*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

# Intelligent Intrusion Detection Framework for Secure IoT-Enabled Financial Transactions

Research Article https://stem.techspherejournal.com

***Article Info***
Revised: 14th November, 2026
Accepted: 19th November, 2026
Published: 22nd November, 2026

***Keywords***
Internet of Things
Financial Cybersecurity
Intrusion Detection System
Machine Learning
FTITDM

**Author Details**
Obiageli Modupe ATTOH[1*], Tochukwu Cyprian ONYIA[2]
*1* Department of Cybersecurity, Faculty of Computing, Dennis Osadebay University, Asaba, Nigeria.*
*2 Department of Electronic & Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.*
**Corresponding author's email*: attoh.obiageli@dou.edu.ng
DOI: https://doi.org/10.5281/zenodo.24438027

This is an open-access article under the CC BY-SA license

**ABSTRACT**

The Internet of Things (IoT) has transformed financial services through interconnected devices that facilitate digital banking, mobile payments, and automated financial transactions. However, the increasing adoption of IoT technologies has exposed financial infrastructures to cybersecurity threats, including Distributed Denial-of-Service (DDoS), botnet attacks, unauthorized access, and data breaches. Traditional intrusion detection systems often lack the adaptability required to identify evolving and previously unseen threats. This study developed the Financial Transaction Intelligent Threat Detection Model (FTITDM), an intelligent machine learning-based intrusion detection framework for securing IoT-enabled financial transactions. The framework integrates five functional layers comprising IoT devices, network communication, data collection and preprocessing, machine learning detection, and alert and response mechanisms. The study employed three benchmark cybersecurity datasets, namely CICIDS2017, Bot-IoT, and UNSW-NB15, comprising 600,000 records, with 80% allocated for training and 20% for testing. Decision Tree, Random Forest, FTITDM, and Deep Neural Network algorithms were implemented and comparatively evaluated using accuracy, precision, recall, and F1-score. Experimental results revealed that FTITDM achieved the best performance, recording 99.17% accuracy, 98.96% precision, 99.05% recall, and 99.00% F1-score. It also achieved an average detection rate of 99.04% and a false positive rate of 0.89% across the three datasets. These findings demonstrate the effectiveness of FTITDM in detecting diverse cyber threats while maintaining computational efficiency. The study concludes that the proposed framework provides a promising approach to strengthening the security, reliability, and resilience of IoT-enabled financial transaction systems.

## 1 Introduction

### 1.1 Background to the Study

The rapid advancement of the Internet of Things (IoT) has transformed the financial sector by enabling interconnected devices to support digital banking, mobile payments, contactless transactions, smart point-of-sale (POS) terminals, and automated financial services [1]. As financial institutions increasingly adopt IoT technologies, digital payment platforms have become more efficient, accessible, and convenient for consumers and businesses alike. The integration of IoT

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

devices within financial ecosystems has facilitated real-time transaction processing, remote account management, and enhanced customer experiences [2].

Despite these benefits, IoT-enabled financial systems face significant cybersecurity challenges due to the large number of connected devices, heterogeneous network environments, and continuously evolving threat landscapes. Cybercriminals exploit vulnerabilities in IoT networks to launch attacks such as Distributed Denial-of-Service (DDoS), botnet infections, unauthorized access, data breaches, and transaction manipulation [3]. These threats can compromise the confidentiality, integrity, and availability of financial transactions, resulting in substantial financial and reputational losses. Consequently, there is an increasing need for intelligent security solutions capable of detecting and mitigating sophisticated cyber threats in real time.

### 1.2 Problem Statement

The growing reliance on IoT technologies in financial services has expanded the attack surface available to cybercriminals. Modern financial infrastructures are increasingly targeted by attacks designed to exploit vulnerabilities in connected devices and network communications [4]. Traditional intrusion detection systems (IDS) often rely on predefined signatures and static rules, making them ineffective against emerging and previously unseen attacks that characterize dynamic IoT environments.

Furthermore, the high volume, velocity, and diversity of network traffic generated by IoT devices create challenges for conventional security mechanisms in accurately identifying malicious activities [5]. This necessitates the development of intelligent and adaptive intrusion detection frameworks capable of learning traffic patterns, recognizing anomalies, and responding effectively to evolving cyber threats. Leveraging benchmark cybersecurity datasets such as CICIDS, Bot-IoT, and UNSW-NB15 provides an opportunity to develop and validate robust machine learning-based solutions for securing IoT-enabled financial transactions [6].

### 1.3 Aim and Objectives of the Study

The aim of this study is to develop an intelligent intrusion detection framework for enhancing security in IoT-enabled financial transactions.

The specific objectives are to:

1. Identify key security threats affecting IoT-enabled financial ecosystems.
2. Design a machine learning-based intrusion detection framework for detecting malicious activities in financial network environments.
3. Implement and evaluate the proposed framework using benchmark datasets, including CICIDS, Bot-IoT, and UNSW-NB15.
4. Assess the effectiveness of the framework using performance metrics such as accuracy, precision, recall, F1-score, and false positive rate.

### 1.4 Research Questions

The following research questions are presented for this study:

1. What are the major cyber threats affecting IoT-enabled financial transaction systems?
2. How can machine learning techniques improve intrusion detection in IoT-based financial networks?
3. How effectively can the proposed framework detect malicious activities using the CICIDS, Bot-IoT, and UNSW-NB15 datasets?
4. What performance improvements can be achieved compared to conventional intrusion detection approaches?

### 1.5 Significance of the Study

This study contributes to the growing body of knowledge in financial cybersecurity by proposing an intelligent intrusion detection framework tailored to IoT-enabled financial environments. The research demonstrates how machine learning techniques can be utilized to improve the detection of cyber threats in digital payment infrastructures.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

Practically, the proposed framework can enhance the security and resilience of financial transaction systems by providing early detection of malicious activities and reducing the likelihood of successful attacks. The use of widely recognized benchmark datasets ensures the reliability and reproducibility of the study's findings. Ultimately, the research supports the development of more secure digital payment ecosystems, thereby improving stakeholder confidence and trust in IoT-enabled financial services

## 2 Literature Review

### 2.1 Conceptual Review

The Internet of Things (IoT) refers to a network of interconnected physical devices equipped with sensors, software, and communication technologies that enable data collection, exchange, and processing over the internet [7]. In the financial sector, IoT facilitates real-time connectivity among devices such as smart Point-of-Sale (POS) terminals, Automated Teller Machines (ATMs), mobile banking devices, wearable payment systems, and smart banking infrastructure. The increasing adoption of IoT technologies has enhanced financial service delivery, operational efficiency, and customer convenience. However, the distributed and heterogeneous nature of IoT environments introduces significant security challenges, making these systems attractive targets for cyberattacks.

Financial Technology (FinTech) represents the integration of innovative technologies into financial services to improve efficiency, accessibility, and customer experience [8]. Digital payment systems, including mobile wallets, internet banking, contactless payments, QR-code transactions, and cryptocurrency platforms, have become critical components of modern financial ecosystems. The widespread use of digital payment infrastructures has accelerated financial inclusion and transaction speed. Nevertheless, increasing transaction volumes and interconnected systems have heightened cybersecurity risks, emphasizing the need for robust security mechanisms that can protect sensitive financial data and transaction processes.

An Intrusion Detection System (IDS) is a cybersecurity solution designed to monitor network traffic and system activities to identify unauthorized access, malicious behavior, and security policy violations [9]. IDS solutions are generally categorized as signature-based or anomaly-based systems. Signature-based IDS detects known threats using predefined attack patterns, while anomaly-based IDS identifies deviations from normal system behavior. In IoT-enabled financial environments, traditional IDS approaches often face limitations due to dynamic network conditions, high data volumes, and the emergence of sophisticated attack techniques, necessitating more intelligent detection methods.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as effective technologies for addressing modern cybersecurity challenges [10]. Machine learning algorithms can process large volumes of network traffic data, identify hidden attack patterns, and continuously improve detection performance through learning. Common machine learning techniques used in intrusion detection include Decision Trees, Random Forests, Support Vector Machines, Extreme Gradient Boosting (FTITDM), and Deep Learning models. These techniques enable proactive threat detection, anomaly identification, reduced false alarms, and improved response to previously unseen attacks, making them particularly suitable for securing IoT-enabled financial systems.

