Delta Journal of Computing, Communications & Media Technologies (DJCCMT)
Journal platform–https://focjournals.dsust.edu.ng

Intelligent Adaptive and Dynamic Threshold (IADT): A Framework to Counter Evasive Cybercrime in Nigeria's Financial Services

Margaret Dumebi ***Okpor****
Department of Cyber Security, Southern Delta University, Ozoro, Nigeria.

Okpomo Eterigho ***Okpu***
Department of Cyber Security, Southern Delta University, Ozoro, Nigeria.

Henry Peter ***Ovili***
Department. of Information Systems and Technology, Southern Delta University, Ozoro Nigeria

Emuejevoke Francis ***Ogbimi***
Department. of Information Systems and Technology, Southern Delta University, Ozoro Nigeria

Osu Joshua ***Orove***
Department. of Information Systems and Technology, Southern Delta University, Ozoro Nigeria

Isaac Ighofewo ***Umukoro***
Department. of Software Engineering, Southern Delta University, Ozoro Nigeria

Endurance ***Adamugono***
Department. of Software Engineering, Southern Delta University, Ozoro Nigeria

Cyril Febau ***Benafa***
Department. of Information Systems and Technology, Southern Delta University, Ozoro Nigeria

Ebejale Kasimir ***Ikunobe***
Department. of Information Systems and Technology, Southern Delta University, Ozoro Nigeria

Amanda ***Okeke***
Department of Computer Science and Informatics, Federal University Otuoke, Nigeria.

David Ovie ***Okpor***
Department of Computer Science and Informatics, Federal University Otuoke, Nigeria.

ARTICLE INFO

Article history:
Received October 2024
Received in revised form Dec. 2024
Accepted December 2024
Available online Jan 2025

Keywords:
Financial Cybercrime
Evasive Maneuvers
Intelligent Adaptive Thresholds
Adaptive Security
Real-time Data Analysis.

ABSTRACT

Financial cybercrime presents a growing threat to the integrity of financial systems in Nigeria, where static threshold–based fraud detection struggles against adaptive attacks such as threshold arbitrage, velocity spikes, and low-and-slow maneuvers. Existing solutions lack real-time adaptability and contextual awareness of user behavior. This paper introduces the Intelligent Adaptive and Dynamic Threshold (IADT) framework, which leverages machine learning and real-time data analytics to generate evolving risk thresholds tailored to emerging threat patterns and individual usage profiles. Unlike predetermined static rules, IADT continuously refines its detection criteria through online learning, enabling timely mitigation of sophisticated evasive tactics. We reviewed the shortcomings of traditional static methods, then detail IADT's architecture—combining anomaly detection models,

feedback loops, and behavioral profiling—and present a UML conceptual design. By demonstrating how dynamic thresholds can outpace modern cyber-attack techniques, our framework offers a promising path toward more resilient fraud detection in Nigeria's financial sector.

Margaret D. Okpor

*Corresponding author.
E-mail address: okporm@dsust.edu.ng

https://doi.org/10.xxx.
DJCCMT112025017

1. Introduction

The rise of digital banking and online financial transactions has led to a significant increase in financial cybercrime, particularly targeting financial service providers in Nigeria. These institutions face an ongoing battle against cybercriminals who use various sophisticated techniques to steal money, compromise accounts, and disrupt financial operations. As cybercriminals continuously evolve their methods to bypass conventional security measures, Nigerian financial service providers find themselves in a constant struggle to protect their systems and customers. (Hassan, 2024). Traditional financial security measures often rely on static thresholds for detecting suspicious activity. These thresholds set fixed limits on specific parameters, such as transaction amounts, to trigger alerts for potential fraud. However, cybercriminals have developed rapidly evolving fraudulent practices (Ahmad, 2024) and evasive maneuvers, such as threshold arbitrage, velocity attacks, IP spoofing, distributed attacks and low-and-slow tactics, that render these static security measures increasingly ineffective. As a result, traditional methods for detecting anomalies fail to keep pace with the sophistication of modern cyber threats that adapt over time.

Despite multiple studies on fraud detection, there is a distinct lack of frameworks that combine adaptive machine learning with real-time dynamic thresholding to counter sophisticated evasive tactics in Nigeria's financial sector. While individual approaches exist separately, the integration of both adaptive and dynamic elements within a unified framework tailored to Nigeria's unique financial environment remains largely unexplored. This paper proposes a conceptual design of Intelligent Adaptive and Dynamic Thresholds (IADT) framework as a robust framework to address these challenges. IADT framework integrates machine learning and real-time data analytics to dynamically adapt to evolving threats, making it more difficult for criminals to evade detection. By continuously learning from and responding to new attack patterns, the framework enhances the detection and mitigation of financial cybercrime, thereby strengthening the resilience of Nigeria's financial service providers.

1.1 Motivation of the Study

The escalating threat of financial cybercrime in Nigeria's financial service providers demands innovative solutions. Static thresholds, currently employed to detect fraudulent activities, are inadequate due to their inability to adapt to the dynamic and intelligent nature of cybercriminal tactics. This limitation results in undetected fraudulent activities, which cause significant financial losses. This paper aims to conceptually design intelligent, adaptive and dynamic thresholds that can outsmart evasive maneuvers in financial cybercrime, providing a robust and effective defense for Nigeria's financial service providers.
This paper has the following key objectives:

a. To investigate the limitations of static threshold-based detection systems in combating financial cybercrime affecting Nigeria's financial service providers. ii.
b. To propose a framework for Intelligent Adaptive and Dynamic Thresholds (IADT) tailored to the specific needs of Nigeria's financial sector.

c. To conceptualize the effectiveness of the IADT framework in detecting and mitigating evasive maneuvers in financial cybercrime targeting Nigeria's financial institutions.
d. To discuss the potential challenges in implementing the IADT framework and outline future research directions to enhance its efficacy.

