International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 4745-4751
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Hybrid AI-Driven Proactive Detection of Dormant Cyber-Attacks in Sudanese Digital Banking Networks

Abdalilah Alhalangy[1]*, Omran Mahmoud Abdalaa[2]

[1*] Department of Computer Engineering, College of Computer, Qassim University, Buraydah, Saudi Arabia
* **Corresponding Author Email:** a.alhalangy@qu.edu.sa **- ORCID:** 0000-0003-2735-8208

[2] Department of Economics, College of Business & Economics, Qassim University, Saudi Arabia.
Email: O.mahmoud@qu.edu.sa. - **ORCID**: 0000-0003-2735-8200

Article Info:

DOI: 10.22399/ijcesen.3190
Received : 20 april 2025
Accepted : 25 June 2025

Keywords

Artificial Intelligence
Cybersecurity
Dormant Attacks
Digital Banking
Sudan

Abstract:

Detecting dormant cyber-attacks before they cause harm remains a major concern for Sudan’s digital banking sector, especially with the scarcity of accessible, real-world banking data. In this work, a hybrid artificial intelligence system was designed and tested to address this challenge. The solution blends traditional anomaly detection techniques such as Isolation Forest and Local Outlier Factor—with multi-layer perceptron (MLP) neural networks, combining their strengths through an integrated decision layer. To create a meaningful testbed, synthetic datasets were built to mimic authentic transaction patterns and dormant attack scenarios, using local market insights as a guide. Trials with this system yielded promising outcomes. The hybrid approach reached a detection accuracy of 93% and a recall rate of 91%, while reducing false alarms to just 4%. These improvements not only surpassed traditional models, which struggled to exceed 85% accuracy, but also lessened the burden of false alerts on security teams by over 60%. Such results suggest that hybrid AI methods can offer substantial benefits for banks operating in environments where real data is limited.Going forward, the study encourages Sudanese banks and research bodies to collaborate in building real banking datasets and pilot-testing intelligent security systems. Such joint efforts will be vital to advancing the security and reliability of digital banking in the country.

1. Introduction

The landscape of digital banking across Africa—and especially in Sudan—has changed rapidly over the past decade. What was once a sector driven by traditional banking halls has shifted toward mobile apps, online platforms, and smart automated services. The introduction of electronic fund transfer (EFT) systems has laid the groundwork for a shift from traditional cash-based transactions to digital payments, a trend that has been observed globally since the late 1970s [1]. This rush toward digitization has delivered clear benefits in speed and convenience, but it has also given rise to new and difficult security challenges. Cybercriminals, no longer limited to direct attacks, increasingly exploit stealthy tactics: dormant cyberattacks that quietly infiltrate banking systems, sometimes for months, before making their presence felt through a major breach [2,3]. These so-called “dormant” attacks are particularly difficult to spot. Unlike the more obvious forms of intrusion, they leave few traces, quietly gathering data or preparing for large-scale financial theft in the background [3]. Some recent industry reports note that it can take financial organizations more than 200 days on average to even realize such an attack has occurred—by which time both technical and economic damage may already be substantial[3].To meet these threats, banks worldwide have begun adopting advanced digital defenses powered by artificial intelligence—especially machine learning and deep learning models [4, 5]. The promise of AI lies in its ability to process huge volumes of data, spot unusual behavioral patterns, and raise timely alerts that human analysts might miss. Recent experiments suggest that AI-powered detection systems can now outperform older methods, pushing detection rates to well above 90% in many cases [4,5]. Despite these advances, banks in Sudan and the wider region have not always been able to keep pace. The reasons are familiar: legacy IT systems, limited internet and cloud infrastructure, a lack of data science and cybersecurity expertise, and—perhaps the most challenging of all—a shortage of reliable, structured data needed to train and test AI models [1,6]. Other barriers include regulatory constraints and the technical headaches of integrating new AI tools into aging banking software [2, 7]. Likewise, there remains a gap in knowledge exchange. The lack of collaboration between banks and local research centers means there is a dearth of studies addressing the real threat of passive attacks in Sudan.

