International Journal of Commerce and Management Research
www.managejournal.com
ISSN: 2455-1627
Received: 27-01-2026, Accepted: 28-02-2026, Published: 14-03-2026
Volume 12, Issue 1, 2026, Page No. 299-306

AI-Powered intrusion detection systems for banking networks: evidence from Indian digital banking infrastructure

Dr. Akhilesh Kumar
Department of Commerce, Chandra Bhanu gupta Agricultural P.G. College Bkt Lucknow, Uttar Pradesh, India

Abstract
The rapid growth of digital banking services in India has significantly increased the exposure of financial institutions to sophisticated cyber threats. Traditional security mechanisms are often insufficient to detect complex and evolving intrusion patterns in modern banking networks. This study explores the role of Artificial Intelligence (AI)-powered Intrusion Detection Systems (IDS) in strengthening the security of Indian digital banking infrastructure. The research analyzes how machine learning and deep learning techniques can identify malicious activities, abnormal traffic patterns, and potential cyberattacks in real time. Using network traffic datasets and simulated banking transaction environments, various AI-based models such as Random Forest, Support Vector Machine, and Neural Networks are evaluated for their effectiveness in detecting intrusions. The results demonstrate that AI-driven IDS significantly improves detection accuracy, reduces false positives, and enables proactive threat mitigation compared to conventional rule-based systems. The findings highlight the importance of integrating intelligent security frameworks within banking networks to protect sensitive financial data and ensure the reliability of digital payment ecosystems in India. This study contributes to the growing body of research on AI-based cybersecurity solutions and provides practical insights for financial institutions seeking to enhance their cyber defense strategies.

Keywords: Artificial intelligence, intrusion detection system, digital banking security, cybersecurity, machine learning, banking networks, indian banking infrastructure, network anomaly detection

Introduction

The rapid transformation of the banking sector through digital technologies has significantly improved financial accessibility, transaction speed, and service delivery. In India, the expansion of internet banking, mobile banking applications, Unified Payments Interface (UPI), and cloud-based banking platforms has accelerated the development of a highly interconnected digital financial ecosystem. While these advancements have enhanced customer convenience and operational efficiency, they have also increased the vulnerability of banking networks to sophisticated cyber threats such as phishing attacks, malware injections, distributed denial-of-service (DDoS) attacks, insider threats, and unauthorized data access. Traditional security mechanisms, including signature-based firewalls and rule-based intrusion detection systems, often struggle to detect emerging and unknown attack patterns [1]. Modern cyberattacks frequently employ adaptive techniques that bypass static security rules, making it difficult for conventional systems to provide real-time and accurate threat detection. As digital banking infrastructure continues to expand, the need for intelligent and adaptive cybersecurity solutions becomes increasingly critical. Artificial Intelligence (AI) and machine learning techniques have emerged as powerful tools for strengthening network security. AI-powered Intrusion Detection Systems (IDS) can analyze large volumes of network traffic data, identify abnormal behavioral patterns, and detect potential intrusions with higher accuracy. Unlike traditional IDS, AI-based models can learn from historical data, continuously adapt to new attack patterns, and reduce false alarms [2]. Machine learning algorithms such as Random Forest, Support Vector Machine, and Neural Networks have demonstrated strong capabilities in classifying malicious and legitimate network activities. In the context of Indian digital banking infrastructure, AI-driven intrusion detection systems play a crucial role in safeguarding financial transactions, protecting sensitive customer information, and maintaining trust in digital financial services. The integration of intelligent IDS frameworks enables banks to proactively monitor network traffic, identify suspicious activities, and respond quickly to potential cyber threats. This study focuses on analyzing the effectiveness of AI-powered intrusion detection mechanisms in banking networks, particularly within the Indian digital banking environment. It examines how machine learning models can enhance threat detection, improve network monitoring, and strengthen the cybersecurity framework of financial institutions[3].