To achieve these objectives, the study addresses the following research questions:

a. What are the critical limitations of current static threshold-based detection systems in Nigeria's financial sector?
b. How can an intelligent, adaptive, and dynamic threshold framework be designed to effectively counter evasive maneuvers in financial cybercrime?
c. What key components and processes should be integrated into the IADT framework to enhance its effectiveness in Nigeria's financial context?
d. What challenges might arise in implementing the IADT framework, and how can these be addressed in future research?

2. Literature Review

2.1 Limitations of Static Thresholds in Financial Cybercrime Detection

In Nigerian financial systems, traditional security measures, such as static thresholds for transaction monitoring and predefined rules for fraud detection, have been commonly employed to safeguard transactions and prevent fraudulent activities. These thresholds are similar to those used globally but may also be tailored to the specific financial environment and regulatory landscape of Nigeria. These traditional security measures have proven insufficient against adaptive cyber threats (Bello et al., 2024a).
Static thresholds set a limit on a specific parameter to identify potentially fraudulent transactions (Abdullahi & Mansor, 2018). These thresholds are predefined limits set to identify unusual activities in financial transactions. These limits are often based on historical data and expert judgment (Gupta et al., 2023). While straightforward and easy to implement, static thresholds are rigid and cannot adapt to new types of cyber threats.

Nigerian financial systems have implemented various static thresholds to detect and prevent fraudulent activities, and these thresholds include the ones on daily transaction limits, alerts on large cash deposits, frequency of transactions, velocity checks, device and IP address monitoring, and login attempts. These thresholds aim to identify unusual patterns and suspicious transactions, such as large sums of money being transferred or deposited, rapid transactions, and multiple failed login attempts.
However, research highlights the limitations of static thresholds as cybercriminals can develop evasive maneuvers to bypass them (Shoetan & Familoni, 2024).
These limitations include:

a. Inflexibility - These thresholds do not adapt to changing fraud patterns, making them less effective against new types of cyber threats (Hilal 2022).
b. High False Positives - Frequent legitimate transactions that exceed these thresholds can trigger false alarms, overwhelming the compliance teams.
c. Evasion by Cybercriminals - Skilled cybercriminals can tailor their activities to remain below these static thresholds, effectively evading detection (Bello et al., 2023).
d. Scalability issues - As the volume and complexity of transactions increase, static thresholds can become cumbersome and difficult to manage, leading to scalability issues.

2.2 The Evolving Nature of Financial Cybercrime and Evasive Maneuvers

As studies have shown and from several case studies reviewed, financial cybercrime encompasses a broad spectrum of illicit activities, including phishing, malware attacks, identity theft, and fraudulent transactions. Financial cybercrime poses a significant threat, with losses reaching billions of dollars annually (Hassan et al., 2024). Criminals use various tactics, including social engineering, evasive maneuvers, account

takeover, and new account fraud (Immadisetty, 2025). Cybercriminals continually evolve their methods to exploit vulnerabilities in financial systems, often staying one step ahead of conventional security measures (Ahmad, 2024).

2.2.1 Evasive Maneuvers in Financial Transactions

Evasive maneuvers in financial transactions refer to techniques used by cybercriminals to bypass transaction thresholds (or aid it) to evade detection by fraud detection systems (Nicholls., 2021). These evasive techniques include:

a. Threshold arbitrage (manipulating transaction amounts)
b. Masking IP addresses
c. Distributed and velocity attacks
d. Low-and-slow attacks
e. Money muling
f. Social engineering
g. vii- Obfuscation
h. Encryption
i. Exploiting vulnerabilities

These tactics help cybercriminals bypass traditional fraud detection methods, highlighting the need for advanced and intelligent security solutions to stay ahead of these evasive maneuvers (Nicholls., 2021).

2.2.2 Cases of Financial Fraud in Nigerian Financial Institutions

Nigeria is not left out as there have been instances where Nigerian financial institutions have fallen victim to cyber-attacks, resulting in significant financial losses and compromised sensitive customer information (Bello et al., 2023). The increasing reliance on digital banking and online transactions in Nigeria has created a vast attack surface for cybercriminals to exploit, emphasizing the need for more effective and adaptive fraud detection measures to combat the evolving threat landscape.

The study by SurfShark, an Amsterdam-based cybersecurity firm, ranked Nigeria as the 32nd most breached nation by the first quarter of 2023 (TechCabal, 2023; Gavou et al 2024). This data breach ranking highlights the increasing cybersecurity challenges faced by the country. Regarding financial losses due to fraud in Nigeria's banking sector, there has indeed been a significant increase. Between July and September 2020, banks lost N3.5 billion, representing a 534% increase from the same period in 2019 (TechCabal, 2023). In 2018, commercial banks reported losses of N15 billion to electronic fraud and cybercrime. Regarding financial losses due to fraud in Nigeria's banking sector, there has indeed been a significant increase. Between July and September 2020, banks lost N3.5 billion, representing a 534% increase from the same period in 2019 (TechCabal, 2023). In 2018, commercial banks reported losses of N15 billion to electronic fraud and cybercrime. A notable incident occurred in September 2022, when suspected fraudsters hacked a customer's account and transferred N523.337 million to 18 different accounts within the same bank.

In November 2022, a gang of hackers known as OPERA1ER stole at least $11 million from companies across Nigeria, Benin, Cameroon, and 11 other African countries, as well as Argentina (Onyejegbu, 2023) . The financial losses in Nigeria's banking sector due to fraud have been considerable. In 2021, the value of fraud was N193.5 billion ($544 million), which increased from N153.4 billion ($431 million) in 2020 (Abiodun, 2023). This upward trend continued in 2022, with losses reaching N273 billion ($762 million). Financial Institutions Training Centre (FITC) reported that in 2024, during Q3 2024, a total of 19,007 fraud cases were reported, marking a significant rise of approximately 65% from the 11,532 cases recorded in Q2 2024. Financial institutions in Nigeria lost N52. 26 billion to fraud in 2024 according to the latest report by the Nigeria Inter-Bank Settlement System (NIBSS, 2025). This represents a significant increase of N34.59 billion compared to the N17.67 billion recorded in 2023. These crimes are often committed through phishing and identity theft and evasive techniques.