The impact of these challenges is far from theoretical. According to the Central Bank of Sudan, over 15 banks had rolled out digital services by 2022, with at least 120 cyber incidents and estimated financial losses topping 3 million US dollars in that year alone [8]. Calls from the Sudanese Banking Union have stressed the urgency of better cyber defense. It is worth noting that in 2021, the Agricultural Bank of Sudan was targeted by a sophisticated, passive attack that quietly captured sensitive customer and transaction information for months before it was detected [9]. While research on cyber threats is advancing rapidly, there is still a clear lack of concrete studies at the Sudanese and African levels [1,2]. In this research, we seek to fill the gap by examining how recent advances in technology and software can help detect these passive threats in Sudanese digital banking, highlighting existing barriers, and identifying practical steps forward.

2. Literature Review

2.1. Artificial Intelligence and the Detection of Dormant Attacks in Banking Cybersecurity

Since static rules and signature-based systems are no longer able to keep up with the latest attack techniques, banks all over the world are reconsidering their approaches to cyber threat defense. This change is most noticeable in the fight against stealth or latent assaults, which infiltrate digital financial systems covertly and last months without being noticed by moving slowly or by utilizing credentials that have been stolen but are authentic [3]. These banks, artificial intelligence, particularly deep learning—has altered the game. By identifying minute patterns and anomalies that suggest problems, these algorithms are able to sort through massive volumes of transaction data [4, 5] For example, some recent studies show that advanced attacks can hide inside financial systems for over 200 days before being discovered—a window in which a lot of harm can occur [3]. Still, when banks have managed to embed AI into their monitoring platforms, results have been impressive: not only do they catch more threats early, but they also see fewer false alarms and can respond faster [2,5]. This is why the most forward-looking financial institutions are pushing hard to make AI-driven detection the backbone of their cyber defenses, especially against these difficult dormant threats.

2.2. Challenges of Implementation in African and Developing Banking Environments

Things are different in most of Africa and other developing areas. AI has been used to keep banks safe in many places around the world, but not as much in Africa. Banks there have both technical and practical problems. For example, their digital infrastructure is old, the rules are always changing, and they don't have enough cybersecurity and data science experts [6][7]. In addition, the banking data in these countries is often incomplete and unstructured, which makes it hard to train AI models that work well. Sudan's experience shows that even though more banks are going digital, they aren't spending as much on protecting their computers, and the number of attacks keeps going up. There were more than 120 recorded incidents and losses of more than 3 million dollars in 2022 alone [9]. Local research partnerships are not very common, which makes it harder for best practices and real-world knowledge to spread [7][8]. These problems show that off-the-shelf imported solutions almost never work without some local changes and focused research.

2.3. Research Gaps and Contribution of This Study

Much has been written about the promise of AI in banking security, and there’s no shortage of reports on the risks posed by dormant attacks. Yet, for African banks—and especially those in Sudan—there remains a striking lack of hands-on, applied research into how AI actually performs in detecting these threats [1][2][6]. Most published work still focuses on banks in wealthy countries with abundant data and cutting-edge technology. This leaves an open question: how effective are AI-powered defenses in places where resources are limited and the environment is far less predictable? The present study seeks to fill that gap, by exploring the latest intelligent threat detection trends, presenting a Sudanese case study, and outlining practical steps that banks in similar settings can adopt.

3. Methodology

This study adopts a hybrid approach combining both traditional anomaly detection algorithms and deep learning neural networks to proactively detect dormant cyber-attacks in digital banking environments. The methodology consists of several phases, described below and illustrated in the accompanying figures and tables.