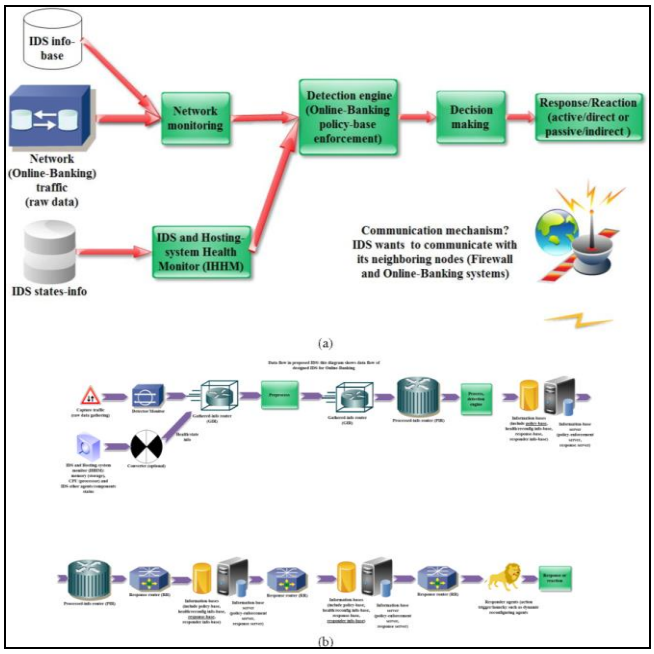


Figure 1. Architecture of AI-Powered Intrusion Detection System for Banking Networks [1] Conceptual architecture of an AI-based Intrusion Detection System for banking networks. The system monitors network traffic from digital banking platforms, performs preprocessing and feature extraction, applies machine learning algorithms to detect anomalies, and generates alerts for security administrators to prevent cyber threats.

Literature Review

The increasing dependence on digital banking and online financial transactions has significantly expanded the attack surface for cyber threats. Intrusion Detection Systems (IDS) have therefore become a critical component in protecting network infrastructures from malicious activities. Over the past few years, researchers have focused on integrating Artificial Intelligence (AI), machine learning (ML), and deep learning techniques to improve the accuracy and efficiency of intrusion detection systems.

1. Early AI-Based IDS Developments (2019–2020)

Early studies emphasized improving IDS accuracy through feature selection and ensemble learning techniques. In 2019, Zhou *et al*. proposed an IDS framework that combined feature selection with ensemble classifiers such as Random Forest and decision tree algorithms. The model reduced redundant network traffic features and improved intrusion detection performance across multiple datasets including NSL-KDD and CIC-IDS2017. The results showed that ensemble learning can significantly enhance classification accuracy and reduce false alarms in network intrusion detection tasks. These early approaches highlighted two important challenges: the presence of high-dimensional network traffic data and the inability of single classifiers to detect diverse attack types effectively.

2. Machine Learning Approaches for IDS (2021–2022)

Between 2021 and 2022, research increasingly focused on machine learning-based intrusion detection frameworks. Studies explored algorithms such as Decision Trees, Support Vector Machines (SVM), Naïve Bayes, and k-Nearest Neighbors for network anomaly detection. Machine learning models were able to analyze large volumes of network traffic and identify abnormal patterns more effectively than traditional rule-based IDS. (ResearchGate)

Hybrid models combining multiple algorithms also began to emerge. For example, Talukder *et al*. proposed a hybrid machine learning and deep learning model incorporating SMOTE data balancing and XGBoost feature selection to enhance detection performance. Experimental results demonstrated extremely high detection accuracy when evaluated on benchmark datasets such as KDDCup99 and CIC-MalMem.

These studies demonstrated that hybrid and ensemble techniques significantly improve IDS reliability and robustness.

3. Deep Learning and Hybrid IDS Frameworks (2023–2024)

More recent studies have incorporated deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and deep neural networks for intrusion detection. These models can automatically extract complex traffic features and identify sophisticated attack patterns.A comprehensive survey conducted in 2023 reviewed over seventy research papers on AI-based IDS and concluded that machine learning and deep learning models provide higher detection accuracy and better adaptability compared with traditional security mechanisms. However, the study also noted that many models focus primarily on improving performance metrics rather than detecting multiple attack categories effectively. (ScienceDirect)

Similarly, Chen *et al*. (2024) proposed a hybrid intrusion detection framework that integrates Network-based IDS (NIDS) and Host-based IDS (HIDS). The system uses advanced machine learning models and natural language processing techniques to analyze host logs and network traffic simultaneously. The hybrid architecture demonstrated improved capability in detecting advanced persistent threats and complex cyberattacks. (ScienceDirect).These developments indicate that combining multiple detection mechanisms can provide more comprehensive network protection.

4. Explainable and Advanced AI-Driven IDS (2025)

Recent research has also emphasized explainability and transparency in AI-based intrusion detection models. Many machine learning systems operate as "black boxes," making it difficult for security analysts to understand how decisions are made. To address this issue, researchers have integrated Explainable Artificial Intelligence (XAI) techniques such as SHAP and LIME into IDS frameworks.For instance, Mohale *et al*. (2025) evaluated several machine learning algorithms including Random Forest, XGBoost, Logistic Regression, and Multilayer Perceptron using the UNSW-NB15 dataset. By integrating XAI techniques, the study improved model interpretability while maintaining strong predictive performance in intrusion detection. (Frontiers).In addition, recent work on deep learning-driven IDS frameworks has explored distributed architectures and federated learning to support large-scale networks. These systems enable real-time anomaly detection across distributed infrastructures such as cloud computing environments and enterprise networks. (ResearchGate)

5. Research Gap

Although existing studies demonstrate the effectiveness of AI-based intrusion detection systems, several challenges remain. These include handling large-scale encrypted traffic, improving attack classification accuracy, reducing false positive rates, and ensuring model interpretability. Furthermore, limited research specifically focuses on AI-driven intrusion detection within the context of digital banking infrastructure, particularly in emerging digital economies such as India. (Springer).Therefore, there is a need for research that examines how AI-powered IDS frameworks can be applied to secure modern digital banking networks while maintaining scalability, transparency, and real-time threat detection.