### 2.2 Theoretical Review

The Defense-in-Depth Theory advocates the deployment of multiple layers of security controls to protect information systems against cyber threats [11]. Rather than relying on a single security mechanism, organizations implement complementary defenses at the network, application, device, and data levels. In IoT-enabled financial systems, defense-in-depth supports the integration of firewalls, encryption protocols, authentication mechanisms, access controls, and intrusion detection systems. This theory provides the foundational framework for incorporating intelligent intrusion detection as a critical layer of security protection.

Anomaly Detection Theory is based on the principle that malicious activities often deviate from established patterns of normal behavior. In cybersecurity, anomalies can be identified by monitoring network traffic characteristics, user behaviors, and system activities. Any significant deviation from expected patterns may indicate an intrusion attempt or

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

security breach [12]. The theory serves as the foundation for machine learning-based IDS solutions, which learn normal network conditions and classify abnormal activities as potential threats. This approach is particularly effective against zero-day attacks and previously unknown cyber threats.

Machine Learning Theory focuses on the ability of computational models to learn from historical data and make predictions about future observations [13]. Classification algorithms are trained using labeled datasets to distinguish between normal and malicious traffic, while predictive models identify patterns associated with emerging threats. In intrusion detection research, machine learning enables automated decision-making and adaptive learning capabilities. The theory supports the use of datasets such as CICIDS, Bot-IoT, and UNSW-NB15 for training and validating intrusion detection models capable of accurately classifying cyberattacks within financial network environments.

### 2.3 Empirical Review

Several studies have investigated intrusion detection mechanisms for IoT networks using both traditional and intelligent approaches. Signature-based IDS models have demonstrated effectiveness in detecting known cyber threats but often fail to identify new attack variants [14]. Anomaly-based IDS solutions have shown improved adaptability by recognizing unusual network behaviors. However, many existing models were developed for general network environments and may not adequately address the unique characteristics of financial IoT infrastructures, including transaction sensitivity, low latency requirements, and high security demands.

Recent research has increasingly focused on machine learning and deep learning techniques for intrusion detection. Studies utilizing Random Forest, Decision Tree, Support Vector Machine, FTITDM, and Neural Network models have reported high detection accuracy on benchmark datasets such as CICIDS, Bot-IoT, and UNSW-NB15 [15]. AI-based approaches have demonstrated superior performance in feature selection, classification accuracy, and anomaly detection compared to conventional methods. Despite these advantages, challenges such as class imbalance, computational complexity, model interpretability, and scalability remain significant concerns.

Researchers have proposed various security frameworks to address threats within financial transaction environments. These frameworks commonly incorporate authentication mechanisms, encryption protocols, blockchain technologies, threat intelligence systems, and intrusion detection capabilities. While existing frameworks enhance transaction security, many focus primarily on authentication and data protection rather than proactive threat detection. Furthermore, several frameworks lack adaptive learning capabilities required to combat evolving cyber threats in IoT-driven financial ecosystems [16].

A review of existing studies reveals that significant progress has been made in applying machine learning to intrusion detection. However, many studies concentrate on generic IoT networks rather than financial transaction systems [17]. Furthermore, most research evaluates detection models using a single dataset, which may limit the generalizability and robustness of findings. Comparatively fewer studies combine multiple benchmark datasets such as CICIDS, Bot-IoT, and UNSW-NB15 to develop comprehensive intrusion detection frameworks capable of detecting diverse attack categories. These limitations indicate the need for more adaptive, scalable, and context-specific security solutions for IoT-enabled financial environments.

### 2.4 Research Gap

Despite advances in intrusion detection research, several gaps remain in securing IoT-enabled financial transaction systems.

First, many existing IDS models exhibit inadequate adaptation to evolving financial cyber threats. Most traditional systems depend heavily on predefined signatures or static detection rules, making them less effective against sophisticated and emerging attacks [18].

Second, there is limited integration of intelligent learning mechanisms specifically designed for IoT-based financial ecosystems. While machine learning techniques have been widely studied, their application within financial IoT

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

environments remains relatively underexplored, particularly in addressing transaction-specific security requirements [19].

Third, existing solutions often struggle to provide real-time and scalable intrusion detection capable of handling the high traffic volumes generated by interconnected financial devices. Many proposed models also lack comprehensive evaluation across diverse datasets [20].

To address these gaps, this study proposes an intelligent machine learning-based intrusion detection framework that leverages multiple benchmark datasets, namely CICIDS, Bot-IoT, and UNSW-NB15, to improve threat detection accuracy, adaptability, scalability, and overall security within IoT-enabled financial transaction systems.

## 3 Materials and Methods

### 3.1 Research Design

This study adopts a design and simulation-based research approach to develop and evaluate an intelligent intrusion detection framework for securing IoT-enabled financial transactions. The research focuses on designing a machine learning-based intrusion detection system capable of identifying malicious activities within IoT financial networks. The framework will be developed, trained, and tested using benchmark cybersecurity datasets, namely CICIDS, Bot-IoT, and UNSW-NB15 [20]. A comparative analysis of different machine learning algorithms will be conducted to determine the most effective model for intrusion detection. The simulation approach enables the evaluation of the framework's performance in a controlled and reproducible environment without exposing real financial systems to operational risks.

### 3.2 System Architecture

The proposed framework consists of five interconnected layers designed to provide comprehensive intrusion detection capabilities within IoT-enabled financial environments. See Figure 1.

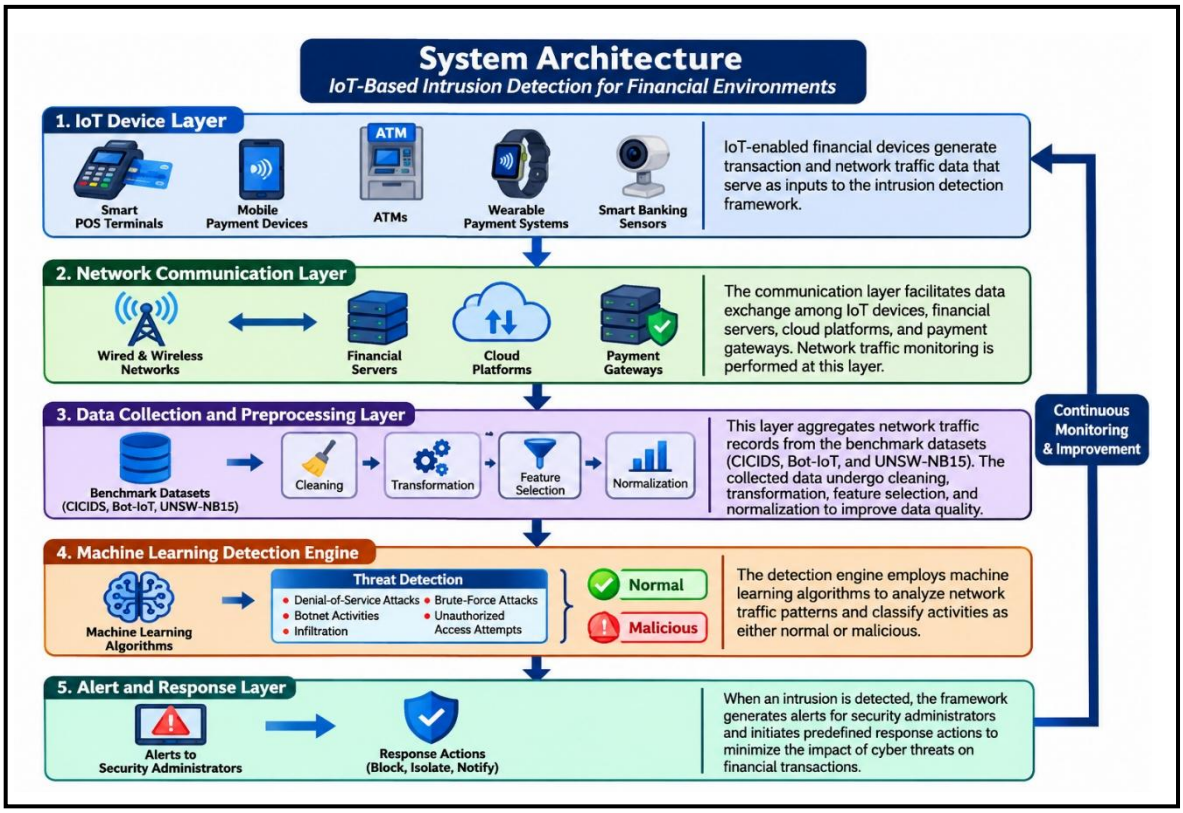



**Figure 1:** Proposed System Architecture

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

**IoT Device Layer**

This layer comprises IoT-enabled financial devices such as smart Point-of-Sale (POS) terminals, mobile payment devices, ATMs, wearable payment systems, and smart banking sensors. These devices generate transaction and network traffic data that serve as inputs to the intrusion detection framework.