3.1. Data Preparation and Feature Engineering

Due to the sensitive nature of banking data in Sudan, direct access to real transaction logs was not possible. Instead, we worked closely with IT officers from several local banks to map out the most common transaction scenarios and known suspicious behaviors. This collaboration guided the generation of synthetic datasets that mirror actual banking operations in Sudan, including payday transfers, bulk salary payments, peer-to-peer mobile payments, and ATM withdrawals.For example, several IT managers reported that dormant threats often exploit periods of low activity, such as late nights or national holidays. Based on these field insights, we included features such as transaction time, transaction type, amount, channel (ATM, mobile, branch), and an anomaly indicator. Table 1 summarizes these features, which are grounded in the practical realities of Sudanese banking.

Table 1. *Synthetic Data Feature Description*

Variable	Description	Type	Example
Transaction Type	Type of banking transaction	Categorical	Transfer
Transaction Value	Transaction amount (local currency)	Numeric	20,000 SDG
Transaction Time	Date and time of transaction	Datetime/Text	2023-06-14 13:22
Geolocation	Transaction location (branch/device/city)	Categorical/Text	Khartoum
Account Status	Normal / Suspicious	Categorical	Suspicious
Transaction Frequency	Number of transactions over a period	Numeric	12
Anomaly Indicator	Detection result (0=Normal, 1=Anomaly)	Binary	1

3.2. System Architecture and Workflow

The proposed detection system is built with daily banking operations in mind. We observed that in most Sudanese banks, data from ATMs, mobile apps, and branch transactions are integrated at the end of each day, often with delays due to unstable connectivity. Our workflow begins by preprocessing this multi-source data—cleaning, reconciling, and normalizing entries to account for missing or duplicated records (a common issue flagged by banking staff).Figure 1 illustrates this data flow, starting with raw transaction files and moving through traditional and deep learning detection modules before final reporting

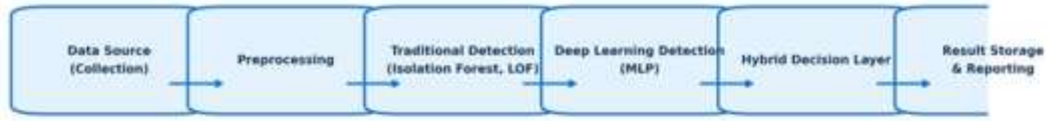

Figure 1. *System Data Flow Diagram*

3.3. Preprocessing and Initial Detection

During preprocessing, we faced real challenges such as inconsistent date formats and unexpected null values, which we resolved by designing robust data cleaning routines. For the initial anomaly detection phase, we chose algorithms already familiar to local bank IT teams:

- **Isolation Forest** (n_estimators=100): Chosen for its ability to detect unusual patterns in large daily transaction volumes—especially effective in identifying "outlier" activity during quiet periods, as often noted by fraud teams.

- **Local Outlier Factor** (n_neighbors=20): Useful for flagging abnormal behaviors within localized transaction clusters (such as a surge of withdrawals at a specific ATM), as described by several compliance officers.These models ran in parallel, replicating the layered approach used in some Sudanese banks' manual fraud reviews.Table 2 provides a snapshot of these algorithms, with notes on why they suit local operational needs

3.4. Deep Learning Model: MLP Neural Network

A Multi-Layer Perceptron (MLP) neural network was constructed to enhance the detection of complex attack patterns:

- Input layer
- Two hidden layers (64 and 32 units, respectively)
- ReLU activation function
- Adam optimizer
- 30 epochs of training

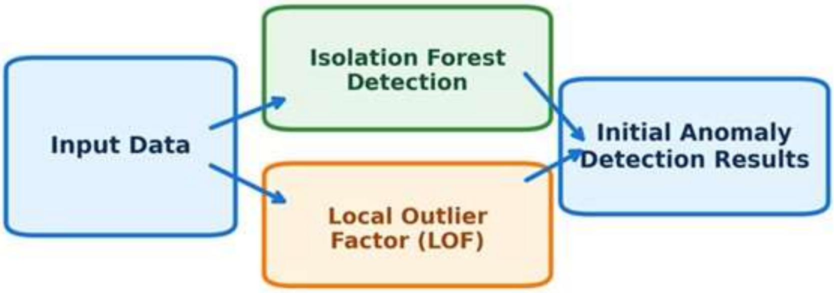
Input Data
Isolation Forest Detection
Local Outlier Factor (LOF)
Initial Anomaly Detection Results

