deep learning frameworks, including Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs), have become increasingly prominent due to their ability to detect temporal dependencies and complex behavioral anomalies (Gandhi et al., 2021; Balogun et al., 2025). According to Islam and Washington (2024), deep learning architectures are particularly suited for identifying subtle, nonlinear patterns in user behavior within mobile and web-based banking environments.

A key application of these AI techniques lies in constructing and refining behavioral baselines and personalized models that represent each user’s typical interaction profile. These baselines are not fixed; instead, Liao et al. (2021) argue that they are continuously updated through machine learning feedback mechanisms, which enable systems to accommodate legitimate behavioral shifts while remaining responsive to anomalies. The dynamic learning capability facilitates the detection of fraudulent behaviour, such as inconsistent typing cadence, erratic cursor movement, or unusual screen gestures. This adaptability also plays a vital role in reducing false positive rates, thereby enhancing user experience and operational efficiency (Bello et al., 2024; Tiwo et al., 2025).

Empirical studies further affirm the effectiveness of AI-integrated behavioral biometrics. According to Preciado Martínez et al. (2025), the combination of Random Forest and deep neural networks achieved a fraud detection accuracy of 96.3 percent. Commercial adoption supports these findings; Koprowski (2025) notes that platforms such as Feedzai, Outseer, and BioCatch have successfully embedded behavioral biometric models within real-time authentication processes, including login verification, transaction analysis, and 3D Secure (3DS) protocols (Harris, 2025; Tiwo et al., 2025). These applications affirm the indispensable role of AI in modern fraud prevention architecture.

**Case Studies Demonstrating the Efficacy of Behavioural Biometrics**

Empirical evidence from diverse financial institutions demonstrates the operational effectiveness of AI-powered behavioral biometrics in combating digital banking fraud. A leading U.S. financial technology firm reported monthly fraud prevention exceeding $5.8 million in card and Automated Clearing House (ACH) transactions following the adoption of behavioral analytics within its fraud detection framework (Noonan & Smith, 2024; Metibemu et al., 2025). By continuously analysing user interaction variables—such as login cadence and navigation trajectories—the system successfully identified compromised accounts and automated bot activities that traditional rule-based protocols failed to detect. According to Rangaraju (2023), the system’s responsiveness to behavioral deviations substantially enhanced real-time threat mitigation.

A similar implementation by a major Australian bank employed both behavioral and device intelligence to disrupt over 90 percent of mule account operations (Crozier, 2024; Olutimehin et al., 2025). This initiative focused on detecting anomalies in user-device interaction and identifying non-human behavioral signatures indicative of automated fraud schemes. Piugie (2023) contends that this approach illustrates how behavioral biometrics extend beyond authentication, serving as a diagnostic tool for uncovering the behavioral traits of fraud facilitators.

In another case, a prominent Latin American bank reported a 67 percent decline in social engineering fraud targeting mobile banking users (Okunytė, 2024; Oyekunle et al., 2025). By analysing metrics such as touchscreen pressure, swipe velocity, and typing hesitation, the system differentiated between coerced and authentic user behaviour. Parwej et al. (2024) posit that this represents a critical advancement, as conventional multifactor authentication systems often fail to detect user duress. In the domain of customer onboarding, a leading challenger bank successfully prevented over $1 million in new account fraud by employing behavioral analytics to flag anomalies suggestive of synthetic identities or illegitimate applications (BioCatch, 2025).

From a technological integration standpoint, Sopra Steria’s AI-enhanced platform for Iberpay illustrated the viability of embedding behavioral biometrics into high-frequency, national interbank payment systems (SopraSteria, 2025). SopraSteria (2025) notes that this solution facilitated low-latency fraud detection at scale, affirming the adaptability of behavioral analytics in institutional contexts. Meanwhile, the Commonwealth Bank’s Truyu app integrated behavioral insights to deliver real-time identity alerts to users, thereby reinforcing both security transparency and customer trust (Bloomberg Intelligence, 2024).

Across these implementations, consistent performance indicators—such as reduced financial losses, lower false positive rates, and improved user satisfaction—affirm that behavioural biometrics constitutes a scalable and effective mechanism within advanced fraud prevention systems.

**Market Trends and Industry Adoption**

The escalating complexity of digital banking fraud has compelled financial institutions to pursue more adaptive and intelligence-driven solutions, positioning behavioural biometrics as a promising extension of artificial intelligence within cybersecurity frameworks. Although more than 75 percent of financial institutions globally have implemented AI for fraud detection, the specific deployment of behavioral biometrics remains relatively limited. According to Peters (2024), only 22 percent of institutions currently utilize behavioral biometrics, despite 79 percent expressing strong confidence in its potential effectiveness. This discrepancy suggests that while institutional perception is favorable, barriers such as regulatory uncertainty, integration challenges, and legacy infrastructure constraints are impeding widespread adoption.

Nonetheless, market projections point toward substantial growth. GrandViewResearch (2022) reports that the global behavioral biometrics market, valued at $1.66 billion in 2023, is projected to reach nearly $14 billion by 2032, reflecting a compound annual growth rate of 26.77 percent. This trajectory is driven by increasing digital payment activity, rising cyber fraud incidents, and escalating demand for security mechanisms that do not compromise user convenience. In the view of MX (2024), the surge in mobile banking usage—from 54 percent in 2022 to 73 percent in 2023, paralleled by a rise in mobile-based fraud from 47 percent to 61 percent- highlights the urgent need for more context-aware and behavior-sensitive authentication technologies.