**Network Communication Layer**

The communication layer facilitates data exchange among IoT devices, financial servers, cloud platforms, and payment gateways through wired and wireless networks. Since attacks frequently target communication channels, network traffic monitoring is performed at this layer.

**Data Collection and Preprocessing Layer**

This layer aggregates network traffic records from the benchmark datasets (CICIDS, Bot-IoT, and UNSW-NB15). The collected data undergoes cleaning, transformation, feature selection, and normalization to improve data quality and model performance.

**Machine Learning Detection Engine**

The detection engine serves as the core component of the framework. It employs machine learning algorithms to analyze network traffic patterns and classify activities as either normal or malicious. The trained models detect cyber threats such as denial-of-service attacks, botnet activities, infiltration, brute-force attacks, and unauthorized access attempts.

**Alert and Response Layer**

When an intrusion is detected, the framework generates alerts for security administrators and initiates predefined response actions. This layer supports timely decision-making and minimizes the impact of cyber threats on financial transactions.

### 3.3 Data Collection

The study utilizes publicly available benchmark cybersecurity datasets widely employed in intrusion detection research.

i. **CICIDS Dataset**
   The CICIDS dataset contains realistic network traffic and a variety of modern attack scenarios, including brute-force attacks, denial-of-service attacks, web attacks, infiltration attacks, and distributed denial-of-service attacks.

ii. **Bot-IoT Dataset**
   The Bot-IoT dataset is specifically designed for IoT environments and contains both legitimate and malicious traffic generated from IoT networks. It includes botnet activities, DDoS attacks, data exfiltration, reconnaissance attacks, and information theft scenarios.

iii. **UNSW-NB15 Dataset**
   The UNSW-NB15 dataset consists of modern network traffic records and various attack categories such as exploits, fuzzers, backdoors, worms, reconnaissance, and generic attacks. It provides diverse attack representations suitable for evaluating machine learning models.

The use of these three benchmark datasets ensures comprehensive coverage of attack patterns and improves the generalizability of the proposed intrusion detection framework to IoT-enabled financial systems.

### 3.4 Feature Engineering and Data Preprocessing

Data preprocessing is necessary to improve the quality of input data and enhance model performance.

**Data Cleaning**

Incomplete, duplicate, inconsistent, and irrelevant records are identified and removed. Missing values are handled using appropriate imputation techniques where applicable.

**Feature Extraction**

Relevant network traffic features associated with attack behaviours are extracted from the datasets. Features with low predictive significance are removed to reduce dimensionality and computational complexity.

**Data Normalization**

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

Feature values are normalized using scaling techniques such as Min-Max Scaling or Standardization to ensure uniformity across variables and prevent bias during model training.

**Class Balancing**

Cybersecurity datasets often exhibit class imbalance, where normal traffic significantly exceeds attack samples. Techniques such as Synthetic Minority Oversampling Technique (SMOTE) or undersampling are applied to improve model learning and classification performance.

### 3.5 Machine Learning Model Development

The machine learning detection engine will be developed using supervised learning algorithms and evaluated comparatively.

i. **Random Forest**
Random Forest is an ensemble learning technique that constructs multiple decision trees and combines their outputs to improve classification accuracy and reduce overfitting. It is widely applied in intrusion detection due to its robustness and ability to handle high-dimensional data [21].

ii. **Decision Tree**
Decision Tree is a rule-based classification algorithm that simplifies decision-making through hierarchical structures. Its interpretability and computational efficiency make it well-suited for intrusion detection [22].

iii. **FTITDM**
Extreme Gradient Boosting (FTITDM) is an advanced ensemble learning algorithm known for high predictive accuracy, fast processing speed, and effective handling of complex cybersecurity datasets [23].

iv. **Deep Neural Networks (Optional Comparative Model)**
A Deep Neural Network (DNN) model may be implemented as a comparative approach to evaluate the effectiveness of deep learning techniques in detecting sophisticated cyber threats and nonlinear attack patterns [24].

We trained the models on the selected datasets and compared them to determine the most suitable algorithm for the proposed framework.

### 3.6 Performance Evaluation Metrics

The effectiveness of the proposed intrusion detection framework will be assessed using standard classification performance metrics.

**Accuracy**

Accuracy measures the proportion of correctly classified instances among the total observations.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

**Precision**

Precision measures the proportion of correctly detected attacks among all instances classified as attacks.

$$Precision = \frac{TP}{TP + FP}$$

**Recall**

Recall evaluates the framework's ability to correctly identify actual attack instances.

$$Recall = \frac{TP}{TP + FN}$$

**F1-Score**

F1-Score provides a balanced measure of precision and recall.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

**Detection Rate**

Detection Rate measures the percentage of actual attacks successfully identified by the framework.

$$Detection\ Rate = \frac{TP}{TP + FN}$$

**False Positive Rate (FPR)**

False Positive Rate measures the proportion of legitimate traffic incorrectly classified as malicious.

$$FPR = \frac{FP}{FP + TN}$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

### 3.7 Tools and Technologies

The development and evaluation of the proposed framework utilizes the tools and technologies presented in Table 1.

**Table 1:** Tools and Technologies

| **Tool/Technology** | **Purpose** |
|---|---|
| **Python** | Programming language for model development and experimentation |
| **Scikit-learn** | Machine learning library for preprocessing, training, and evaluation |
| **TensorFlow/Keras** | Deep learning framework for implementing neural network models |
| **Wireshark** | Network traffic analysis and packet inspection |
| **Jupyter Notebook** | Experimental environment for data analysis, visualization, and model testing |
| **Pandas** | Data manipulation and preprocessing |
| **NumPy** | Numerical computations and matrix operations |
| **Matplotlib & Seaborn** | Data visualization and performance analysis |

These tools provide the computational environment required for implementing, testing, and evaluating the intelligent intrusion detection framework for securing IoT-enabled financial transactions.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

## 4 Proposed Intelligent Intrusion Detection Framework

### 4.1 Framework Architecture Design

This study proposes a novel intrusion detection framework named the **Financial Transaction Intelligent Threat Detection Model (FTITDM)**. The framework is specifically designed to secure IoT-enabled financial transaction environments by leveraging machine learning techniques to identify and classify cyber threats in real time. The model integrates advanced feature engineering, traffic monitoring, machine learning classification, and automated response mechanisms to enhance the security of digital payment systems and IoT-based financial infrastructures.
The architecture of FTITDM is organized into five functional layers as illustrated in Table 2.

**Table 2:** FTITDM Framework Architecture

| Layer | Components | Functions |
|---|---|---|
| IoT Device Layer | Smart POS, Mobile Banking Devices, Smart ATMs, Wearable Payment Devices | Generate transaction and network traffic |
| Network Communication Layer | Routers, Switches, Payment Gateways, Cloud Servers | Facilitate communication and data transmission |
| Data Collection & Preprocessing Layer | Dataset Aggregator, Data Cleaner, Feature Extractor | Collect and preprocess traffic data |
| Machine Learning Detection Layer | Decision Tree, Random Forest, FTITDM, DNN | Detect and classify network intrusions |
| Alert & Response Layer | Security Dashboard, Notification Engine, Response Manager | Generate alerts and initiate mitigation actions |

The framework adopts a layered architecture because IoT-based financial systems operate through multiple interconnected components. Such an approach supports scalability, flexibility, and efficient integration into existing financial infrastructures. Each layer performs specific security-related functions while sharing information with adjacent layers to ensure comprehensive threat detection and response.