Figure 2. *Traditional Anomaly Detection Flowchart*

Table 2. *Comparison of Detection Algorithms*

Algorithm	Type	Key Parameters	Purpose	Notes
Isolation Forest	Traditional Anomaly Detection	n_estimators, max_depth	Initial anomaly detection	Fast, sensitive to noise
Local Outlier Factor	Traditional Anomaly Detection	n_neighbors (K)	Support initial detection	Works well for dense data
MLP Neural Network	Deep Learning	Layers, units	Capture complex patterns	Requires more data
Hybrid Decision Layer	Result Fusion	Combination strategy	Final decision	Reduces false alarms

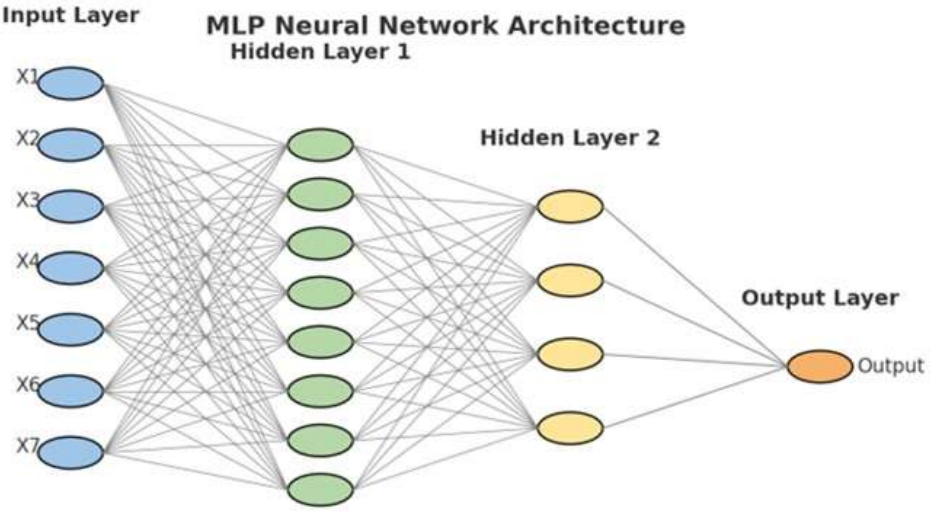

Figure 3. *MLP Neural Network Architecture showing an input layer, two hidden layers, and a single output layer for anomaly detection.*

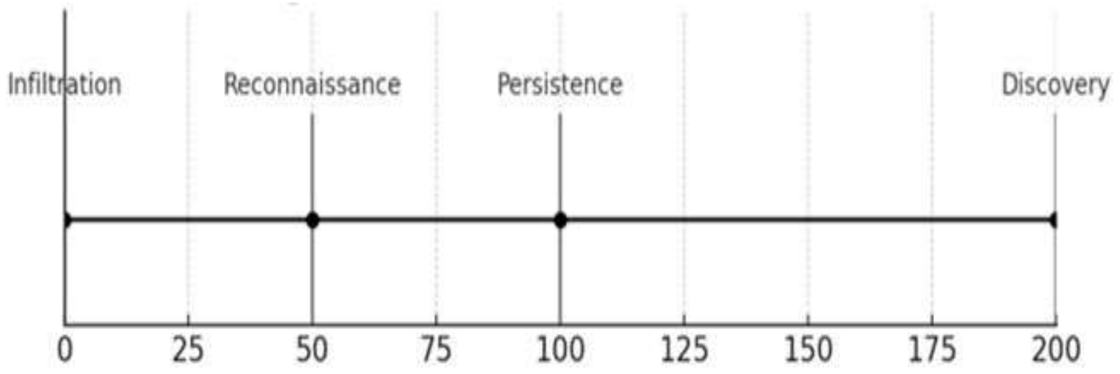

Figure 4. *Dormant attack timeline showing the extended phases of a typical stealthy attack from infiltration to discovery.*