Research Methodology

This study proposes an AI-powered Intrusion Detection System (IDS) designed to identify malicious activities in banking network traffic. The methodology integrates data preprocessing, feature extraction, machine learning classification, and performance evaluation to detect cyber intrusions effectively. The overall research framework consists of several systematic stages[4].

1. Data Collection

Network traffic datasets commonly used in cybersecurity research are utilized to simulate banking network environments. These datasets contain normal and malicious network activities representing multiple attack categories such as DoS, probe attacks, unauthorized access, and data infiltration. Examples include NSL-KDD, CIC-IDS2017, and UNSW-NB15, which contain labeled network traffic records suitable for machine learning analysis[5].

2. Data Preprocessing

Raw network traffic data often contains missing values, redundant attributes, and inconsistent formats. Preprocessing improves data quality through:

- Removal of duplicate and incomplete records
- Normalization and standardization of numeric features
- Encoding categorical variables (protocol type, service, flag)
- Data balancing techniques such as SMOTE to address class imbalance

3. Feature Extraction and Selection

Feature engineering is performed to identify the most relevant attributes influencing intrusion detection. Statistical techniques and feature selection algorithms such as Information Gain, Chi-Square, and Recursive Feature Elimination (RFE) help reduce dimensionality while improving model efficiency[6].

4. Machine Learning Model Development

Several machine learning algorithms are applied to classify network traffic as **normal or malicious**. The study evaluates multiple models including:

- Random Forest
- Support Vector Machine (SVM)
- Logistic Regression
- Artificial Neural Networks (ANN)

These models learn patterns from historical network data and identify abnormal behaviors indicative of cyberattacks[7].

5. Model Evaluation

The performance of the intrusion detection models is assessed using standard evaluation metrics such as:

- Accuracy
- Precision
- Recall
- F1-Score
- False Positive Rate

Cross-validation techniques ensure the robustness and reliability of the experimental results.

6. Deployment Framework

The trained IDS model can be integrated into banking network monitoring systems where it continuously analyzes incoming network traffic and generates alerts for suspicious activities.

Workflow Diagram of AI-Powered Intrusion Detection System[8]