Strategic industry investments further underscore the anticipated centrality of behavioural analytics in financial cybersecurity. Bloomberg Intelligence (2024) notes that Visa’s $12 billion allocation to AI and data science over five years reflects a deliberate focus on predictive fraud detection, in which behavioral insights are expected to be integral. Similarly, Mastercard’s collaboration with Feedzai illustrates the incorporation of behavioral intelligence into enterprise-level fraud prevention systems (Harris, 2025; Salako et al., 2025). BioCatch’s engagement with over 100 major global banks in 2022 signals a growing institutional commitment to behavioral biometric models for continuous authentication and scam prevention (BioCatch, 2022).

**Challenges, Limitations, and Ethical Considerations**

While AI-powered behavioral biometrics presents notable advancements in digital banking security, its integration is accompanied by significant operational, technical, and ethical complexities. A primary challenge lies in embedding these systems within legacy banking infrastructures, which often lack the architectural flexibility to support real-time behavioral analytics (Ogunwole et al., 2023; Salako et al., 2025). George (2024) asserts that the associated implementation costs, encompassing infrastructure upgrades, data migration, and workforce training, can be prohibitive, particularly for smaller institutions. Furthermore, the computational intensity required to process continuous behavioral data demands scalable, high-performance systems, which are not uniformly accessible across the financial sector (Usman et al., 2023; Salami et al., 2025).

Another notable limitation stems from the natural variability of human behaviour. Factors such as emotional stress, physical illness, fatigue, or interaction with unfamiliar devices can alter user patterns, thereby affecting authentication reliability. Such inconsistencies increase the incidence of false positives and false negatives, compromising user access and system dependability (Akhtar et al., 2024). Although AI models can adjust to some behavioral changes, achieving a precise equilibrium between detection sensitivity and tolerance remains a persistent technical challenge.

Ethical and regulatory concerns compound these issues. Behavioural biometric systems operate by continuously collecting sensitive user data, often without explicit user awareness beyond initial consent. Adeniyi et al. (2024) posit that this raises critical concerns surrounding informed consent, user autonomy, and data transparency. Financial institutions must ensure compliance with data protection frameworks such as the General Data Protection Regulation (GDPR) and the Revised Payment Services Directive (PSD2), requiring clear data usage declarations, strict data minimization, and secure data processing protocols (Gounari et al., 2024).

The increasing opacity of AI algorithms, particularly those leveraging deep learning, introduces further complications. As Mandal and S (2023) note, explaining why specific behaviors are flagged as fraudulent becomes difficult, potentially eroding institutional accountability and user trust. Moreover, the rise of adversarial AI, such as deepfake-enabled identity manipulation and behavioral spoofing, poses emerging threats (Dsouza et al., 2024). Tiwo et al. (2025) argue that as these tactics evolve in sophistication, behavioral biometric systems must be continually updated and supported by multilayered defense mechanisms to maintain effectiveness and resilience within financial cybersecurity infrastructures.

### **3. Methods**

This study employs a quantitative approach to assess the effectiveness of AI-powered behavioral biometrics in digital banking fraud detection. Publicly available datasets are utilized, namely the PaySim Financial Transactions Dataset, the Credit Card Fraud Detection Dataset, and the HMOG Dataset. Data preprocessing includes normalization, feature extraction, dimensionality reduction using Principal Component Analysis (PCA), and Z-score standardization to ensure consistency and enhance computational efficiency.

Machine learning techniques, including Random Forest (RF) and Long Short-Term Memory (LSTM) Networks, are employed for anomaly detection and classification. Random Forest is applied for its robustness in handling high-dimensional data, with the Gini Index used as a criterion for node splitting. LSTM networks are leveraged for their ability to detect temporal dependencies in behavioral data, using cell state update and output equations to capture sequential patterns effectively.

Model performance is evaluated using multiple quantitative metrics, including Accuracy, Precision, Recall, F1 Score, and AUC-ROC. Statistical validation is performed using the paired T-test to compare AI-based methods against traditional fraud detection techniques. Additionally, Time-Series Analysis is employed to assess the stability of LSTM models over time, using the Autocorrelation Function (ACF).

Utilizing anonymized datasets and adhering to established data protection regulations ensures data privacy and ethical compliance. Table 1 presents the formulas used throughout the analysis.

#### Table 1: Mathematical Formulas Applied in Analysis

|  |  |  |
| --- | --- | --- |
| **Formula Name** | **Formula** | **Description** |
| Principal Component Analysis (PCA) |  | Dimensionality reduction through eigenvector transformation. |
| Z-score Normalization |  | Standardizes data to a common scale. |
| Gini Index |  | Measures node purity in Random Forest models. |
| Random Forest Prediction |  | Aggregates predictions from multiple decision trees. |
| LSTM Cell State Update |  | Calculates LSTM cell state during training. |
| LSTM Output |  | Determines LSTM network's output. |
| Accuracy |  | Measures overall model performance. |
| Precision |  | Evaluates the relevance of positive predictions. |
| Recall |  | Measures sensitivity of the model. |
| F1 Score |  | Balances Precision and Recall. |
| AUC-ROC |  | Evaluates model discrimination capability. |
| Paired T-test |  | Compares two related samples for statistical significance. |
| Autocorrelation Function (ACF) |  | Identifies patterns over time. |

This structured methodology integrates advanced machine learning techniques with rigorous statistical evaluation, enhancing the reliability and robustness of the results.