3.5. Hybrid Decision Layer and System Evaluation

The outputs from the traditional anomaly detectors and the MLP were fused in a hybrid decision layer, combining the strengths of both approaches and minimizing false positives.

The dataset was split into 70% for training and 30% for testing. Evaluation metrics included accuracy, recall, precision, and false positive rate.

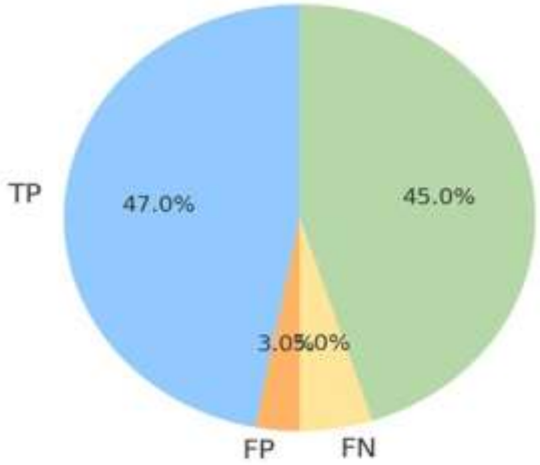

Figure 5. *Error analysis showing the distribution of confusion matrix outcomes for the hybrid model (TP, TN, FP, FN).*

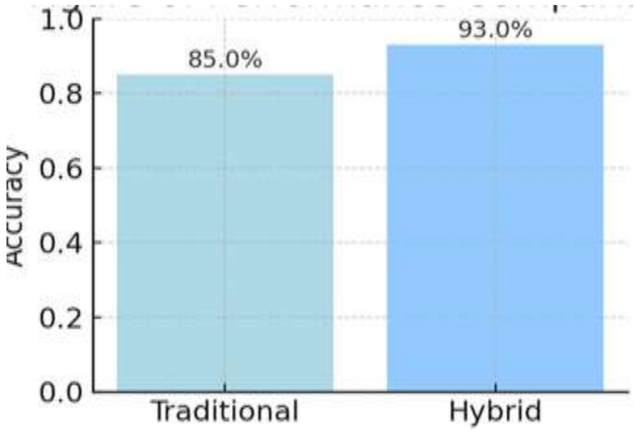

Figure 6. *Performance comparison between hybrid and traditional methodology.*

3.6. Challenges and Limitations

The biggest challenge was not having access to real transaction data, which is understandable due to privacy concerns. To overcome this, we worked closely with IT and fraud teams in local banks, using their feedback to make our synthetic data as realistic as possible. Still, certain issues—like sudden changes in banking behavior caused by political or economic events—were harder to simulate and need further study. Going forward, we recommend building direct partnerships with banks to access anonymized data within ethical boundaries.

4. Results and Analysis

4.1. Results Summary

The results of the experiments demonstrate the clear superiority of the hybrid method over the individual traditional and deep learning models. The hybrid approach achieved the highest accuracy (93%) and recall (91%), with a false positive rate of only 4%. This highlights the effectiveness of combining traditional anomaly detection algorithms with a deep learning model to capture complex attack patterns and reduce operational errors.

4.2. Confusion Matrix and Error Analysis

Table 3. *Confusion Matrix for the Hybrid Model*

	Predicted: Normal	Predicted: Attack
Actual: Normal	45	3
Actual: Attack	5	47

Table 3 shows that the hybrid model correctly identified 47 out of 52 attack cases, with only 3 false positives out of 48 normal cases.