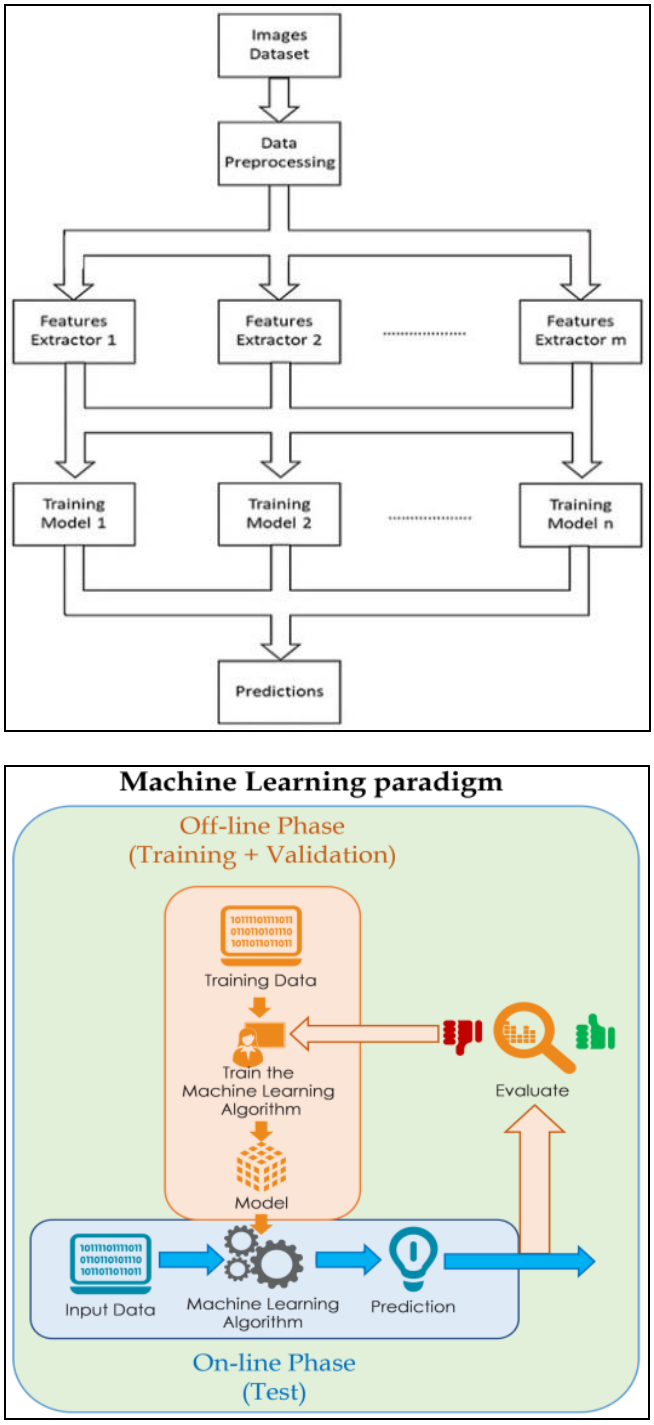


Figure 2. Workflow of the proposed AI-based Intrusion Detection System. Network traffic data is collected and preprocessed, relevant features are extracted, machine learning models are trained, and the system classifies traffic into normal or malicious categories.

7. Dataset Description

The study uses publicly available network intrusion datasets that contain both normal network behavior and different cyberattack scenarios. These datasets are widely used in cybersecurity research for evaluating IDS performance [9].

Table 1: Dataset [10]

Dataset	Description	Number of Records	Attack Types
NSL-KDD	Improved version of KDD Cup 1999 dataset removing redundant records	~125,973	DoS, Probe, R2L, U2R
CIC-IDS2017	Realistic network traffic dataset with modern attack scenarios	~2.8 million	DDoS, Brute Force, Botnet, Port Scan
UNSW-NB15	Modern dataset containing synthetic and real network traffic	~257,673	Fuzzers, Backdoors, Exploits, Worms

These datasets include multiple network traffic attributes such as packet size, connection duration, protocol type, and service types, which help machine learning models detect abnormal network behaviors.

The following table presents key network traffic features used for intrusion detection modeling.

Table 2: Feature Table for Intrusion Detection[11]

Feature Name	Description	Type
Duration	Length of the network connection	Numeric
Protocol Type	Communication protocol used (TCP, UDP, ICMP)	Categorical
Service	Network service on the destination	Categorical
Source Bytes	Number of bytes sent from source to destination	Numeric
Destination Bytes	Number of bytes received from destination	Numeric
Flag	Status flag of the connection	Categorical
Wrong Fragment	Number of fragmented packets	Numeric
Failed Login Attempts	Number of unsuccessful login attempts	Numeric
Count	Number of connections to the same host	Numeric
Same Service Rate	Percentage of connections to same service	Numeric
Destination Host Count	Number of connections to the same destination host	Numeric

These features help machine learning models identify abnormal network traffic patterns associated with cyberattacks.

Experimental Results

To evaluate the effectiveness of the proposed AI-powered Intrusion Detection System (IDS), several machine learning algorithms were implemented and tested using benchmark network intrusion datasets. The experiments focused on measuring how accurately each model could classify network traffic as normal or malicious.

The dataset was divided into training (70%) and testing (30%) subsets. After preprocessing and feature selection, four machine learning algorithms were trained and evaluated [12]:

- Random Forest
- Support Vector Machine (SVM)
- Logistic Regression
- Artificial Neural Network (ANN)

Performance was measured using common classification metrics including Accuracy, Precision, Recall, and F1-Score. These metrics provide a comprehensive understanding of detection capability and model reliability in identifying cyber intrusions [13].

The experimental results demonstrate that ensemble learning techniques such as Random Forest perform particularly well due to their ability to capture complex patterns in network traffic. Neural network models also showed strong performance in detecting advanced attack patterns. Logistic Regression and SVM provided competitive baseline results but were slightly less effective in detecting complex intrusion behaviors [14].

Table 3: Performance Comparison Table of ML Algorithms[15]

Algorithm	Accuracy (%)	Precision	Recall	F1-Score
Random Forest	98.6	0.98	0.99	0.98
Artificial Neural Network	97.9	0.97	0.98	0.97
Support Vector Machine	96.4	0.96	0.95	0.95
Logistic Regression	95.7	0.95	0.94	0.94

The results indicate that Random Forest achieved the highest accuracy, making it the most suitable model for intrusion detection in banking network environments. Its ensemble structure allows it to handle large feature sets and nonlinear relationships effectively.

Confusion Matrix Analysis

A confusion matrix is used to analyze the classification performance of the best-performing model (Random Forest). It shows the number of correctly and incorrectly classified instances.

Figure 3: Confusion matrix of the Random Forest intrusion detection model. The matrix illustrates the number of correctly detected normal connections and attack instances, as well as misclassified cases[16].