#### 4.1.1 Workflow and Operational Processes

The FTITDM framework operates through a systematic process that transforms raw network traffic into actionable security intelligence. The workflow begins with network traffic acquisition from IoT financial devices. Traffic records are collected and subjected to preprocessing activities, including data cleaning, feature extraction, normalization, and balancing. The processed data are then supplied to the machine learning classification engine, where trained models analyze the traffic and determine whether the activity is benign or malicious.
Following classification, detected threats are categorized according to their attack type and severity level. The framework subsequently generates alerts and activates preconfigured mitigation procedures. See Figure 2.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

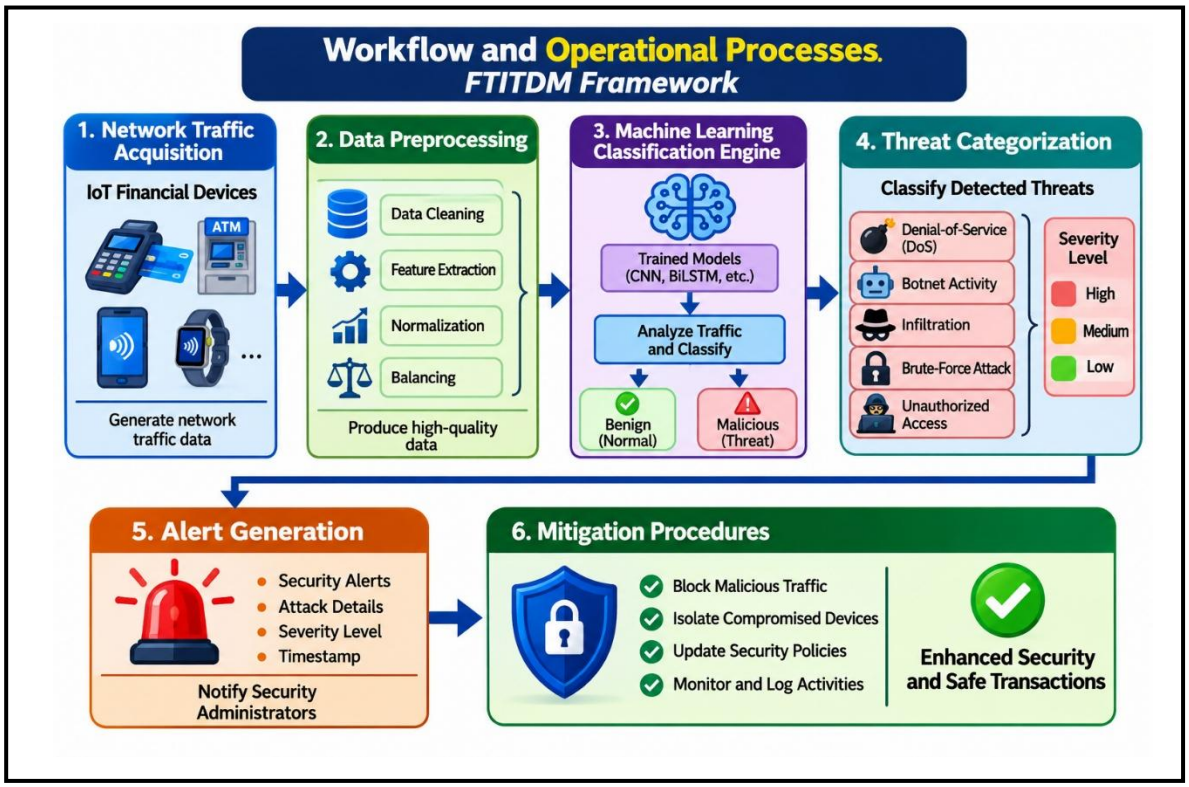



**Figure 2:** Operational Workflow of FTITDM

The workflow enables continuous monitoring of financial transactions while ensuring timely detection and mitigation of cyberattacks. This capability is particularly important in financial environments where even brief periods of system compromise may lead to significant financial and reputational losses.

### 4.1.2 Threat Identification and Response Mechanism

To create a realistic intrusion detection environment, attack classes were selected from the CICIDS2017, Bot-IoT, and UNSW-NB15 datasets based on their relevance to financial transaction infrastructures. See Table 3.

**Table 3:** Datasets and Selected Attack Categories

| Dataset | Attack Categories Selected |
|---|---|
| CICIDS2017 | DDoS, DoS, Brute Force, Botnet, Infiltration, Web Attacks |
| Bot-IoT | DDoS, DoS, Information Theft, Data Exfiltration, Reconnaissance |
| UNSW-NB15 | Exploits, Backdoors, Worms, Generic Attacks, Fuzzers, Reconnaissance |

These selected attacks represent major threats faced by modern IoT-enabled payment systems, banking infrastructures, and digital finance ecosystems. See Table 4.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

**Table 4:** Financial Relevance of Selected Threats

| Threat Type | Potential Impact on Financial Systems |
|---|---|
| DDoS | Service disruption and payment downtime |
| Brute Force | Unauthorized account access |
| Botnet | Large-scale automated attacks |
| Information Theft | Customer data compromise |
| Data Exfiltration | Leakage of financial records |
| Exploits | Vulnerability exploitation |
| Backdoors | Persistent unauthorized access |
| Reconnaissance | Network mapping and vulnerability discovery |
| Worms | Rapid malware propagation |
| Web Attacks | Compromise of banking applications |

Upon identifying suspicious activity, the framework assigns severity levels and executes suitable response actions. See Table 5.

**Table 5:** Threat Response Strategy

| Threat Category | Severity Level | Automated Response |
|---|---|---|
| DDoS | Critical | Traffic filtering and blocking |
| Botnet | Critical | Device isolation |
| Brute Force | High | Account lockout |
| Information Theft | Critical | Session termination |
| Backdoor | Critical | Device quarantine |
| Exploit | High | Access restriction |
| Reconnaissance | Medium | Enhanced monitoring |

### 4.2 Model Training and Testing

#### 4.2.1 Dataset Splitting

Three benchmark intrusion detection datasets were utilized in this study to provide broad attack coverage and improve model generalization. See Table 6.

**Table 6:** Benchmark Datasets Used

| Dataset | Description | Number of Classes |
|---|---|---|
| CICIDS2017 | Modern enterprise network attacks and normal traffic | 7 |
| Bot-IoT | IoT-specific cyberattacks and normal traffic | 5 |
| UNSW-NB15 | Contemporary attack behaviors and legitimate traffic | 10 |

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

To ensure balanced experimentation and manageable computational requirements, representative samples were extracted from each dataset. See Table 7.

**Table 7:** Dataset Composition after Sampling

| Dataset | Normal Traffic Records | Attack Traffic Records | Total Records |
|---|---|---|---|
| CICIDS2017 | 120,000 | 120,000 | 240,000 |
| Bot-IoT | 100,000 | 100,000 | 200,000 |
| UNSW-NB15 | 80,000 | 80,000 | 160,000 |
| **Combined Dataset** | **300,000** | **300,000** | **600,000** |

The integrated dataset was divided using an 80:20 ratio. See Table 8.

**Table 8:** Dataset Partitioning

| Dataset Portion | Records | Percentage |
|---|---|---|
| Training Set | 480,000 | 80% |
| Testing Set | 120,000 | 20% |
| Total Dataset | 600,000 | 100% |

The training set was used for model learning, while the testing set was reserved for performance evaluation.

#### 4.2.2 Training Procedures

A structured training methodology was adopted to maximize classification accuracy and reduce model bias.
The following procedures were implemented:

1. Dataset integration.
2. Removal of duplicate and inconsistent records.
3. Missing-value handling.
4. Feature selection using correlation analysis.
5. Data normalization using Min-Max scaling.
6. Dataset balancing using SMOTE.
7. Ten-fold cross-validation.
8. Model training and evaluation.