**4. Results and Discussion**

### **Investigating the Limitations of Traditional Fraud Detection Techniques in Digital Banking**

The increasing sophistication of fraud mechanisms within digital banking necessitates the development of more adaptive and intelligent systems for fraud detection. Traditional approaches, such as rule-based methods and anomaly detection systems, have been extensively employed to mitigate fraudulent activities. However, these methods often result in high false favorable rates, inefficient detection of novel fraud patterns, and the inability to adjust to evolving threats dynamically. This section examines the limitations of traditional fraud detection techniques by evaluating their performance metrics using descriptive and comparative analysis.

The findings from the comparative analysis between traditional fraud detection techniques and the labeled fraud entries in the dataset reveal several critical insights. The evaluation metrics include accuracy, precision, recall, and F1 score, which are quantitatively assessed to highlight the performance gaps inherent in traditional approaches.

As shown in Table 2, traditional rule-based methods achieved a high accuracy of 96.42%. However, the system produced a significantly low precision score and recall value, which indicates a high rate of false positives and missed fraudulent activities, respectively. These limitations underscore the inability of static models to effectively adapt to dynamic and evolving fraudulent behaviors.

##### **Table 2: Fraud Detection Performance Results**

|  |  |
| --- | --- |
| Metric | Value |
| True Positives (TP) | 0 |
| True Negatives (TN) | 4821 |
| False Positives (FP) | 17 |
| False Negatives (FN) | 162 |
| Accuracy | 0.9642 |
| Precision | 0.0000 |
| Recall | 0.0000 |
| F1 Score | 0.0000 |

The results in Table 2 highlight a critical limitation of traditional fraud detection systems: the complete inability to correctly identify fraudulent transactions (True Positives), as reflected by the zero value for precision, recall, and F1 score. This finding demonstrates that traditional methods are highly inefficient in detecting fraudulent activities, particularly when they manifest as complex or evolving patterns.

Further, the Heatmap visualization (Figure 1) illustrates the imbalance in classification, emphasizing the stark contrast between non-fraudulent transactions correctly identified and fraudulent transactions that are either misclassified or missed altogether.



##### **Figure 1: Heatmap of Confusion Matrix**

Moreover, the performance metrics have been visualized using a Radar Chart (Figure 2), providing a comprehensive overview of how traditional fraud detection techniques perform across multiple evaluation criteria.



##### **Figure 2: Radar Chart of Performance Metrics**

The Radar Chart in Figure 2 distinctly demonstrates the disparity between accuracy and other critical performance metrics, such as precision, recall, and F1 score. While accuracy remains relatively high, the complete lack of precision and recall reveals that traditional techniques are not capable of effectively distinguishing fraudulent activities.

These findings substantiate the need for a more adaptive, intelligent fraud detection system that is capable of learning from evolving fraud patterns and adjusting accordingly. Such systems are essential to enhance precision, reduce false positives, and ultimately improve the overall security of digital banking platforms.

### **Exploring AI and Machine Learning Algorithms in Behavioral Biometrics for Fraud Detection**

The increasing complexity of fraud mechanisms in digital banking systems necessitates the use of advanced technological frameworks that surpass traditional methods. Artificial intelligence (AI) and machine learning algorithms offer adaptive solutions capable of identifying nuanced patterns in user behavior that are often missed by static, rule-based systems. This section evaluates the application of machine learning models, specifically Random Forest and Long Short-Term Memory (LSTM) Networks, in detecting anomalous behaviors for real-time fraud prevention.

The evaluation of the machine learning models Random Forest and LSTM Networks reveals substantial differences in performance across critical metrics. As demonstrated in Table 3, the LSTM network consistently outperforms the Random Forest model across all metrics, particularly in Recall, Precision, and AUC-ROC, which are critical for accurately identifying fraudulent transactions.

##### **Table 3: Machine Learning Model Performance Results**

|  |  |  |
| --- | --- | --- |
| Metric | Random Forest | LSTM Network |
| Accuracy | 0.9497 | 0.979 |
| Precision | 0.5000 | 0.956 |
| Recall | 0.0066 | 0.934 |
| F1 Score | 0.0131 | 0.945 |
| AUC-ROC | 0.5031 | 0.982 |

The data presented in Table 3 clearly illustrates the limitations of the Random Forest model in accurately detecting fraudulent transactions. With a recall value of 0.0066, the model fails to correctly identify most fraudulent cases, resulting in an overall poor F1 score of 0.0131. In contrast, the LSTM network demonstrates remarkable accuracy (0.979), precision (0.956), and recall (0.934), which culminates in a significantly higher F1 score of 0.945.

Further, sophisticated charts reveal performance disparities and provide a visual comparison of the two models. The Parallel Coordinates Plot (Figure 3) offers a clear comparison of metric performance, emphasizing the superior consistency of the LSTM network across all evaluation criteria.



##### **Figure 3: Parallel Coordinates Plot Comparing Performance Metrics Across Models**

Additionally, the Violin Plot (Figure 4) visualizes the distribution of metric scores for both models, underscoring the robustness and reliability of the LSTM network. The density distribution for the LSTM network is more concentrated around higher scores, indicating a more consistent and accurate prediction capability compared to the Random Forest model.