More recently, more financial service providers fell victims to similar fraud incidents in Nigeria. They include:

a. Flutterwave-- Flutterwave experienced its fourth cybersecurity breach in 14 months, with ₦11 billion ($7 million) transferred to accounts across five financial institutions over four days in April 2024 (Techcabal, 2024). The perpetrators made deposits below fraud detection limits (i.e., evaded transaction threshold) to avoid triggering alerts.
b. Interswitch--In 2023, Interswitch, an African fintech company, lost ₦30 billion ($38 million) to chargeback fraud, which is believed to have been carried out by its own employees who exploited vulnerabilities in the system over several years.
c. Access Bank-- Access Bank reported in 2023 that it lost23 ₦ 5.46 billion to fraudulent transfers, withdrawals and reactivation of accounts in the first six months of 2023. This represents 355 percent increase from ₦ 1.2 billion lost to fraudsters in the corresponding period of 2022 (Economy Post, 2023)
d. First Bank--A former employee of First Bank in Nigeria, allegedly diverted ₦40 billion from the bank through his position on the electronic products team. He exploited his authority to process customer refunds, instead crediting the funds to a merchant account he controlled, allowing him to embezzle the money over almost two years without detection.

All the evidences presented highlight the inadequacy of traditional methods for financial cybercrime detection in Nigeria, demonstrating the need for more dynamic and intelligent security solutions.

2.3 Advances in Adaptive Fraud Detection Techniques

Financial cybercrime is a growing threat and traditional methods often struggle to keep pace with evolving criminal tactics (Emran et al., 2024). This section investigates advanced techniques that use machine learning (ML), big data analytics, and behavioral analytics to combat these threats

2.3.1 Machine Learning (ML) Algorithms

ML algorithms excel at identifying patterns in vast datasets, uncovering anomalies that might be missed by static rules (Yang et al., 2022). Techniques like anomaly detection, clustering, and predictive modeling are increasingly utilized in financial cybersecurity (Odeyemi et al., 2024).

Anomaly detection techniques identify transactions or user behaviors that deviate significantly from established patterns, potentially indicating fraudulent activity (Bansal et al., 2024).

Clustering techniques, on the other hand, group similar data points together, allowing analysts to identify groups with a high prevalence of fraud or suspicious behavior (Hilal, 2022).

Predictive modeling techniques analyze historical data to statistically predict the likelihood of future fraudulent events. By identifying high-risk transactions in advance, institutions can take preventive measures (McCarthy et al., 2022).

2.3.2 Big Data Analytics

Big data analytics involves examining large and complex datasets to uncover trends, anomalies, and hidden insights (Emran, 2024). This plays a crucial role in financial cybercrime detection by enabling real-time analysis and future predictions.

Real-time data processing techniques like stream processing utilize tools like Apache Kafka and Spark Streaming to analyze vast amounts of data instantaneously. This allows for immediate detection and response to suspicious activities (Udeh et al., 2024). Predictive analytics is an advanced analytical technique which utilizes historical data, statistical models, and ML algorithms to forecast future fraudulent behavior. By proactively identifying high-risk transactions, institutions can take preventative actions (Bello et al., 2024b).

2.3.3 Behavioral Analytics

Behavioral analytics focuses on analyzing user interactions with financial systems to understand patterns and identify deviations that might indicate fraud (Aziz, 2023). This approach is particularly effective as it considers the unique characteristics of each user's behavior.

Integral Components of Behavioral Analytics in financial transactions include:

a. Continuous Monitoring - Real-time monitoring of user activities and transactions allows for immediate identification of deviations from normal behavior patterns, enabling a swift response to potential fraud (Kian, 2022).
b. Adaptive Systems - As user behavior evolves over time, adaptive systems adjust fraud detection models to maintain accuracy and effectiveness. This reduces false positives and improves the detection of new fraudulent patterns (Bello, 2024).
c. Risk Scoring - Transactions are assigned risk scores based on how closely they align with a user's typical behavior. Higher risk scores indicate a greater deviation from normal patterns, prompting additional verification or actions to mitigate potential fraud.
d. Context-Aware Risk Assessment - This approach incorporates contextual information like user location, recent activity, and transaction history into the risk assessment process. By considering these factors, institutions can more accurately distinguish between legitimate and fraudulent activities.

2.4 Critical Synthesis and Research Gap

While significant advancements have been made in financial cybercrime detection, several critical limitations remain in the current body of research.

First, most existing solutions address either adaptive learning or real-time processing, but rarely both simultaneously. The literature reveals a lack of integration between these two essential components for effective fraud detection in the Nigerian context.

Second, while machine learning algorithms have shown promise in identifying patterns of fraud, their implementation in Nigerian financial institutions has been limited due to challenges in obtaining quality training data that reflects the unique patterns of Nigerian financial transactions and cybercrime tactics. This creates a gap between theoretical models and practical applications.

Third, existing approaches tend to focus on either technical solutions or process improvements, but seldom address both dimensions. This fragmented approach fails to provide a comprehensive framework capable of addressing the multi-faceted nature of financial cybercrime in Nigeria.

Fourth, behavioral analytics systems currently in use often lack the contextual understanding necessary to differentiate between legitimate cultural banking practices in Nigeria and genuinely suspicious behavior, leading to high rates of false positives and diminishing the effectiveness of fraud detection systems.