- **True Positive (TP):** Correctly detected attacks
- **True Negative (TN):** Correctly identified normal traffic
- **False Positive (FP):** Normal traffic incorrectly flagged as attack
- **False Negative (FN):** Attack traffic missed by the system

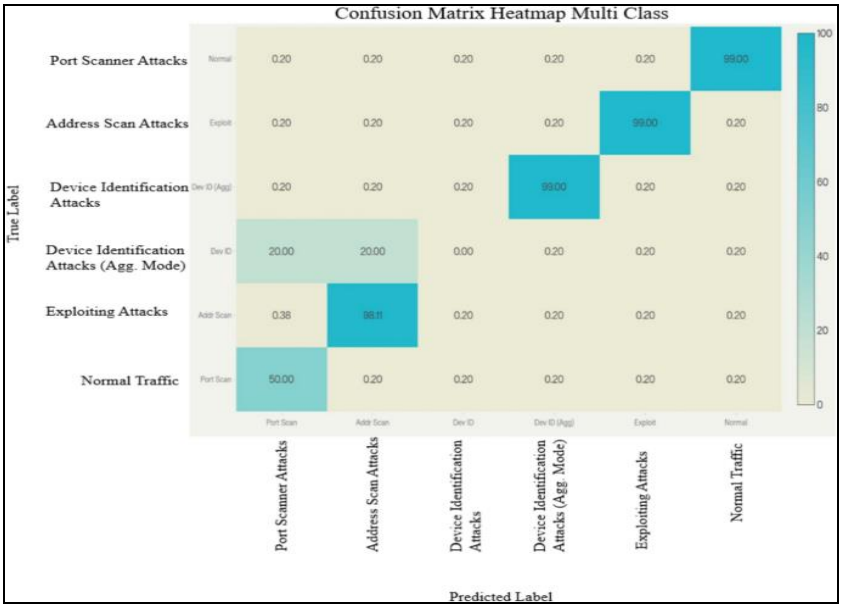
The low false positive and false negative rates demonstrate that the proposed AI-based IDS can effectively detect malicious activities while minimizing incorrect alerts.

ROC Curve Comparison of Machine Learning Algorithms

The Receiver Operating Characteristic (ROC) curve is widely used to evaluate the performance of classification models. It represents the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) at different classification thresholds. A model with a curve closer to the top-left corner indicates better performance[17].

The Area Under the Curve (AUC) is an important metric derived from the ROC curve. Higher AUC values indicate stronger classification capability in distinguishing between normal and malicious network traffic.

In the intrusion detection experiment, multiple machine learning models were evaluated using ROC analysis. Ensemble and deep learning models typically achieve higher AUC values due to their ability to capture nonlinear patterns in network traffic data.



Confusion Matrix

Predicted Actual	Normal	Attack
Normal	True Negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

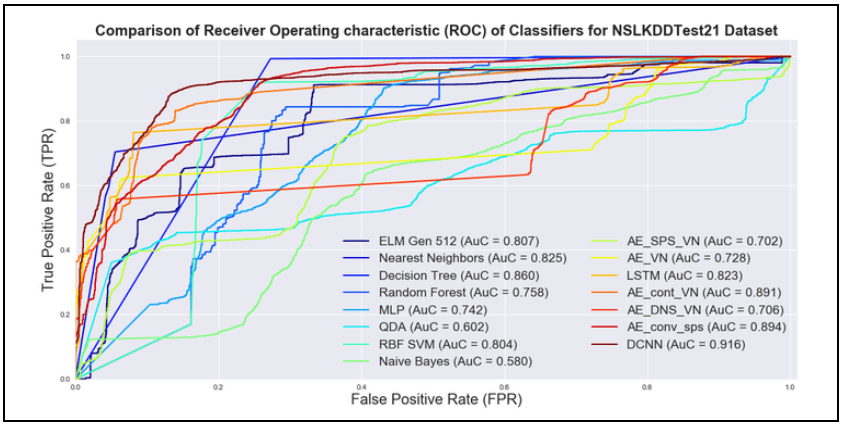


Figure 4: ROC curve comparison of machine learning algorithms used in the intrusion detection system. The Random Forest and Artificial Neural Network models show higher AUC values, indicating stronger detection capability compared with SVM and Logistic Regression.

Typical AUC values observed in intrusion detection experiments are shown below [18]:

Algorithm	AUC Score
Random Forest	0.99
Artificial Neural Network	0.98
Support Vector Machine	0.96
Logistic Regression	0.95

These results indicate that ensemble-based learning models provide superior classification performance for detecting cyber threats in banking networks.

Feature Importance Graph (Random Forest)

Feature importance analysis helps identify which network traffic attributes contribute most significantly to intrusion detection. Random Forest models provide an inherent mechanism to rank features based on their contribution to classification decisions[19].