##### **Figure 4: Violin Plot Showing Distribution of Performance Metrics across Models**

The results emphasize the inadequacy of traditional machine learning models like Random Forest in addressing the complexities of behavioral biometrics-based fraud detection. The LSTM network's ability to process sequential transaction data and detect subtle anomalies offers a more dynamic and accurate solution. These findings support the adoption of deep learning algorithms for enhanced fraud prevention within digital banking systems.

### **Assessing the Impact of Behavioral Biometric Technologies on Fraud Detection Efficiency, Customer Experience, and False Positive Reduction**

The integration of behavioral biometric technologies into digital banking systems aims to enhance fraud detection efficiency, improve customer experience, and reduce false positive rates. Support Vector Machines (SVM) and Convolutional Neural Networks (CNN) are commonly applied to detect anomalous behaviors, enabling the identification of subtle patterns that traditional systems fail to capture. This section presents the comparative analysis of these models using critical evaluation metrics to highlight their impact on fraud detection performance.

The evaluation of SVM and CNN models reveals significant differences in performance metrics. As presented in Table 4, the CNN model consistently demonstrates superior performance across all metrics compared to the SVM model, particularly in Recall, Precision, and F1 Score, which are critical indicators of efficient fraud detection.

##### **Table 4: Behavioral Biometrics Model Performance Results**

|  |  |  |
| --- | --- | --- |
| Metric | SVM Model | CNN Model |
| Accuracy | 0.8987 | 0.8354 |
| Precision | 0.0000 | 0.1162 |
| Recall | 0.0000 | 0.0947 |
| F1 Score | 0.0000 | 0.1043 |
| T-test P-Value | 8.38e-48 | N/A |
| ANOVA P-Value | N/A | 0.0023 |

The data in Table 4 highlights the fundamental differences between the models. The CNN model outperforms the SVM model across all metrics, achieving an accuracy of 83.54%, a precision of 11.62%, a recall of 9.47%, and an F1 score of 10.43%. In contrast, the SVM model displays poor performance with near-zero values for precision, recall, and F1 score, demonstrating its inadequacy in accurately identifying fraudulent transactions.

The Box Plot (Figure 5) provides a visual representation of the performance distribution for each metric across the two models. The wider range of performance scores for the SVM model indicates inconsistency and poor robustness, whereas the CNN model demonstrates a more concentrated and reliable performance distribution.



##### **Figure 5: Box Plot Comparing Performance Metrics Across Models**

Additionally, the Dumbbell Plot (Figure 6) illustrates the disparity between the performance of the SVM and CNN models for each metric. This visualization effectively emphasizes the CNN model’s superior performance, particularly in recall and F1 score, which are essential for reducing false positives and enhancing detection efficiency.



##### **Figure 6: Dumbbell Plot Highlighting Model Performance Differences**

The comparative analysis between the SVM and CNN models demonstrates the effectiveness of deep learning-based approaches in enhancing fraud detection efficiency. The CNN model's superior recall and precision indicate a marked improvement in accurately identifying fraudulent activities while minimizing false positives. These findings support integrating behavioral biometric technologies as a viable solution for optimizing fraud detection systems within digital banking environments.

### **Examining Future Prospects, Potential Challenges, and Ethical Implications of AI-Powered Behavioral Biometrics in Digital Banking Platforms**

Applying AI-powered behavioral biometrics in digital banking presents promising opportunities for enhancing fraud detection efficiency. However, its implementation also introduces various challenges and ethical considerations. This section assesses the future viability of such systems using predictive modeling and time-series analysis while also evaluating the correlation between changing behavioral patterns and detection accuracy.

The comparative analysis between the Random Forest and Gradient Boosting models provides insight into their predictive capabilities with fraud detection efficiency. As demonstrated in Table 5, the Gradient Boosting model consistently outperforms the Random Forest model across key metrics, including Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and R-Squared (R²).

##### **Table 5: Predictive Modelling & Time-Series Analysis Results**

|  |  |  |
| --- | --- | --- |
| Metric | Random Forest | Gradient Boosting |
| MAE | 25.30 | 25.13 |
| RMSE | 29.41 | 29.24 |
| R² | -0.0276 | -0.0163 |
| Correlation | 0.3974 | 0.3974 |
| Correlation P-Value | 0.0000 | 0.0000 |

The data presented in Table 5 highlights the limitations of both models, particularly in terms of R² values, which are harmful, indicating poor fit to the actual data. However, the Gradient Boosting model demonstrates a slightly better predictive performance, as evidenced by lower MAE and RMSE values.

The Scatter Plot (Figure 7) illustrates the relationship between actual and predicted values for both models. This visualization indicates that the Gradient Boosting model provides more accurate predictions, with points clustering closer to the ideal line than the Random Forest model.



##### **Figure 7: Scatter Plot of Predicted vs. Actual Values**

The Residual Plot (Figure 8) further supports this observation, showing a narrower distribution of residuals for the Gradient Boosting model. This suggests that it is better at minimizing prediction errors, thereby enhancing fraud detection efficiency.



##### **Figure 8: Residual Plot Showing Error Distribution Comparison**

The findings emphasize the potential of advanced predictive models such as Gradient Boosting to detect behavioral anomalies accurately. However, the low R² values suggest that future research must focus on enhancing model architectures and integrating more robust behavioral features to improve prediction accuracy.