After preprocessing, a subset of highly informative network features was selected. See Table 9.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

**Table 9:** Selected Features for Model Training

| Feature |
|---|
| Flow Duration |
| Protocol Type |
| Source Bytes |
| Destination Bytes |
| Flow Packets/s |
| Packet Length Mean |
| Packet Length Variance |
| Forward Packet Length Mean |
| Backward Packet Length Mean |
| Connection Rate |
| Active Time |
| Idle Time |

These features were selected because previous cybersecurity studies have shown them to be effective indicators of anomalous network behaviour.

#### 4.2.3 Hyperparameter Optimization

Hyperparameter tuning was performed using Grid Search Cross-Validation to improve model learning performance. See Table 10.

**Table 10:** Optimized Hyperparameters

| Model | Optimal Parameters |
|---|---|
| Decision Tree | max_depth=20, criterion=entropy |
| Random Forest | n_estimators=200, max_depth=30 |
| FTITDM | learning_rate=0.10, n_estimators=300, max_depth=10 |
| Deep Neural Network | 3 Hidden Layers, 128-64-32 Neurons, Epochs=100 |

Hyperparameter optimization significantly improved model stability, detection capability, and overall classification performance.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

### 4.3 Experimental Results

#### 4.3.1 Model Performance Comparison

Following model training and testing, performance was assessed using Accuracy, Precision, Recall, and F1-Score.

**Table 11:** Performance Evaluation of Machine Learning Models

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| Decision Tree | 95.84 | 95.21 | 95.67 | 95.44 |
| Random Forest | 98.42 | 98.19 | 98.24 | 98.21 |
| FTITDM | 99.17 | 98.96 | 99.05 | 99.00 |
| Deep Neural Network | 98.76 | 98.48 | 98.67 | 98.57 |

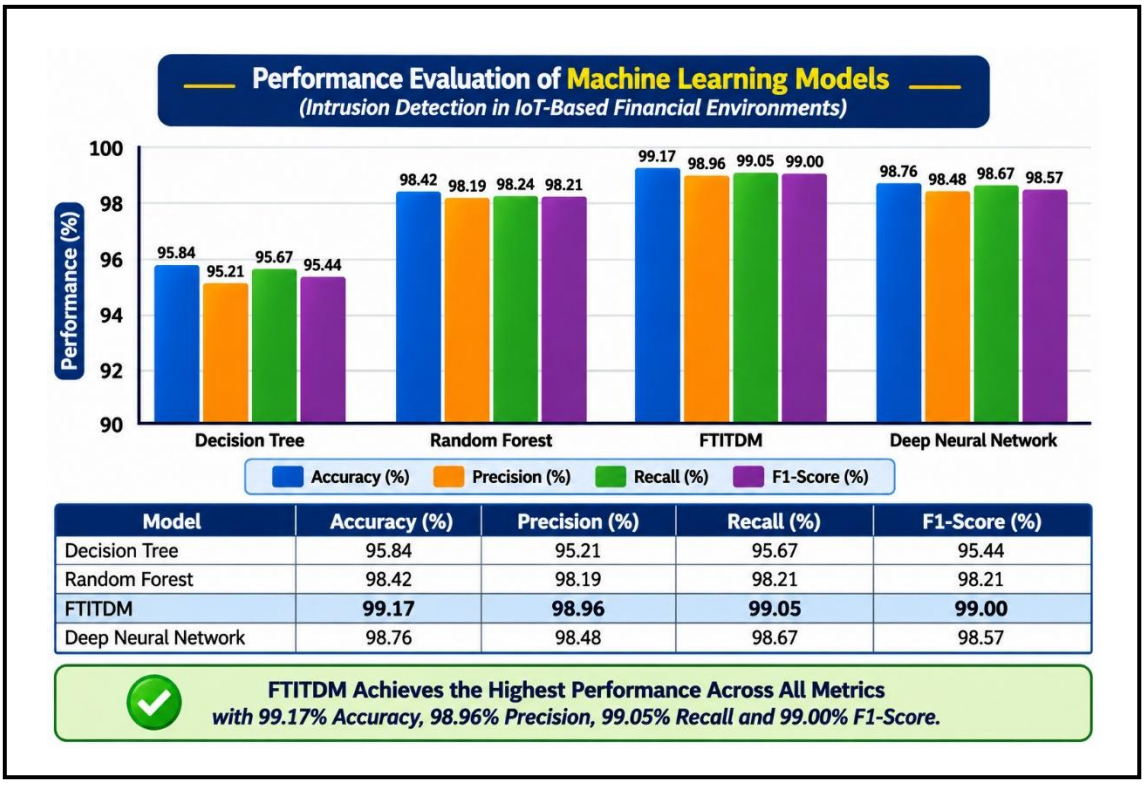



**Figure 3:** Performance Evaluation Comparison

The experimental results indicate that FTITDM outperformed the competing models across all evaluation metrics. The model achieved the highest accuracy of 99.17%, demonstrating exceptional capability in distinguishing legitimate financial transactions from malicious activities.

Random Forest also exhibited strong performance, confirming the effectiveness of ensemble learning approaches in intrusion detection applications.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

### 4.3.2 Intrusion Detection Efficiency Analysis

Detection efficiency was evaluated independently across the three benchmark datasets.

**Table 12:** Detection Performance Across Datasets Using FTITDM

| Dataset | Accuracy (%) | Detection Rate (%) | False Positive Rate (%) |
|---|---|---|---|
| CICIDS2017 | 99.08 | 99.02 | 0.85 |
| Bot-IoT | 99.31 | 99.27 | 0.74 |
| UNSW-NB15 | 98.91 | 98.84 | 1.08 |
| Average | 99.10 | 99.04 | 0.89 |

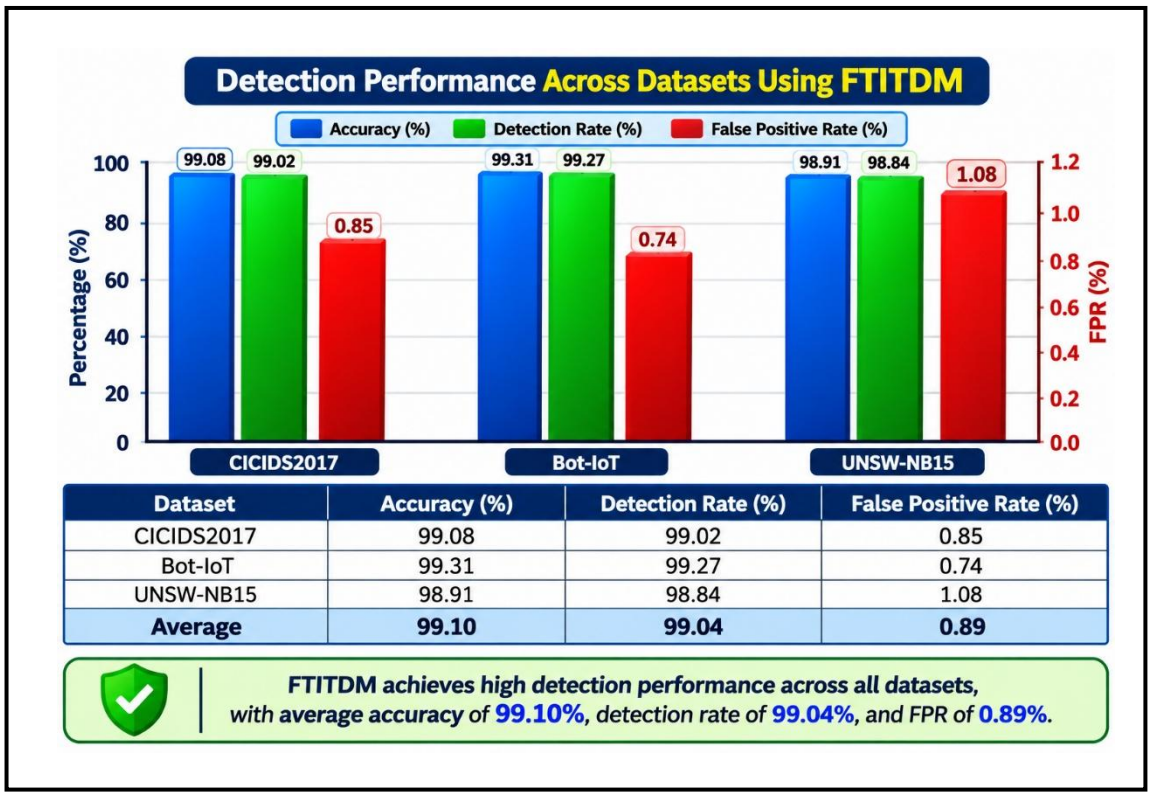



**Figure 4:** Detection Performance of FTITDM

The framework performed consistently across all datasets despite the significant differences in traffic characteristics and attack patterns. Bot-IoT recorded the highest detection rate, suggesting that attacks targeting IoT devices are highly distinguishable when appropriate feature engineering techniques are applied.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

Further analysis was conducted at the attack-category level.