The concept of intelligent thresholds that adapt based on real-time data and historical trends has been explored in research. However, limited research investigates the integration of both adaptive and dynamic elements within a single framework tailored specifically to Nigeria's unique financial ecosystem. This research gap is particularly pronounced when considering the sophisticated evasive maneuvers employed by cybercriminals targeting Nigerian financial institutions.

The proposed IADT framework addresses these limitations by integrating machine learning capabilities with real-time data analytics, providing a holistic approach that continuously adapts to evolving threats while maintaining sensitivity to the unique characteristics of Nigeria's financial environment. By combining adaptive learning with dynamic threshold adjustment, the IADT framework offers a promising solution to the challenges faced by Nigerian financial service providers in combating increasingly sophisticated financial cybercrime.

3. Methodology

3.1 Choice of Methodology

This research employs a conceptual design approach to develop the Intelligent Adaptive and Dynamic Thresholds (IADT) framework. The work is primarily design-based, focusing on creating a comprehensive architectural framework rather than empirical testing or simulation-based validation at this stage. This conceptual approach was chosen to establish a solid theoretical foundation before proceeding to implementation and testing in future research.

The success of this conceptual design will be evaluated based on the following criteria:

a. Theoretical soundness - The framework's alignment with established principles in cybersecurity, machine learning and risk management
b. Architectural completeness - The comprehensiveness of the framework in addressing the identified limitations of static threshold systems
c. Logical coherence - The clear and logical relationship between different components of the proposed framework
d. Potential for implementation - The feasibility of implementing the framework in real-world financial systems in Nigeria
e. Theoretical advantage - The conceptual advantages the framework offers over existing solutions in countering evasive maneuvers

3.2 Intelligent Adaptive and Dynamic Thresholds (IADT) Framework

The IADT framework is designed to detect fraudulent financial activities, especially evasive maneuvers by utilizing machine learning and real-time data analysis to continuously adjust and refine thresholds. This approach enables:

i. Adaptive thresholds that adjust to changing patterns and anomalies
ii. Dynamic thresholds that respond to emerging threats in real-time
iii. Continuous learning and improvement through feedback loops

3.2.1 Algorithm of the IADT Framework

The algorithm for the framework is given in Algorithm 1 below:

Algorithm 1: Intelligent Adaptive and Dynamic Threshold (IADT) Framework for Financial Fraud detection

---

i. User initiates a transaction. (real-time transaction from various sources, e.g. banking systems, e-payment gateways, lending platforms)
ii. The transaction data is sent to the IADT module.
iii. The IADT module retrieves the user's historical data and current dynamic threshold.
iv. The transaction data is forwarded to the Machine Learning Model for analysis.
v. The ML model generates a risk score based on the analysis.
vi. The risk score is sent back to the IADT module.
vii. The IADT module compares the risk score with the dynamic threshold.
If the score is below the threshold, the transaction is considered likely legitimate.
If the score exceeds the threshold, the transaction is considered suspicious.
viii Based on the assessment:

For a legitimate transaction, the system completes the transaction process and confirmation is sent to the Stakeholders
For a suspicious transaction:
Alert Generation:

The IADT module generates an alert for the suspicious transaction.

Response Coordination:

The alert is sent to the Security Response System for further investigation or potential action.

The Security Response System coordinates the response by assigning the alert to appropriate security teams or automated response systems.

Communication with Stakeholders:

Notifications are sent to relevant stakeholders (e.g., bank fraud department, affected customer) to inform them of the suspicious activity.

Stakeholders provide feedback or take necessary actions, such as temporarily blocking the transaction or account.

ix. The system logs the outcome of the transaction (legitimate or fraudulent) for continuous learning and improvement

The IADT module updates the historical data with the new transaction details and the outcome (approved or flagged as fraudulent).

The machine learning models are retrained periodically with updated data to improve their accuracy and adapt to new fraud patterns.

3.2.2 Pseudocode for Adaptive Threshold and Risk Score Generation Module

This pseudocode defines the Adaptive Threshold and Risk Score Generation Module of IADT framework for fraud detection. The module plays a crucial role in fraud detection by extracting key transaction and user behavior data, predicting risk scores using machine learning, and dynamically assessing transactions against an adaptive threshold. It classifies transactions as either legitimate or suspicious and continuously updates models through feedback to enhance fraud detection accuracy and system adaptability.

The pseudocode is as follows:

```
Input:
        text_data
        fraud_patterns
        user_behavior
        risk_threshold
CalculateDynamicThresholdFunction:
        risk_level = analyze(fraud_patterns, user_behavior)
        dynamic_threshold = adjust(risk_threshold, risk_level)
RiskScoreGeneration:
        features = extract(text_data)
        risk_score = predict(features)
DecisionMaking:
        if risk_score <= dynamic_threshold:
                + "Legitimate"
        else:
                + "Suspicious"
FeedbackLoop:
        review flagged transactions
        update model with feedback
        repeat
Output:
        Transaction status
        Dynamic threshold value
        Risk score
```

The ***analyze()*** function evaluates the current risk level based on observed fraud patterns and user behavior, utilizing a weighted scoring system that considers factors such as transaction history, location anomalies,

and temporal patterns. The ***adjust()*** function then modifies the base risk threshold according to this risk level using a dynamic formula that incorporates both immediate risk factors and longer-term trends identified in the system. The ***extract()*** function processes raw transaction data to identify relevant features for risk assessment, while ***predict()*** function utilizes trained machine learning models to generate a risk score based on these features.

3.3. Components and Architecture of IADT framework

The Intelligent Adaptive and Dynamic Thresholds (IADT) framework is a cutting-edge framework designed to detect and prevent fraudulent transactions in real-time, leveraging a combination of machine learning, real-time data analysis and adaptive threshold mechanism to provide a robust and effective solution for securing financial transactions. The framework consists of several key components, starting with the User Interface which initiates transactions from various sources and sends transaction data to the IADT Module. The IADT Module receives the data, retrieves user's historical data and current dynamic threshold, performs Real-Time Data Analysis using Apache Kafka and Spark Streaming, and employs Stochastic Gradient Descent (SGD) to continuously update the ML models. It then forwards the transaction data to the Machine Learning Model for analysis.