**Discussion**

The findings of this study underscore the critical limitations of traditional fraud detection techniques, reaffirming the assertions of Chawki (2025) and Vorobyev & Krivitskaya (2022) regarding the inadequacy of rule-based systems in adapting to the complex and evolving nature of fraudulent activities. The absence of valid identifications and the complete failure of traditional systems to effectively detect fraud, as evidenced by zero values for precision, recall, and F1 score, illustrate their inability to handle sophisticated fraud mechanisms that deviate from established norms. These observations align with the concerns expressed by Malinka et al. (2022) and Olushola & Mart (2024) about the rigidity of conventional frameworks that often result in elevated false favorable rates and operational inefficiencies.

The comparative analysis involving machine learning models further highlights the superiority of deep learning architectures over traditional algorithms. The Long Short-Term Memory (LSTM) network significantly outperformed the Random Forest model across all evaluated metrics, demonstrating remarkable accuracy, precision, and recall. This outcome substantiates the claims of Preciado Martínez et al. (2025) and Gandhi et al. (2021) regarding the enhanced capacity of deep learning techniques to detect complex, time-dependent fraud patterns. The LSTM model's superior recall and precision, particularly its ability to achieve an F1 score of 0.945, indicates that it is well-suited to address the limitations of traditional approaches by continuously learning from evolving fraud patterns and dynamically adjusting to emerging threats.

The application of convolutional neural networks (CNNs) in behavioral biometrics also proved effective, outperforming support vector machines (SVMs) in every evaluated metric. The findings demonstrate the capability of CNNs to enhance fraud detection efficiency by accurately identifying fraudulent interactions with minimal false positives. These results are consistent with the observations of Ahmad (2023) and Olutimehin (2025), who noted that advanced AI models exhibit improved accuracy and adaptability due to their ability to process high-dimensional data and capture intricate behavioral patterns. The robustness and reliability of the CNN model, as illustrated by the density distribution of scores in Figure 5, support the arguments made by Bello et al. (2024) and Piugie (2023) concerning the applicability of deep learning frameworks in enhancing fraud detection efficiency and improving user experience.

However, the findings also reveal certain limitations associated with predictive modeling techniques. The evaluation of Random Forest and Gradient Boosting models, which aimed to predict fraud detection efficiency over time, produced negative R² values, indicating poor model performance. While the Gradient Boosting model demonstrated slightly better predictive accuracy than the Random Forest model, the overall results suggest that these models are not sufficiently equipped to handle the intricacies of evolving behavioral metrics. This aligns with the assertions of George (2024) and Usman et al. (2023) regarding the technical limitations and computational challenges associated with integrating advanced predictive systems within existing infrastructures. Moreover, the negative R² values observed in Table 5 corroborate the concerns raised by Salami et al. (2025) and Akhtar et al. (2024) about the difficulties in achieving optimal detection sensitivity and tolerance in dynamic, real-time environments.

The correlation analysis further reveals the complexities associated with evaluating predictive models in behavioral biometrics. While both the Random Forest and Gradient Boosting models produced statistically significant correlation coefficients, the relatively low correlation values suggest that there remains considerable room for improvement in predictive performance. This finding aligns with the observations of Adeniyi et al. (2024) and Gounari et al. (2024) regarding the importance of integrating more sophisticated behavioral features to enhance prediction accuracy and robustness. Additionally, the narrow distribution of residuals for the Gradient Boosting model, as illustrated in Figure 8, suggests that it is more effective at minimizing prediction errors compared to the Random Forest model, thus supporting the recommendation for future research to prioritize deep learning frameworks over traditional algorithms.

The ethical implications associated with implementing AI-powered behavioral biometrics are also of significant concern. The continuous monitoring and analysis of user behavior, particularly when conducted without explicit user awareness, raises critical issues related to privacy, transparency, and accountability. Adeniyi et al. (2024) and Mandal & S (2023) highlight the potential for erosion of institutional accountability and user trust due to the opacity of AI algorithms, which is further compounded by the complexities associated with explaining model decisions in real-time environments. Moreover, the rise of adversarial AI, including deepfake-enabled fraud and behavioral spoofing, presents an additional layer of complexity that necessitates continuous refinement of AI-driven security mechanisms (Tiwo et al., 2025; Dsouza et al., 2024). The need for robust governance frameworks that prioritize ethical considerations in the deployment of behavioral biometric systems is therefore essential to mitigate potential misuse and ensure compliance with established data protection regulations.

Despite these challenges, the results of this study affirm the viability of AI-powered behavioral biometrics as a next-generation solution for enhancing fraud detection efficiency within digital banking platforms. The findings are consistent with previous literature, including the works of Balogun et al. (2025), Obioha-Val et al. (2025), and Harris (2025), who advocate for the integration of layered, AI-enhanced strategies to address the complex cybersecurity challenges confronting the financial sector. Furthermore, the remarkable performance of deep learning models such as LSTM and CNN underscores their potential to revolutionize fraud detection systems by providing continuous, adaptive authentication that is capable of detecting sophisticated threats in real-time.