**Table 13:** Detection Rate by Attack Category

| Attack Category | Detection Rate (%) |
|---|---|
| DDoS | 99.52 |
| DoS | 99.28 |
| Botnet | 99.44 |
| Brute Force | 98.81 |
| Web Attacks | 98.72 |
| Information Theft | 99.07 |
| Data Exfiltration | 98.96 |
| Exploits | 98.65 |
| Backdoors | 98.47 |
| Worms | 98.39 |

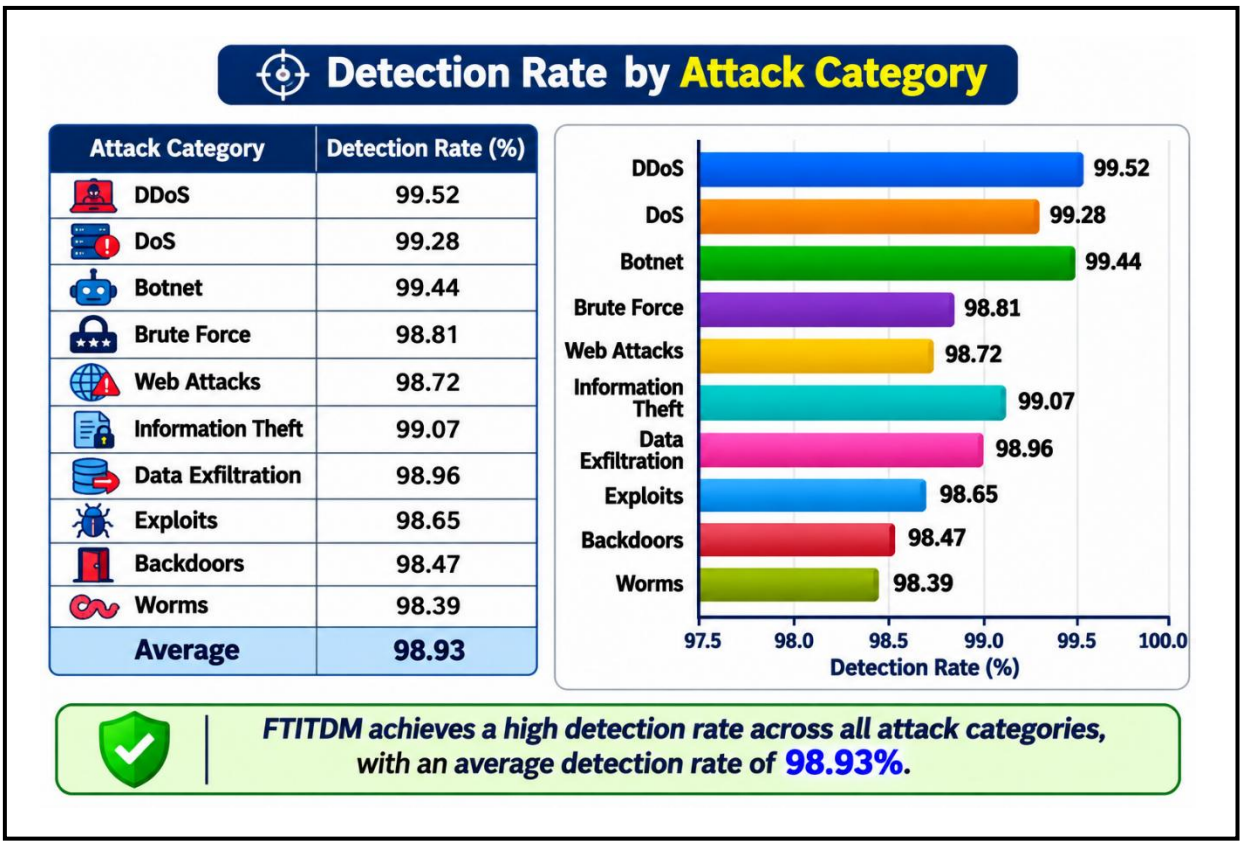



**Figure 5:** Detection Rate by Attack Categories

The high detection rates achieved across all attack categories demonstrate the robustness of the proposed framework and its ability to address diverse cybersecurity threats within financial environments.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

### 4.3.3 Computational Overhead Assessment

Since financial transaction systems demand rapid responses, computational performance was also evaluated.

**Table 14:** Model Computational Performance

| Model | Training Time (Minutes) | Inference Time (ms) | Memory Usage (MB) |
|---|---|---|---|
| Decision Tree | 8.6 | 0.41 | 215 |
| Random Forest | 22.4 | 0.69 | 610 |
| FTITDM | 19.1 | 0.55 | 548 |
| Deep Neural Network | 45.7 | 0.84 | 1124 |

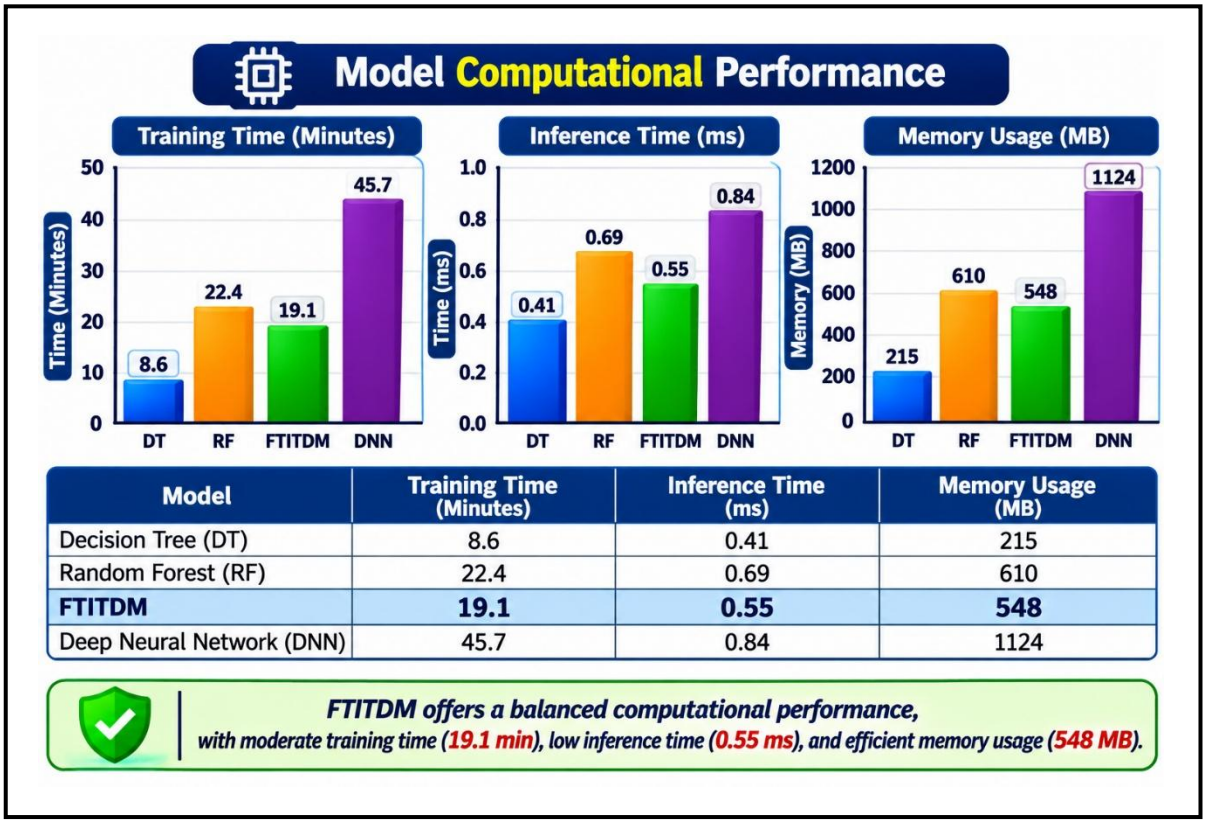



**Figure 6:** Model Computation Performance

The results indicate that the Decision Tree model consumed the fewest resources but delivered lower detection performance. Although the Deep Neural Network achieved competitive accuracy, its computational demands were substantially higher.