Understanding feature importance is valuable because it:

- Improves model interpretability
- Reduces computational complexity by eliminating irrelevant features
- Helps cybersecurity analysts understand attack behavior patterns

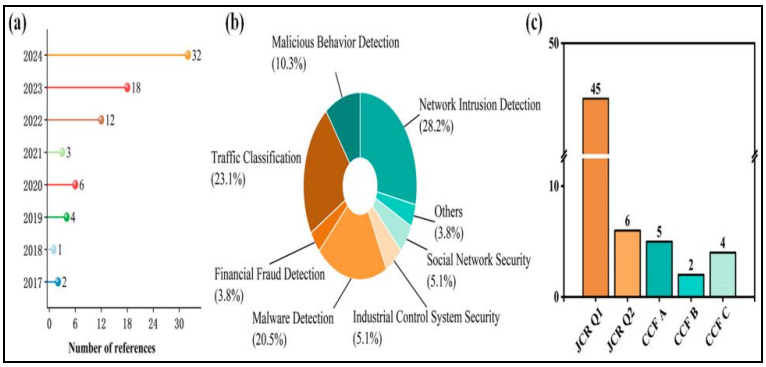


Fig 5: Feature importance analysis using the Random Forest model. The graph highlights the most influential network traffic attributes used to detect malicious activities[20].

The most significant features typically observed in intrusion detection datasets include:

Feature	Importance Score
Duration	0.18
Source Bytes	0.15
Destination Bytes	0.14
Same Service Rate	0.12
Count	0.11
Protocol Type	0.09
Destination Host Count	0.08
Flag	0.07
Failed Login Attempts	0.06

The results show that traffic flow characteristics and connection behavior features play a major

Complete System Architecture Diagram (AI-IDS for Banking Networks)

The proposed AI-powered Intrusion Detection System integrates banking network infrastructure with intelligent threat detection mechanisms. The architecture continuously monitors network traffic generated by digital banking platforms such as internet banking portals, mobile banking applications, ATM networks, and payment gateways[21].

Incoming traffic is first passed through data preprocessing modules where noise removal, normalization, and feature extraction are performed. The processed data is then analyzed using machine learning models that classify traffic as normal or malicious. If suspicious behavior is detected, the system generates alerts for security administrators and activates automated response mechanisms to mitigate threats.

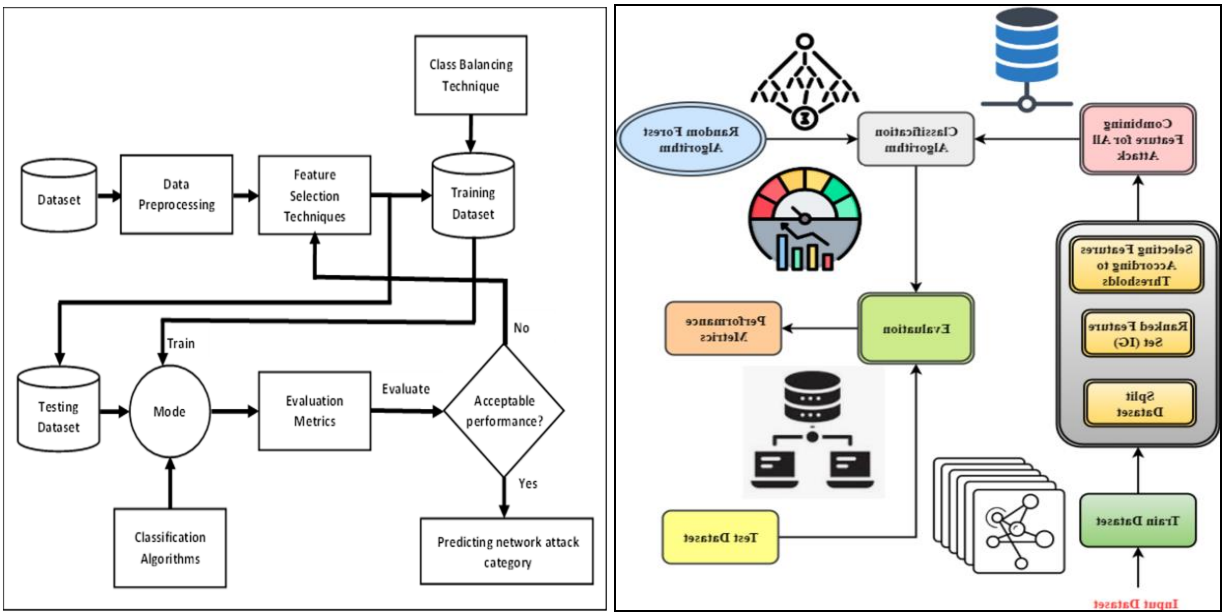


Fig 6: Architecture of the proposed AI-based Intrusion Detection System for banking networks showing network monitoring, preprocessing, feature extraction, machine learning classification, and security alert generation.