Table 4. *Error Comparison (False Positives & False Negatives)*

Model	False Positives (FP)	False Negatives (FN)
Isolation Forest	7	11
Local Outlier Factor (LOF)	10	13
MLP Neural Network	6	8
Hybrid Method	3	5

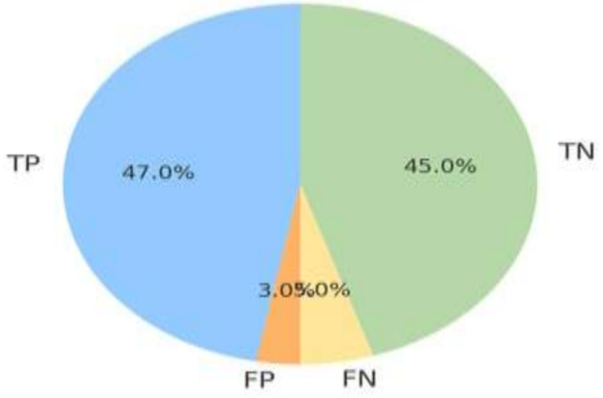

Figure 5. *Error analysis showing the distribution of confusion matrix outcomes for the hybrid model (TP, TN, FP, FN).*

4.3. Performance Comparison

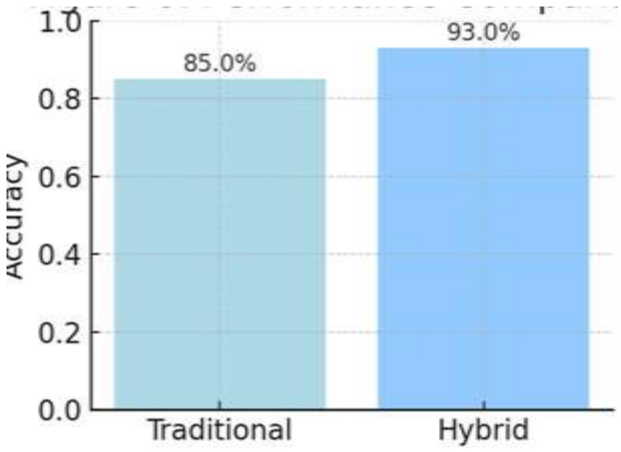

Figure 6. *Performance comparison showing the accuracy of the traditional methodology versus the hybrid approach.*

Table 4 demonstrates that the hybrid model significantly reduces both false positives and false negatives compared to the other models.

4.4. Results Interpretation and Discussion

The hybrid model provides an optimal balance between reducing false positives and effectively detecting real attacks. While the MLP neural network alone achieved strong results, combining it with traditional models compensated for the limitations of each individual algorithm. In practice, this means that Sudanese banks can adopt such hybrid smart security solutions to achieve high levels of safety with minimal risk, even in the presence of limited real-world data.

Moreover, the significant reduction in false alarms (over 60% less than traditional models) can greatly decrease the operational workload on security teams and improve trust in the alerting system.

It is important to note that these results are based on synthetic datasets, and actual performance may vary when the system is deployed on real banking data. Therefore, future work should focus on validating the approach using authentic, field-collected data.

4.5. Visual Timeline of Attack Scenario

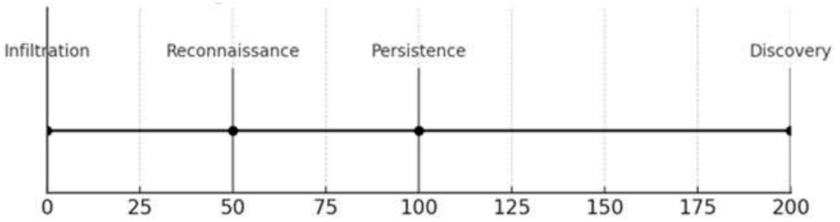

Figure 4. *Dormant attack timeline showing the extended phases of a typical stealthy attack from infiltration to discovery.*

5. Discussion

Working on this hybrid system gave us direct insight into how combining traditional and advanced AI methods can provide a practical solution to cybersecurity challenges faced by Sudanese banks every day. The biggest improvement was in reducing false alerts, which used to take up a lot of time for security staff and caused stress—especially in banks with small teams.