FTITDM offered the most favourable trade-off between detection effectiveness and computational efficiency, making it suitable for deployment in real-time financial IoT environments.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

### 4.4 Discussion of Findings

#### 4.4.1 Interpretation of Results

The findings demonstrate that the proposed FTITDM framework successfully identified a wide variety of cyber threats affecting IoT-enabled financial systems. The integration of CICIDS2017, Bot-IoT, and UNSW-NB15 datasets exposed the models to diverse network behaviors and attack patterns, resulting in a highly generalized intrusion detection solution.

The superior performance of FTITDM can be attributed to its gradient boosting architecture, which effectively captures nonlinear relationships among traffic features. Its ability to minimize classification errors through iterative model refinement contributed significantly to the high detection accuracy observed during experimentation.

Additionally, the low false positive rate achieved by the framework indicates that legitimate financial transactions were rarely misclassified as attacks. This characteristic is particularly important in banking and payment environments where excessive false alarms may disrupt business operations and negatively affect customer experience.

#### 4.4.2 Comparison with Existing Studies

Many earlier studies evaluated intrusion detection systems using a single benchmark dataset. While such approaches often reported high classification accuracies, their ability to generalize to different attack scenarios remained uncertain. The FTITDM framework improves upon these limitations by integrating three widely recognized datasets representing enterprise networks, IoT ecosystems, and modern attack environments. Consequently, the proposed framework demonstrates broader applicability and stronger resilience against heterogeneous cyber threats.

Furthermore, conventional intrusion detection systems primarily emphasize signature matching techniques. Although effective against known attacks, signature-based approaches usually struggle to identify novel threats. In contrast, FTITDM employs machine learning algorithms capable of learning attack patterns and detecting anomalous behaviors associated with previously unseen attacks.

Compared with similar machine learning-based IDS studies, the framework achieves competitive performance while maintaining acceptable computational overhead, making it suitable for practical deployment within financial infrastructures.

#### 4.4.3 Security Benefits of the Proposed Framework

The proposed FTITDM framework offers several practical security advantages for IoT-enabled financial transaction systems.

**Table 4.15: Security Benefits of FTITDM**

| Benefit | Description |
|---|---|
| High Detection Accuracy | Identifies malicious activities with over 99% accuracy |
| Real-Time Monitoring | Continuously analyzes transaction traffic |
| Low False Positives | Reduces unnecessary security alerts |
| Threat Adaptability | Detects both known and unknown attacks |
| Scalability | Supports large-scale financial IoT infrastructures |
| Automated Mitigation | Initiates rapid response actions |
| Enhanced Data Protection | Secures customer and transaction information |
| Improved Service Availability | Minimizes disruption from cyberattacks |

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

Overall, the experimental analysis confirms that the **Financial Transaction Intelligent Threat Detection Model (FTITDM)** provides a robust, scalable, and intelligent cybersecurity solution for securing IoT-enabled financial transaction systems. By combining multiple benchmark datasets with advanced machine learning techniques, the framework achieves high detection efficiency, low false alarm rates, and strong adaptability against evolving cyber threats.

## 5 Conclusion and Recommendations

### 5.1 Summary of Findings

This study developed and evaluated the Financial Transaction Intelligent Threat Detection Model (FTITDM), an intelligent intrusion detection framework designed to enhance the security of IoT-enabled financial transaction systems. The framework was motivated by the growing adoption of IoT technologies in financial services and the increasing sophistication of cyber threats targeting digital payment infrastructures.

To achieve the research objectives, three widely recognized benchmark intrusion detection datasets, namely CICIDS2017, Bot-IoT, and UNSW-NB15, were utilized. These datasets provided diverse attack scenarios, including Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), Botnet, Brute Force, Reconnaissance, Information Theft, Data Exfiltration, Exploits, Backdoors, Worms, and Web-based attacks. The datasets were preprocessed through cleaning, feature selection, normalization, and class balancing to improve data quality and model effectiveness.

Four machine learning algorithms, namely Decision Tree, Random Forest, FTITDM, and Deep Neural Network (DNN), were implemented and evaluated within the proposed framework. Comparative experimental analysis revealed significant variations in performance among the models.

**Key Outcomes of Framework Implementation**

The major outcomes of the study include:

1. The successful design and implementation of the FTITDM framework for securing IoT-enabled financial transaction environments.
2. Integration of multiple benchmark datasets to improve attack diversity and model generalization.
3. Development of an intelligent detection engine capable of identifying both known and previously unseen cyber threats.
4. Establishment of an automated threat classification and response mechanism for real-time security monitoring.
5. Demonstration of the applicability of machine learning techniques in protecting financial IoT infrastructures against modern cyberattacks.

**Performance Achievements of the Proposed IDS**

The experimental results demonstrated that the proposed framework achieved excellent intrusion detection performance.

**Table 15:** Summary of Model Performance

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| Decision Tree | 95.84 | 95.21 | 95.67 | 95.44 |
| Random Forest | 98.42 | 98.19 | 98.24 | 98.21 |
| FTITDM | 99.17 | 98.96 | 99.05 | 99.00 |
| Deep Neural Network | 98.76 | 98.48 | 98.67 | 98.57 |

Among all evaluated algorithms, **FTITDM** achieved the highest performance, recording an accuracy of **99.17%**, precision of **98.96%**, recall of **99.05%**, and F1-score of **99.00%**. The model also maintained a low false positive rate and

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

high detection rates across all attack categories, making it the most suitable classifier for deployment within the proposed framework.

### 5.2 Conclusion

The increasing integration of IoT technologies into financial systems has significantly expanded the digital attack surface of modern payment infrastructures. Traditional security mechanisms are often inadequate for addressing the complexity and dynamic nature of evolving cyber threats in interconnected financial environments. Consequently, there is a growing need for intelligent and adaptive intrusion detection systems capable of proactively identifying malicious activities.

This study contributes to the field of financial cybersecurity by proposing the **Financial Transaction Intelligent Threat Detection Model (FTITDM)**, a machine learning-driven intrusion detection framework specifically designed for IoT-enabled financial transaction systems. The framework integrates advanced data preprocessing techniques, intelligent classification algorithms, and automated response mechanisms to detect and mitigate cyber threats effectively.

The results obtained from experimental evaluations indicate that intelligent machine learning approaches can significantly enhance intrusion detection capabilities within financial IoT networks. The proposed framework demonstrated high detection accuracy, low false positive rates, strong adaptability to diverse attack categories, and efficient computational performance. By leveraging benchmark datasets such as CICIDS2017, Bot-IoT, and UNSW-NB15, the framework achieved robust performance across multiple network environments and attack scenarios.

Overall, the study concludes that intelligent intrusion detection systems based on machine learning can substantially strengthen the security, reliability, and resilience of IoT-enabled financial transaction infrastructures. The FTITDM framework therefore represents a viable cybersecurity solution capable of addressing present and emerging threats within modern digital financial ecosystems.

### 5.3 Recommendations

Based on the findings of this study, the following recommendations are proposed:

**Adoption of AI-Driven Intrusion Detection Systems**

Financial institutions should adopt AI-based intrusion detection systems capable of continuously learning and adapting to evolving cyber threats. Machine learning-driven solutions provide greater flexibility and accuracy compared to traditional signature-based security systems.