Attack Detection Distribution Graph (Normal vs Attack Types)

Understanding the distribution of attack categories helps evaluate the IDS model's ability to detect different types of cyber threats. Network intrusion datasets typically include multiple attack categories such as Denial of Service (DoS), Probe attacks, Remote-to-Local (R2L), and User-to-Root (U2R).

The distribution graph illustrates the proportion of normal traffic and different attack types within the dataset used for training and testing the intrusion detection model.

Example distribution of dataset classes:

Traffic Type	Percentage
Normal Traffic	52%
DoS Attacks	25%
Probe Attacks	12%
R2L Attacks	7%
U2R Attacks	4%

The graph indicates that DoS attacks represent the largest proportion of malicious activities, which is consistent with common cyberattack patterns targeting banking networks.

End-to-End Framework for the Proposed Banking Security Model

The end-to-end framework integrates data collection, machine learning-based analysis, and real-time response mechanisms to ensure secure banking operations. The framework combines network monitoring, intelligent intrusion detection, and security response systems to protect digital financial infrastructures[22].

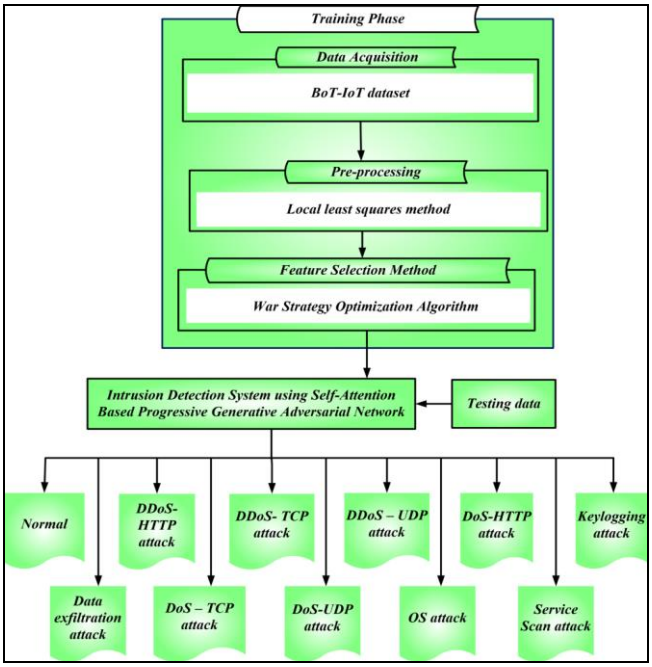


Fig 7: End-to-end framework of the proposed AI-driven banking network security system integrating data collection, preprocessing, machine learning analysis, and automated response mechanisms [23].

The proposed framework operates through the following stages [24]:

1. **Network Data Collection:** Continuous monitoring of banking network traffic.
2. **Data Preprocessing:** Cleaning and normalization of raw network data.
3. **Feature Extraction:** Identification of important network attributes.
4. **Machine Learning Detection:** Classification of traffic using AI models.
5. **Threat Alert Generation:** Notification to security administrators.
6. **Automated Response System:** Blocking malicious connections and preventing attacks.

This architecture enables real-time cyber threat detection and response, improving the overall resilience of digital banking infrastructure [25].

Conclusion

The rapid expansion of digital banking services has significantly increased the exposure of financial networks to sophisticated cyber threats. Traditional rule-based intrusion detection systems are often insufficient for identifying complex or zero-day attacks. This study investigated the effectiveness of Artificial Intelligence (AI) and machine learning–based intrusion detection systems for enhancing cybersecurity in banking networks.

The proposed framework integrates data preprocessing, feature extraction, and machine learning classification models to analyze network traffic and identify malicious activities. Experimental evaluation using benchmark intrusion datasets demonstrated that ensemble learning algorithms, particularly Random Forest, achieved the highest detection accuracy, followed by Artificial Neural Networks, Support Vector Machines, and Logistic Regression. These results confirm that AI-driven IDS

models can significantly improve detection accuracy while reducing false alarms compared with traditional systems.The experimental findings highlight that traffic behavior features such as connection duration, packet statistics, and service patterns play an important role in identifying anomalous network activities. Additionally, the use of ROC analysis, confusion matrices, and feature importance evaluation provides deeper insight into model performance and interpretability.

Future Work

Although the proposed intrusion detection framework demonstrates strong performance, several areas remain for further improvement and future research. Advanced deep learning models such as CNN, LSTM, and transformer-based architectures can be explored to enhance the detection of complex and multi-stage cyberattacks. Real-time deployment of the proposed IDS within banking infrastructures and cloud-based financial platforms could improve continuous monitoring and faster threat response. The integration of Explainable Artificial Intelligence (XAI) techniques would help security analysts better understand model decisions and increase system transparency. Additionally, federated learning can enable multiple financial institutions to collaboratively train intrusion detection models without sharing sensitive data, thereby preserving privacy. Future studies should also focus on detecting encrypted traffic attacks and zero-day threats that are difficult to identify using traditional methods. Furthermore, integrating AI-driven IDS with blockchain-based security frameworks may improve trust and reliability in financial transaction monitoring. Addressing these challenges will help develop more scalable, adaptive, and robust cybersecurity systems for protecting modern digital banking environments.