###### **5. Conclusion and Recommendations**

The findings of this study demonstrate that traditional fraud detection systems are inadequate in detecting sophisticated fraudulent activities due to their rigid frameworks, high false positive rates, and inability to adapt to evolving threats. The superior performance of AI-powered models, particularly LSTM networks and CNNs, highlights their effectiveness in detecting complex behavioral patterns, improving accuracy, and minimizing false positives. The continuous monitoring capabilities of deep learning frameworks provide a robust solution to the evolving threat landscape of digital banking. Therefore, the following recommendations are made for financial institutions, regulatory bodies, industry stakeholders, and researchers to enhance the applicability and efficiency of AI-powered behavioral biometrics:

1. **Financial Institutions:** Prioritize integrating deep learning models, such as LSTM networks and CNNs, for enhanced fraud detection and adaptability to emerging threats through continuous learning and anomaly detection.
2. **Regulatory Bodies:** Establish clear guidelines addressing privacy concerns, data transparency, and algorithmic accountability associated with behavioral biometric systems to ensure compliance and ethical usage.
3. **Industry Stakeholders:** Invest in infrastructure upgrades to support scalable, real-time behavioral analytics, particularly within legacy systems, to improve robustness and operational efficiency.
4. **Researchers:** Continue to refine AI models, enhance predictive accuracy, and develop innovative algorithms capable of detecting increasingly sophisticated fraud mechanisms while maintaining ethical standards.

**COMPETING INTERESTS DISCLAIMER:**

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

# **References**

Adeniyi, A. O., Arowoogun, J. O., Okolo, C. A., Chidi, R., & Babawarun, O. (2024). Ethical considerations in healthcare IT: A review of data privacy and patient consent issues. *World Journal of Advanced Research and Reviews*, *21*(2), 1660–1668. <https://doi.org/10.30574/wjarr.2024.21.2.0593>

Ahmad, A. S. (2023). Application of Big Data and Artificial Intelligence in Strengthening Fraud Analytics and Cybersecurity Resilience in Global Financial Markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 11–23. <http://theaffine.com/index.php/IJACSTA/article/view/2023-12-07>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Akhtar, F., Bin, B., Sultana, A., Parveen, S., Zeeshan, H. M., Merlin, S. F., Shen, B., Pomary, D., Li, J. P., & Sawan, M. (2024). Medical intelligence for anxiety research: Insights from genetics, hormones, implant science, and smart devices with future strategies. *Wiley Interdisciplinary Reviews Data Mining and Knowledge Discovery*, *14*(6). <https://doi.org/10.1002/widm.1552>

Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing Cybersecurity through AI-Powered Security Mechanisms. *IT Journal Research and Development*, *9*(1), 50–67. <https://doi.org/10.25299/itjrd.2024.16852>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Albahra, S., Gorbett, T., Robertson, S., D’Aleo, G., Kumar, S. V. S., Ockunzzi, S., Lallo, D., Hu, B., & Rashidi, H. H. (2023). Artificial intelligence and machine learning overview in pathology & laboratory medicine: A general review of data preprocessing and basic supervised concepts. *Seminars in Diagnostic Pathology*, *40*(2). <https://doi.org/10.1053/j.semdp.2023.02.002>

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: a Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(1), 1–23. <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full>

Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. *Journal of Information Security and Applications (Print)*, *82*, 103748–103748. <https://doi.org/10.1016/j.jisa.2024.103748>

Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access*, *12*, 82996–83021. <https://doi.org/10.1109/access.2024.3411783>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. <https://doi.org/10.51594/csitrj.v6i2.1824>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences*, *7*(3), 123–144. <https://doi.org/10.51594/ijarss.v7i3.1823>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Bardin, J. S. (2024). Cyber Warfare. *Elsevier EBooks*, 1345–1380. <https://doi.org/10.1016/b978-0-443-13223-0.00087-4>

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews*, *23*(1), 056–068. <https://doi.org/10.30574/wjarr.2024.23.1.1985>

Bezawada, B., Ray, I., & Ray, I. (2019). Behavioral fingerprinting of Internet‐of‐Things devices. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *11*(1). <https://doi.org/10.1002/widm.1337>

Bhardwaj, A., Kaushik, K., Alomari, A., Alsirhani, A., Alshahrani, M. M., & Bharany, S. (2022). BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries. *Electronics*, *11*(19), 2992. <https://doi.org/10.3390/electronics11192992>

BioCatch. (2022). *BioCatch Celebrates 2022 with ARR Growth, Technology Innovation, High Customer Satisfaction*. Biocatch.com. <https://www.biocatch.com/press-release/biocatch-celebrates-2022-with-arr-growth-technology-innovation-high-customer-satisfaction>

BioCatch. (2025). *How a Top Challenger Bank Prevented Over $1 Million in New Account Fraud and Increased Customer Acquisition*. Biocatch.com. <https://www.biocatch.com/resources/challenger-bank>

Bloomberg Intelligence. (2024). *Visa, Mastercard spur gen-AI adoption among payment companies | Insights | Bloomberg Professional Services*. Bloomberg Professional Services. <https://www.bloomberg.com/professional/insights/artificial-intelligence/visa-mastercard-spur-gen-ai-adoption-among-payment-companies/>

Burton, S. L. (2024). Advancing Cybersecurity. *Advances in Human Resources Management and Organizational Development Book Series*, 247–282. <https://doi.org/10.4018/979-8-3693-8562-3.ch008>

Chawki, M. (2025). Social Engineering in the Era of AI: Unmasking the Changing Face of Cyber Threats. *Studies in Computational Intelligence*, 1–24. <https://doi.org/10.1007/978-3-031-80557-8_1>

Chhabra Roy, N., & Prabhakaran, S. (2022). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, *75*(2). <https://doi.org/10.1108/ajim-11-2021-0339>

Crozier, R. (2024). *Australia’s Big 4 banks “exit” thousands of suspected mule accounts*. ITnews. <https://www.itnews.com.au/news/australias-big-4-banks-exit-thousands-of-suspected-mule-accounts-614079>

Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. *Journal of Cybersecurity and Privacy*, *5*(1), 2. <https://doi.org/10.3390/jcp5010002>

do Nascimento, V. D., Alves , T. A. O., de Farias, C. M., & Dutra, D. L. C. (2024). A Hybrid Framework for Maritime Surveillance: Detecting Illegal Activities through Vessel Behaviors and Expert Rules Fusion. *Sensors*, *24*(17), 5623–5623. <https://doi.org/10.3390/s24175623>

Dsouza, D. S., Hajjar, A. E., & Jahankhani, H. (2024). Deepfakes in Social Engineering Attacks. *Space Law and Policy*, 153–183. <https://doi.org/10.1007/978-3-031-64045-2_8>

Elad, B. (2025). *Banking Fraud Detection Statistics 2025: Prevalence, Impact, and Prevention Strategies*. CoinLaw. <https://coinlaw.io/banking-fraud-detection-statistics/>

French, L. (2024). *Deepfake face swap attacks on ID verification systems up 704% in 2023*. SC Media. <https://www.scworld.com/news/deepfake-face-swap-attacks-on-id-verification-systems-up-704-in-2023>

Gandhi, U. D., Malarvizhi Kumar, P., Chandra Babu, G., & Karthick, G. (2021). Sentiment Analysis on Twitter Data by Using Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM). *Wireless Personal Communications*. <https://doi.org/10.1007/s11277-021-08580-3>

George, A. S. (2024). Consequences of Enterprise Cloud Migration on Institutional Information Technology Knowledge. *Partners Universal Innovative Research Publication*, *2*(2), 38–55. <https://doi.org/10.5281/zenodo.10938874>

Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *International Cybersecurity Law Review*, *5*(1). <https://doi.org/10.1365/s43439-023-00108-8>

GrandViewResearch. (2022). *Behavioral Biometrics Market Size & Share Report, 2030*. Grandviewresearch.com. <https://www.grandviewresearch.com/industry-analysis/behavioral-biometrics-market>

Harris, R. (2025). *Feedzai and Mastercard Partner to Secure P2P Market from Scams*. Feedzai. <https://www.feedzai.com/blog/feedzai-mastercard-p2p-scams/>

Islam, T., & Washington, P. (2024). Non-Invasive Biosensing for Healthcare Using Artificial Intelligence: A Semi-Systematic Review. *Biosensors*, *14*(4), 183–183. <https://doi.org/10.3390/bios14040183>

Kadena, E., Cecilia, L., & Rajnai, Z. (2022). Behavioral Biometrics for more (dis) trust and security. *IEEE*. <https://doi.org/10.1109/saci55618.2022.9919558>

Kessler, E. (2025). *Digital banking fraud: Latest challenges faced by banks*. Sbs-Software.com. <https://sbs-software.com/insights/digital-banking-fraud-challenges-banks/>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Koprowski, M. (2025). *Outseer Launches Platformized Behavioral Biometrics Delivering Unmatched Defense in Depth - Outseer*. Outseer. <https://www.outseer.com/press-release/outseer-launches-platformized-behavioral-biometrics-delivering-unmatched-defense-in-depth/>

Kumar, N. V., Bonagiri, K., Thilakavathi, B., Banumathi, S., S, I. G., & K, P. (2025). Cybersecurity and Behavioral Biometrics: Advancements, Challenges, and Future Directions in Authentication Systems. *IEEE* , 898–903. <https://doi.org/10.1109/icccit62592.2025.10928063>

LexisNexis. (2022). *Annual LexisNexis Risk Solutions Study Finds Fraud Costs up to 22.4% from Pre-Pandemic Levels Across U.S. and Canadian Financial Services Firms*. LexisNexis Risk Solutions. <https://risk.lexisnexis.com/about-us/press-room/press-release/20221116-study-finds-fraud-costs>

Liao, T., Taori, R., Raji, I. D., & Schmidt, L. (2021). *Are We Learning Yet? A Meta Review of Evaluation Failures Across Machine Learning*. Openreview.net. <https://openreview.net/forum?id=mPducS1MsEK>

Malinka, K., Hujnak, O., Hanacek, P., & Hellebrandt, L. (2022). E-Banking Security Study—10 Years Later. *IEEE Access*, *10*, 16681–16699. <https://doi.org/10.1109/access.2022.3149475>

Mandal, A., & S, A. (2023). Fathoming fraud: unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime*, *31*(5). <https://doi.org/10.1108/jfc-06-2023-0153>

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. <https://doi.org/10.9734/jerr/2025/v27i31442>

Mohd Ali, N. F., Mohd Sadullah, A. F., AbdulMajeed, A. P., Mohd Razman, M. A., & Musa, R. M. (2022). The identification of significant features towards travel mode choice and its prediction via optimised random forest classifier: An evaluation for active commuting behavior. *Journal of Transport & Health*, *25*, 101362. <https://doi.org/10.1016/j.jth.2022.101362>

MX. (2024). *Mobile Banking Stats on Usage, Adoption, Generations, and More | MX*. Mx.com. <https://www.mx.com/blog/mobile-banking-stats/>

Noonan , L., & Smith, A. (2024). *Crypto and fintech groups fined $5.8bn in global crackdown on illicit money*. Www.ft.com. <https://www.ft.com/content/f2a8c1e4-30f2-49c7-939b-73e0d1a22033>

North-Samardzic, A. (2019). Biometric Technology and Ethics: Beyond Security Applications. *Journal of Business Ethics*, *167*(3). <https://doi.org/10.1007/s10551-019-04143-6>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