The Machine Learning Model generates the risk score based on its analysis of the transaction data and sends the risk score to the IADT Module, which then compares the risk score with the dynamic threshold to determine the transaction's legitimacy, generates alerts for suspicious transactions and updates historical data with new transaction details and outcomes. The Machine Learning (ML) Model employs a combination of ML algorithms, including Random Forest for transaction classification, Isolation Forest for anomaly detection, and DBSCAN (Density-Based Spatial Clustering of Applications with Noise) for clustering and outlier detection. These algorithms analyze transaction data in real-time, taking into account various features such as transaction amount, location, time and user behavior.

The IADT Module then sends alerts for suspicious transactions to the Security Response System, responsible for coordinating the response by assigning the alert to appropriate security teams or automated response systems and communicating with Stakeholders who receive notifications about suspicious transactions and provide feedback or take necessary actions.

Finally, the framework incorporates Data Storage module for user's historical data and outcomes and a Continuous Learning and Improvement mechanism that updates machine learning models with new data to improve accuracy and adapt to new fraud patterns.

3.3.1 Machine Learning Algorithm Selection Rationale

The IADT framework incorporates specific machine learning algorithms chosen for their complementary strengths in detecting various types of financial fraud:

i. Random Forest for Transaction Classification: This algorithm was selected for its high accuracy in classification tasks and robustness against overfitting. Random Forest's ensemble approach, combining multiple decision trees, is particularly effective at handling the complex, non-linear relationships often present in financial transaction data. It also provides importance scores for features, enhancing the interpretability of the model's decisions.

ii. Isolation Forest for Anomaly Detection: This algorithm was chosen for its efficiency in identifying outliers without requiring labeled fraud data. Isolation Forest specifically excels at detecting anomalies in high-dimensional spaces and is computationally efficient, making it suitable for real-time processing of large transaction volumes. Its approach of isolating anomalies rather than profiling normal instances makes it particularly effective for detecting novel fraud patterns.

iii. DBSCAN (Density-Based Spatial Clustering of Applications with Noise) for Clustering and Outlier Detection: DBSCAN was selected for its ability to discover clusters of arbitrary shapes without requiring a predefined number of clusters. This is crucial for identifying groups of similar

transactions and detecting outliers that don't fit into any cluster. DBSCAN is particularly useful for identifying distributed attacks where multiple small transactions might collectively form a pattern.

iv. Stochastic Gradient Descent (SGD) for Continuous Model Updates: SGD was chosen for its efficiency in updating machine learning models incrementally with new data. This enables the framework to continuously adapt to evolving fraud patterns without requiring complete retraining of models, which is essential for maintaining real-time responsiveness.

3.3.2 High-level Architecture of the Framework

The high-level model of the framework is shown in Figure 1. This model illustrates the IADT Framework's integrated approach to fraud detection through real-time data analysis, machine learning and adaptive thresholding mechanisms. The system's continuous learning capabilities enable dynamic adaptation to emerging fraud patterns through feedback integration and stochastic model updates.