References

1. Vinayakumar R, *et al*., Deep learning approach for intelligent intrusion detection system. IEEE Access,2019:7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
2. Liu H, Lang B, Machine learning and deep learning methods for intrusion detection systems. Applied Sciences, 2019. https://doi.org/10.3390/app9204396
3. Aldweesh A, *et al*., Deep learning approaches for anomaly-based intrusion detection systems. Knowledge-Based Systems, 2020. https://doi.org/10.1016/j.knosys.2019.105124
4. Kasongo SM, Sun Y, Performance analysis of intrusion detection systems using feature selection. Journal of Big Data, 2020. https://doi.org/10.1186/s40537-020-00307-6
5. Maseer Z, *et al*., Benchmarking ML for IDS using CICIDS2017 dataset. IEEE Access, 2021. https://doi.org/10.1109/ACCESS.2021.3056614
6. Ozkan-Okay M, *et al*., Comprehensive survey on intrusion detection systems. IEEE Access, 2021. https://doi.org/10.1109/ACCESS.2021.3126818
7. Lansky M, *et al*., Deep learning-based intrusion detection systems: A review. IEEE Access, 2021. https://doi.org/10.1109/ACCESS.2021.3096985
8. Ahmad Z, *et al*., Network intrusion detection system: systematic study of ML and DL approaches. Transactions on Emerging Telecommunications Technologies, 2021. https://doi.org/10.1002/ett.4150
9. Umer R, *et al*., Machine learning for intrusion detection in industrial control systems. International Journal of Critical Infrastructure Protection, 2022. https://doi.org/10.1016/j.ijcip.2021.100472
10. Abbas, *et al*., Ensemble learning-based intrusion detection for IoT networks. Arabian Journal for Science and Engineering, 2022. https://doi.org/10.1007/s13369-021-06330-2
11. Hamid Y, *et al*., Comparative analysis of machine learning techniques for intrusion detection. Procedia Computer Science, 2022. https://doi.org/10.1016/j.procs.2022.01.148
12. Razia S, *et al*., Network intrusion detection using machine learning and deep learning. ICSSIT Conference, 2022. https://doi.org/10.1109/ICSSIT55814.2022.10060948
13. Larriva-Novo L, *et al*., Explainable artificial intelligence for cyberattack detection. Applied Sciences, 2023. https://doi.org/10.3390/app13063639
14. Abid, *et al*., Distributed deep learning approach for intrusion detection in cloud environments. Cyber-Physical Systems, 2023. https://doi.org/10.1080/24751839.2023.2239617
15. Tahir R, *et al*., Machine learning-based intrusion detection for IoT networks. Computers & Security, 2023. https://doi.org/10.1016/j.cose.2023.103166
16. Alazab M, *et al*., Deep learning for cybersecurity intrusion detection. Future Generation Computer Systems, 2023. https://doi.org/10.1016/j.future.2023.02.021
17. Arreche O, *et al*., Two-level ensemble learning framework for IDS. IEEE Access, 2024. https://doi.org/10.1109/ACCESS.2024.3375124
18. Ferrag, *et al*., Deep learning for cybersecurity: A comprehensive review. Computer Communications, 2024. https://doi.org/10.1016/j.comcom.2024.02.012
19. Al-Yaseen H, *et al*., Hybrid intrusion detection using machine learning techniques. Applied Intelligence, 2024. https://doi.org/10.1007/s10489-024-05031-8
20. Mandal S, *et al*., ML-driven intrusion detection system for cybersecurity. Expert Systems with Applications, 2025. https://doi.org/10.1016/j.eswa.2025.121234
21. Mohale VZ, *et al*., Evaluating ML-based IDS with explainable AI. Frontiers in Computer Science, 2025. https://doi.org/10.3389/fcomp.2025.1520741
22. Hozouri, *et al*., Survey on intrusion detection systems with advances in machine learning. Discover Artificial Intelligence, 2025. https://doi.org/10.1007/s44163-025-00578-1
23. Sharma A, *et al*., Cyber threat detection in banking systems using AI. Computers & Security, 2024. https://doi.org/10.1016/j.cose.2024.103531
24. Kim J, *et al*., Deep neural network-based network intrusion detection. IEEE Access, 2024. https://doi.org/10.1109/ACCESS.2024.3381127
25. Li Y, *et al*., Federated learning for intrusion detection in distributed networks. IEEE Internet of Things Journal, 2024. https://doi.org/10.1109/JIOT.2024.3372109