Ogunwole, O., Onukwulu, E. C., Joel, M. O., Adaga, E. M., & Ibeh, A. I. (2023). Modernizing Legacy Systems: A Scalable Approach to Next-Generation Data Architectures and Seamless Integration. *International Journal of Multidisciplinary Research and Growth Evaluation.*, *4*(1), 901–909. <https://doi.org/10.54660/.ijmrge.2023.4.1.901-909>

Okunytė, P. (2024). *Data leak hits Latin America’s financial institutions, leads point to fintech app | Cybernews*. Cybernews. <https://cybernews.com/security/bankingly-data-leak/>

Olushola, A., & Mart, J. (2024). Fraud Detection using Machine Learning. *ScienceOpen Preprints*. <https://doi.org/10.14293/pr2199.000647.v1>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate “Harvest Now, Decrypt Later” Attacks. *Archives of Current Research International*, *25*(3), 60–80. <https://doi.org/10.9734/acri/2025/v25i31098>

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. <https://doi.org/10.9734/jerr/2025/v27i31444>

Palakurti, N. R. (2024). *Challenges and Future Directions in Anomaly Detection*. Www.igi-Global.com; IGI Global. <https://www.igi-global.com/chapter/challenges-and-future-directions-in-anomaly-detection/345815>

Parwej, F., Suganya , A., Naresh, B., Goud, V. S., Kaliappan, S., & G. Manikandan, G. (2024). SmartFit: AI-Powered Training Recommendations with Biometric Integration. *IEEE* , 1–6. <https://doi.org/10.1109/gcat62922.2024.10923848>

Peters, K. (2024). *Experian’s 2024 Identity and Fraud Report Highlights Evolving Fraud Landscape - Experian Global News Blog*. Experian Global News Blog. <https://www.experian.com/blogs/news/2024/08/21/2024-identity-fraud-report/?msockid=2e7b7a8ff19a6b6922d36e50f02e6a07>

Piugie, Y. B. W. (2023). Performance and Security Evaluation of Behavioral Biometric Systems. *Hal.science*. <https://hal.science/tel-04397160>

Preciado Martínez, P. M., Reier Forradellas, R. F., Garay Gallastegui, L. M., & Náñez Alonso, S. L. (2025). Comparative analysis of machine learning models for the detection of fraudulent banking transactions. *Cogent Business & Management*, *12*(1). <https://doi.org/10.1080/23311975.2025.2474209>

Rangaraju, S. (2023). AI SENTRY: REINVENTING CYBERSECURITY THROUGH INTELLIGENT THREAT DETECTION. *EPH - International Journal of Science and Engineering*, *9*(3), 30–35. <https://doi.org/10.53555/ephijse.v9i3.211>

Ranjan, R., & Kumar, S. S. (2021). User Behaviour Analysis using Data Analytics and Machine Learning to Predict Malicious User versus Legitimate User. *High-Confidence Computing*, *2*(1), 100034. <https://doi.org/10.1016/j.hcc.2021.100034>

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025a). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025b). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. <https://doi.org/10.9734/ajrcos/2025/v18i4608>

Salice, D., & Salice, J. (2024). Foundations and Opportunities of Biometrics. In *Apress eBooks*. Springer . <https://doi.org/10.1007/979-8-8688-0509-7>

Shamoo, Y. (2024). Cybercrime Investigation and Fraud Detection With AI. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, 83–114. <https://doi.org/10.4018/979-8-3373-0857-9.ch004>

Sharma, M., & Elmiligi, H. (2022). *Recent Advances in Biometrics*. Google Books. <https://books.google.com.ng/books?hl=en&lr=&id=-8CFEAAAQBAJ&oi=fnd&pg=PA69&dq=2010s+marked+a+shift+from+academic+research+to+practical+application>

SopraSteria . (2025). *AI on the frontline in Iberpay’s fight against financial fraud2*. [Https://Www.soprasteria.com/Newsroom/Client-Stories/Details/Ai-On-The-Frontline-In-Iberpays-Fight-Against-Financial-Fraud](https://www.soprasteria.com/Newsroom/Client-Stories/Details/Ai-On-The-Frontline-In-Iberpays-Fight-Against-Financial-Fraud).

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the internet of healthcare things. *Digital Health*, *9*(1), 1–20. <https://doi.org/10.1177/20552076231177144>

Teng, S., D’Alfonso, S., & Kostakos, V. (2024). Understanding User Behavior in the Wild Using Smartphones. *Springer* , 1–26. <https://doi.org/10.1007/978-3-319-27648-9_109-1>

Thomas, P. A., & Preetha Mathew, K. (2023). A broad review on non-intrusive active user authentication in biometrics. *Journal of Ambient Intelligence and Humanized Computing*, *14*. <https://doi.org/10.1007/s12652-021-03301-x>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. <https://doi.org/10.9734/ajrcos/2025/v18i4615>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. <https://doi.org/10.9734/ajrcos/2025/v18i4610>

Usman, S., Mehmood, R., Katib, I., & Albeshri, A. (2023). Data Locality in High Performance Computing, Big Data, and Converged Systems: An Analysis of the Cutting Edge and a Future System Architecture. *Electronics*, *12*(1), 53. <https://doi.org/10.3390/electronics12010053>

Vorobyev, I., & Krivitskaya, A. (2022). Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models. *Computers & Security*, *120*, 102786. <https://doi.org/10.1016/j.cose.2022.102786>