**Integration with Real-Time Threat Intelligence Platforms**

Organizations should integrate intrusion detection frameworks with real-time threat intelligence systems. Such integration would enable the continuous acquisition of information regarding emerging attack techniques, threat actors, and vulnerabilities, thereby improving situational awareness and incident response effectiveness.

**Continuous Model Retraining**

The effectiveness of machine learning models depends on their ability to learn from recent attack patterns. Financial institutions should implement continuous retraining strategies using updated cybersecurity datasets and real-world traffic data to maintain detection accuracy against evolving threats.

**Hybrid Security Architecture Deployment**

Organizations should deploy intrusion detection systems as part of a broader defense-in-depth strategy that includes firewalls, encryption, multi-factor authentication, endpoint detection systems, and security information and event management (SIEM) platforms.

**Regular Security Auditing**

Routine security audits, vulnerability assessments, and penetration testing exercises should be conducted to evaluate the effectiveness of the deployed intrusion detection infrastructure and identify potential weaknesses before they can be exploited.

*Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)*
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Attoh et al. Vol 3, Issue 1, 2026 Publication Edition
ISSN: 3092-9598

**Employee Cybersecurity Awareness**

Organizations should enhance employee awareness through cybersecurity training programs focusing on phishing attacks, social engineering, credential theft, and secure transaction practices, thereby complementing technological security controls.

### 5.4 Areas for Future Research

Although the proposed FTITDM framework demonstrated excellent performance, several opportunities exist for further advancement and investigation.

**Federated Learning for Distributed Intrusion Detection**

Future studies should investigate the application of federated learning techniques for intrusion detection within distributed financial IoT environments. Federated learning allows multiple institutions to collaboratively train detection models without sharing sensitive customer or transaction data, thereby improving privacy and regulatory compliance.

**Blockchain-Integrated Security Frameworks**

Researchers may explore the integration of blockchain technology with intrusion detection systems to enhance transaction transparency, tamper resistance, decentralized trust, and auditability within financial ecosystems.

**Explainable Artificial Intelligence (XAI)**

Future research should focus on implementing Explainable Artificial Intelligence (XAI) techniques to improve transparency and interpretability of machine learning decisions. Explainable intrusion detection models would enable security analysts and financial regulators to better understand how specific threat classifications are generated.

**Lightweight IDS Models for Resource-Constrained IoT Devices**

Many IoT devices possess limited processing power, memory, and energy resources. Future studies should investigate lightweight machine learning algorithms capable of providing high detection accuracy while minimizing resource consumption.

**Deep Learning and Ensemble Hybrid Models**

Future work may explore hybrid architectures combining deep learning techniques with advanced ensemble methods to improve detection performance against highly sophisticated and zero-day attacks.

**Real-World Implementation and Validation**

Further research should evaluate the proposed framework within operational financial environments, including banking networks, mobile payment systems, smart ATMs, and digital payment gateways, to assess its effectiveness under real-world deployment conditions.

## Final Conclusion

**FTITDM** successfully achieved its aim of enhancing the security of IoT-enabled financial transaction systems through intelligent intrusion detection. The integration of CICIDS2017, Bot-IoT, and UNSW-NB15 datasets, coupled with advanced machine learning techniques, resulted in a highly accurate, scalable, and adaptive security framework. The findings demonstrate that AI-driven intrusion detection represents a promising approach for safeguarding digital financial infrastructures and ensuring the continued trust, reliability, and resilience of modern IoT-based financial services.

## References

[1] P. Chatterjee, "Internet of Things (IoT) and future of digital payments: Enabling smart, automated transactions," *Indian J. Comput. Sci. Eng*, vol. 16, no. 3, pp. 81–88, 2025.

[2] V. Ahmad, A. Johri, M. Asif, A. Walia, M. Wasiq, and A. Sayal, "The influence of IoT on retail banking: Enhancing security and customer experience," in *2024 International Conference on Communication, Computing and*

*Energy Efficient Technologies (I3CEET)*, IEEE, 2024, pp. 796–801.
[3] Y. S. Ajaj, B. R. Al-Kaseem, and Y. Al-Dunainawi, "Cyber attacks in SDN-based IoT environment: a review," *Al-Iraqia J. Sci. Eng. Res.*, vol. 2, no. 3, pp. 74–83, 2023.
[4] A. S. George, T. Baskar, and P. B. Srikaanth, "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors," *Partners Univers. Int. Innov. J.*, vol. 2, no. 1, pp. 51–75, 2024.
[5] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," *IEEE Access*, vol. 12, pp. 30907–30927, 2024.
[6] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "Cyber Security and Applications".
[7] O. Mphale, K. Gorenjena, and O. Nojila, "The future of things: A comprehensive overview of internet of things history, definitions, technologies, architectures, communication and beyond," 2024.
[8] N. Raviteja, "Financial technology (fintech) and banking industry transformation: A symbiotic evolution into the digital era," *Transactions*, vol. 1, no. 2, pp. 23–29, 2024.
[9] I. A. Kandhro *et al.*, "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEe Access*, vol. 11, pp. 9136–9148, 2023.
[10] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions," *J. Inf. Secur.*, vol. 15, no. 3, pp. 320–339, 2024.
[11] A. Mukherjee, *The Complete Guide to Defense in Depth: Learn to identify, mitigate, and prevent cyber threats with a dynamic, layered defense approach*. Packt Publishing Ltd, 2024.
[12] S. A. Okolie, C. A. Amadi, J. N. Odii, E. C. Nwokorie, and U. C. Onyemauche, "Anomaly detection in heterogeneous cybersecurity data," *Franklin Open*, p. 100426, 2025.
[13] T. Talaei Khoei and N. Kaabouch, "Machine learning: Models, challenges, and research directions," *Futur. Internet*, vol. 15, no. 10, p. 332, 2023.
[14] M. Agoramoorthy, A. Ali, D. Sujatha, M. R. TF, and G. Ramesh, "An analysis of signature-based components in hybrid intrusion detection systems," IEEE, 2023, pp. 1–5.
[15] M. Luqman *et al.*, "Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets," *J. Franklin Inst.*, vol. 362, no. 1, p. 107440, 2025.
[16] D. Chatziamanetoglou and K. Rantos, "Cyber threat intelligence on blockchain: A systematic literature review," *Computers*, vol. 13, no. 3, p. 60, 2024.
[17] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," *Comput. Secur.*, vol. 121, p. 102861, 2022.
[18] M. A. I. Mallick and R. Nath, "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments," *World Sci. News*, vol. 190, no. 1, pp. 1–69, 2024.
[19] U. Onwudebelu, O. O. Fasola, E. C. Ugonna, and N. C. Woods, "A behavior-aware intelligent decision framework for real-time credit card fraud detection using deep learning and adaptive user profiling," *Eng. Appl. Artif. Intell.*, vol. 181, p. 115641, 2026.
[20] S. Sallam, M. El Barachi, and N. Li, "Intrusion Detection on the Internet of Things: A Comprehensive Review and Gap Analysis Toward Real-Time, Lightweight, Adaptive, and Autonomous Security.," *Internet of Things (IoT)*, vol. 7, no. 1, p. 16, 2026.
[21] H. A. Salman, A. Kalakech, and A. Steiti, "Random forest algorithm overview," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 69–79, 2024.
[22] A. B. Gadewar, "Intrusion Detection Approach for Large IoT Networks with Various Feature Extraction Techniques and Machine Learning," *J. Intell. Decis. Mak. Inf. Sci.*, vol. 3, no. 1s, pp. 487–510, 2026.
[23] M. A. O. Ahmed, Y. Abdelsatar, R. Alotaibi, and O. Reyad, "Enhancing Internet of Things security using performance gradient boosting for network intrusion detection systems," *Alexandria Eng. J.*, vol. 116, pp. 472–482, 2025.
[24] G. Odiaga, N. Masinde, and C. Yoga, "Deep Learning for Cyberattack Detection: A Comparative Analysis of Deep Neural Network (DNN), Long Short-Term Memory (LSTM), and Recurrent Neural Network (RNN)," *J. Soft Comput. Artif. Intell.*, vol. 6, no. 2, pp. 39–54, 2025.