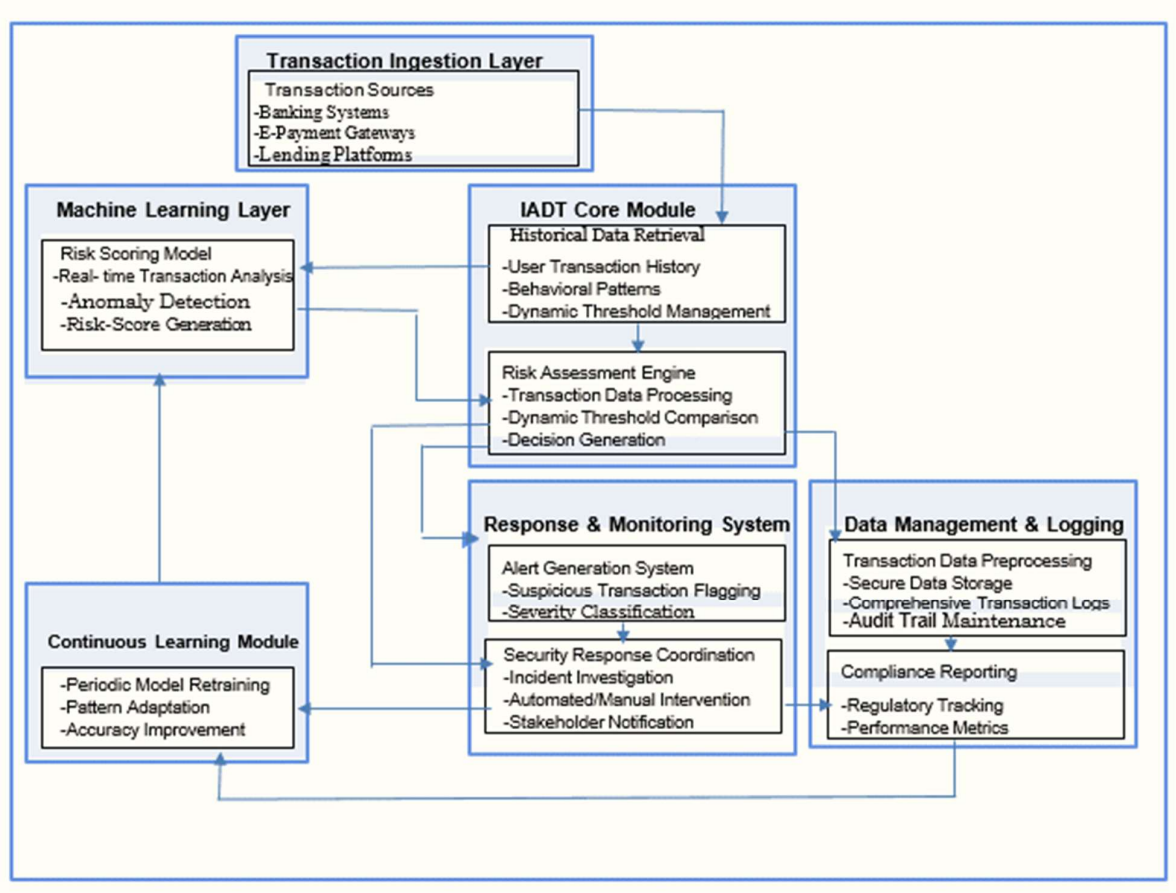

Figure 1: High level model of the IADT framework

3.3.3 Sequence Diagram of IADT framework

Figure 2 shows the sequence of operations in the IADT framework and shows how the various components interact to detect and mitigate cyber threats using intelligent adaptive and dynamic thresholds. The key components in the system include: The User module, Intelligent Adaptive and Dynamic Threshold Module, Machine Learning Model, Security Response module and the Stakeholders module. Below is a description of each step in the sequence diagram.

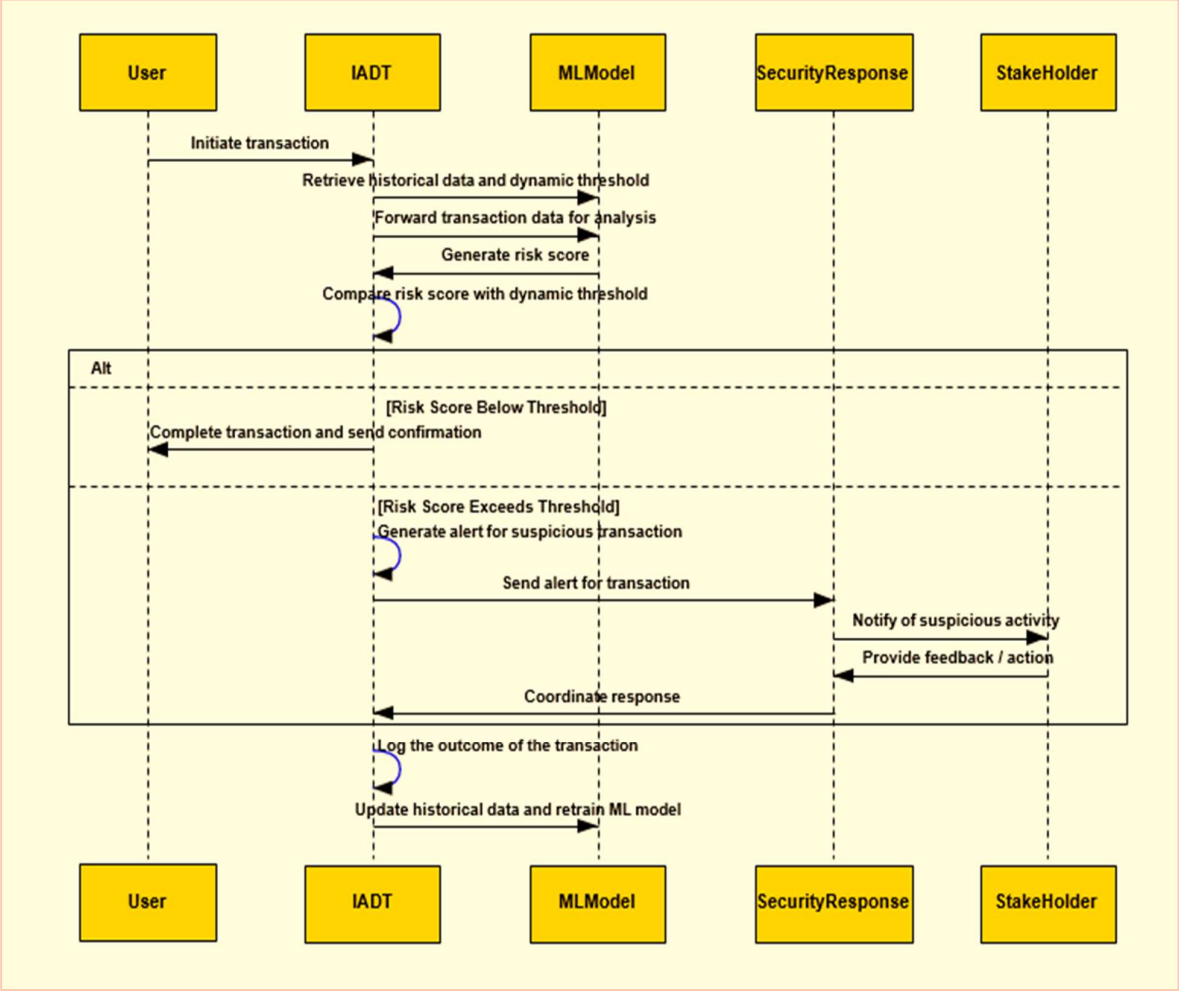

Figure 2: Sequence diagram of IADT Framework

3.4 Data Requirements and Processing Scale

The IADT framework is designed to process transaction data from multiple sources within Nigeria's financial ecosystem, including:

i. Banking Systems: Traditional banking transactions including deposits, withdrawals, transfers, and payments
ii. E-payment Gateways: Online payment processors and mobile money platforms
iii. Lending Platforms: Loan applications and repayment transactions
iv. Point of Sale (POS) Terminals: Retail transaction data
v. Mobile Banking Applications: Transactions initiated through mobile banking channels

The framework is architected to handle large-scale transaction processing with the following capabilities:

i. Peak Processing Capacity: Up to 1,000 transactions per second
ii. Daily Transaction Volume: Designed to handle up to 50 million daily transactions
iii. Data Storage: Scalable storage for historical transaction data spanning up to 7 years
iv. Feature Vector Size: Each transaction is represented by approximately 200 features
v. Response Time: Sub-second response time for transaction risk assessment

Data preprocessing includes normalization, feature extraction and transformation to ensure consistency across different data sources. The framework employs a federated approach where possible, allowing models to learn from distributed data sources without centralizing all sensitive transaction data.