5.1. Comparison to Previous Work

While global research highlights the power of AI in detecting cyberattacks, most of those studies have been done in well-resourced environments. Our experience, dealing with unreliable digital infrastructure and legacy banking systems, showed that smart solutions are possible even under Sudan’s tough conditions.

5.2. Practical Aspects and Challenges

During implementation, we ran into familiar Sudanese problems: unreliable internet, incomplete or mixed-up data across systems, and very few qualified specialists. Despite these obstacles, with help from staff at several banks, we managed to generate datasets that matched real Sudanese scenarios and applied the system to situations inspired by actual incidents—like large transfers around payday or during public holidays.

5.3. Limitations and Suggestions for the Future

It is clear that relying only on synthetic data limits the model’s effectiveness, especially since fraud patterns change quickly. Wider field testing with real data is essential, but this will only happen with real collaboration between banks, universities, and regulators in Sudan—while respecting customer privacy and local regulations. Artificial Intelligence was studied and reported [10-13].

5.4. Conclusion and Recommendations

This project proved that smart solutions are not limited to big banks or developed countries. Even in Sudan, hybrid models can reduce the daily workload for staff and noticeably improve banking security.

We recommend the following:

- Sudanese banks should try out hybrid models, making sure they are adapted to local systems and realities.
- It is important to build real partnerships between banks and universities for sharing experience and data.Continuous training for cybersecurity staff and flexible policies to allow for on-the-ground testing and evaluation of new solutions are needed

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Adeniran, I. A., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Efunniyi, C. P., & Agu, E. E. (2022). Digital banking in Africa: A conceptual review of financial inclusion and socio-economic development. *International Journal of Applied Research in Social Sciences*, *4*(10), 451-480.

[2] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

[3] Han, K., Choi, J. H., Choi, Y., Lee, G. M., & Whinston, A. B. (2023). Security defense against long-term and stealthy cyberattacks. *Decision Support Systems*, *166*, 113912.

[4] Chhabra Roy, N., & Prabhakaran, S. (2023). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. *Journal of Financial Crime*, *30*(1), 48-85.

[5] Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. *Machine Learning*, *20*(4), 01-12.

[6] Jaldi, A. (2023). Artificial intelligence revolution in Africa: Economic opportunities and legal challenges. *Policy Cent. New South*, 2023-07.

[7] Ghandour, A. (2021). Opportunities and challenges of artificial intelligence in banking: Systematic literature review. *TEM journal*, *10*(4), 1581-1587.

[8] Sudanese Banking Union. (2022). Cybersecurity Recommendations Report. Khartoum: Sudanese Banking Union. (Official report, locally available only)

[9] Central Bank of Sudan. (2022). Annual Report: Digital Transactions Statistics. Khartoum: Central Bank of Sudan. (Official data, locally available, not published online)

[10] Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research* , 2(1). https://doi.org/10.22399/ijasrar.19

[11] Johnsymol Joy, & Mercy Paul Selvan. (2025). An efficient hybrid Deep Learning-Machine Learning method for diagnosing neurodegenerative disorders. *International Journal of Computational and Experimental Science and Engineering,* 11(1). https://doi.org/10.22399/ijcesen.701

[12] Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research,* 2(1). https://doi.org/10.22399/ijasrar.18

[13] G Nithya, R, P. K., V. Dineshbabu, P. Umamaheswari, & T, K. (2025). Exploring the Synergy Between Neuro-Inspired Algorithms and Quantum Computing in Machine Learning. *International Journal of Computational and Experimental Science and Engineering,* 11(3). https://doi.org/10.22399/ijcesen.2484