3.5 Computational Requirements and Performance Considerations

The IADT framework depends on a highly resilient, distributed computing environment in which containerized services—deployed and managed via Kubernetes—can seamlessly scale to meet fluctuating demand. Each processing node is provisioned with at least 64 GB of RAM to enable efficient in-memory analytics, while a hybrid storage strategy combines high-speed SSD volumes for active datasets with cost-effective object stores for long-term retention. A low-latency network backbone, delivering 10 Gbps or more between services, ensures that data moves swiftly through the detection pipeline.

To uphold the framework's real-time promise, we target an end-to-end risk-scoring latency of no more than 100 milliseconds, even under heavy load. Horizontal scaling allows throughput to grow in step with transaction volume, and built-in redundancy guarantees 99.99 percent availability: if a node fails, the system automatically redeploys its workloads within thirty seconds, maintaining continuous operation without human intervention.

At its heart, IADT processes incoming transactions as an uninterrupted stream rather than in discrete batches, with the flexibility to reorder late-arriving events within a configurable time window. Stateful processing across the cluster preserves each user's behavioral context, enabling consistent risk assessments. Finally, a dynamic resource-scaling policy continuously monitors transaction flow and provisions or decommissions compute resources in real time, ensuring that the framework remains both responsive and cost-efficient during peak activity.

4. Results and Discussion

The IADT framework is designed to analyze transaction data in real-time, enabling swift detection and response to potential threats through its real-time transaction analysis capability. Additionally, the framework's adaptive risk management capabilities allow it to adjust risk scoring and thresholding in real-time, ensuring that it stays effective against evolving threats. Furthermore, the IADT framework's anomaly detection algorithms can identify suspicious transactions that deviate from expected behavior, while its machine learning algorithms analyze transaction data, generate risk scores and improve its detection capabilities over time. The framework's continuous learning and improvement mechanism also enables it to update its models with new data, ensuring that it stays accurate and effective.

While this paper presents a conceptual framework, further empirical validation through simulations and pilot implementations would be necessary to quantify the framework's effectiveness. Future research should include performance metrics such as detection rates, false positive reduction and response time improvements when compared to traditional static threshold systems.

When implemented, the IADT framework would offer several advantages over traditional static threshold systems. While static thresholds are rigid and prone to generating false positives, IADT's adaptive approach can reduce false positives by considering the context and historical patterns of transactions. Additionally, while cybercriminals can easily circumvent static thresholds by staying just below the threshold limit, IADT's dynamic adjustment makes such evasion more difficult.

The IADT framework's capabilities have significant implications for the detection and prevention of fraudulent transactions. By providing real-time analysis and adaptive risk management, the framework can help financial institutions in Nigeria stay ahead of emerging threats.

4.1 Implementation Challenges and Strategic Considerations for IADT in Nigerian Financial Institutions

While the adoption of IADT framework holds great promise for enhancing fraud detection and overall cybersecurity in the financial sector, these improvements come with notable trade-offs. Institutions must carefully assess and address the following challenges:

i. Data Privacy and Security - Implementing adaptive and dynamic thresholds requires extensive data collection and analysis, which raises significant concerns about data privacy and security. Nigerian financial institutions must comply with the Nigeria Data Protection Regulation (NDPR) and protect user information from unauthorized access.
ii. Computational Resources - Real-time analysis of large volumes of transaction data demands substantial computational resources. Requirements such as 64GB RAM per processing node, high-performance distributed systems (e.g., Kubernetes clusters), and 10Gbps network infrastructure exceed the current capabilities of many institutions, especially smaller banks.
iii. Continuous Model Updates - The machine learning models underpinning the IADT framework must be updated regularly to remain effective against evolving fraud patterns. This requires a dedicated pipeline for model retraining and validation, as well as highly skilled data science and cybersecurity personnel.
iv. High Implementation and Maintenance Costs - The financial burden of deploying and maintaining the IADT infrastructure is considerable. Initial investments may range from ₦75–155 million per institution, with annual costs for software maintenance, system updates, and personnel training. Despite potential returns, such costs can be prohibitive for many institutions.

To effectively overcome these challenges, the following strategic measures are recommended:

i. Regulatory Engagement - Early and continuous collaboration with the Central Bank of Nigeria (CBN) and relevant data protection authorities is crucial. This helps institutions align implementation with regulatory expectations, leverage regulatory sandboxes for innovation and clarify data-sharing protocols.
ii. Tiered Deployment Models - Offering scalable implementation options tailored to the size and capacity of each institution ensures inclusivity. Smaller banks can start with basic functionalities and gradually scale as their infrastructure and expertise grow.
iii. Model Lifecycle Management - Institutions should establish automated pipelines and dedicate expert teams for continuous machine learning model training, testing and deployment. This ensures that the system remains adaptive and effective in detecting new fraud patterns.
iv. Hybrid Processing Architecture - By combining edge processing (for time-sensitive analysis on-premises) with cloud-based processing (for deeper analytics), institutions can reduce infrastructure pressure and enhance processing efficiency while maintaining control over sensitive data.
v. Total Cost of Ownership (TCO) Analysis -A thorough TCO evaluation helps institutions make informed investment decisions by weighing the upfront and recurring costs against expected benefits like fraud reduction, improved operational efficiency and enhanced customer trust.

4.3 Future Directions

The IADT framework provides a foundation for further research and development. Future directions include:

i. Integration with Blockchain Technology - Blockchain technology offers potential enhancements to adaptive security measures through its decentralized and immutable ledger system. Integrating blockchain can increase the transparency and security of financial transactions.
ii. Collaborative Threat Intelligence - Sharing threat intelligence among financial institutions can improve adaptive security measures. Collaborative platforms enable the exchange of information about emerging threats and successful defense strategies, fostering a collective defense against cybercrime.
iii. Advancements in Artificial Intelligence - Continued advancements in artificial intelligence (AI) and machine learning will further enhance the capabilities of adaptive security systems. Future research should focus on developing more sophisticated models that can better detect and respond to evolving cyber threats.

5. Conclusion

In an era where cybercriminals continually refine their tactics, static fraud-detection rules can no longer safeguard financial systems. This paper has introduced the Intelligent Adaptive and Dynamic Threshold (IADT) framework—a proactive security architecture that leverages machine learning, real-time analytics, and behavior-driven risk scoring to continuously recalibrate defenses against emerging threats. By deploying containerized services across a resilient Kubernetes cluster, maintaining sub-100 ms scoring latency, and automatically recovering from failures, IADT transforms financial cybersecurity from a reactive posture into a self-tuning, always-on shield. Implementing such a system in Nigeria's financial sector demands significant infrastructure investment and organizational commitment, but the payoff—higher detection rates, fewer false positives, and uninterrupted service—justifies the effort. Looking ahead, pilot deployments will be essential to validate performance at scale, refine adaptive algorithms, and shape regulatory guidelines that support dynamic security models. Ultimately, only by embracing intelligence-driven, evolving thresholds can financial institutions stay a step ahead of sophisticated adversaries and preserve the integrity of their operations.

References

Abdullahi, R., & Mansor, N. (2018). Fraud Prevention Initiatives in the Nigerian Public Sector: Understanding the Relationship of Fraud Incidences and the Elements of Fraud Triangle Theory. *Journal of Financial Crime, 25,* 527-544. https://doi.org/10.1108/jfc-02-2015-0008

Abiodun, A. (2023). *Nigeria's financial sector under siege: The alarming rise of cyber fraud and inadequate defenses*. Business Day.

Ahmad, N. (2024). Deep Learning for Fraud Detection in Financial Transactions: A Novel Approach to Detect Hidden Anomalies. MCS.

Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

Bansal, P. K., Nimma, D., Das, N. N., Paruchuri, B. P., Anandaram, H., & Karthik, M. (2024). Boosting Anomaly Detection in Financial Transactions: Leveraging Deep Learning with Isolation Forest for Enhanced Accuracy. In *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA)* (pp. 1-6). IEEE.

Bello O.A (2022). Machine Learning Algorithms for Credit Risk Assessment: An Economic and Financial Analysis. International Journal of Management Technology, pp109 - 133

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.

Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. *World Journal of Advanced Engineering Technology and Sciences, 12(2)*, 21–34.

Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology, 10(1)*, 85–108.

Emran, A. K. M., & Rubel, M. T. H. (2024). Big Data Analytics and Ai-Driven Solutions for Financial Fraud Detection: Techniques, Applications, and Challenges. *Frontiers in Applied Engineering and Technology*, *1*(01), 269-285.

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in The Financial Sector: A Comparative Analysis of the Usa And Nigeria. Computer Science & IT Research Journal, 5(4), 850-877.

FITC (2024). Report on Fraud and Forgeries in the Nigerian Banking Industry for Q3 Year 2024

Gavou, T. P., Iliya, J., Ihuoma, E. C., & Gusen, J. N. (2024). Cyber security enhancement in Nigeria. A case study of six states in the north central (middle belt) of Nigeria. *American Journal of Humanities and Social Sciences Research*, *8*(05), 95-115.

Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Artificial intelligence-driven effective financial transaction monitoring. In *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance* (pp. 79-91). Singapore: Springer Nature Singapore.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems with applications*, *193*, 116429.

Immadisetty, A. (2025). Real-Time Fraud Detection Using Streaming Data in Financial Transactions. *Journal of Recent Trends in Computer Science and Engineering (JRTCSE)*, *13*(1), 66-76.

Kian, R., & Obaid, H. S. (2022). Detection of fraud in banking transactions using big data clustering technique customer behavior indicators. *Journal of applied research on industrial engineering*, *9*(3), 264-273.

McCarthy, R. V., McCarthy, M. M., Ceccucci, W. & Halawi, L. (2022). *Applying predictive analytics* (pp. 89-121). Springer International Publishing.

Narayan, A., Madhu Kumar, S. D., & Chacko, A. M. (2023). A review of financial fraud detection in e-commerce using machine learning. In V. Bhateja, X. S. Yang, J. Chun-Wei Lin, & R. Das (Eds.), *Intelligent data engineering and analytics. FICTA 2022* (Smart Innovation, Systems and Technologies, Vol. 327, pp. 237-248). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-7524-0_21

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access, 9*, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

Odeyemi, O., Okoye, C. C., Ofodile, O. C., Adeoye, O. B., Addy, W. A., & Ajayi-Nifise, A. O. (2024). Integrating AI with blockchain for enhanced financial services security. *Finance & Accounting Research Journal, 6*(3), 271–287.

Onyejegbu, C. D. (2023). Exploratory study of the internet and business operations in Nigeria.

Shoetan, P. O., & Familoni, B. T. (2024). Transforming Fintech Fraud Detection with Advanced Artificial Intelligence Algorithms. Finance & Accounting Research Journal, 6(4), 602-625

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746-1760.

Yang, Y., Yu, Y., & Li, T. (2022). Deep learning techniques for financial fraud detection. In *2022 14th International Conference on Computer Research and Development (ICCRD)* (pp. 16-22). IEEE. https://doi.org/10.1109/ICCRD54409.2022.9730314