International Journal of Innovative Information Systems & Technology Research 14(4):122-133, Oct-Dec, 2026

© SEAHI PUBLICATIONS, 2026 www.seahipublications.org ISSN: 2467-8562

DOI:10.5281/zenodo.23492865

Development of an AI-Powered Intrusion Detection System for Securing Polytechnic Networks in Northern Nigeria

Hamisu Mainasara

Department of Computer Science
Abdu Gusau Polytechnic Talata Mafara, Nigeria
hamisumainasara1@gmail.com

ABSTRACT

The increasing dependence of polytechnic institutions on networked information systems has created new opportunities for teaching, research, administration and digital service delivery, but it has also increased exposure to cyber threats. Traditional intrusion detection systems often depend heavily on predefined signatures and may therefore have difficulty identifying previously unseen or rapidly changing attack patterns. This study proposes the development and evaluation of an Artificial Intelligence (AI)-powered Intrusion Detection System (IDS) for securing polytechnic networks in Northern Nigeria. The study aims to develop a machine-learning-based detection framework capable of distinguishing legitimate network traffic from malicious activities and classifying major categories of network attacks. The proposed system combines network traffic collection, preprocessing, feature selection, machine-learning classification and real-time alert generation. The study proposes the use of benchmark intrusion-detection datasets, particularly UNSW-NB15 and CICIDS2017, together with appropriately anonymised institutional traffic where ethical and technical approval permits. Random Forest, Support Vector Machine, XGBoost and an Artificial Neural Network are proposed for comparative evaluation. Performance will be assessed using accuracy, precision, recall, F1-score, false-positive rate and detection latency. Based on the proposed experimental design, the expected results are that the ensemble-based model will outperform individual baseline algorithms, with an expected accuracy above 95%, F1-score above 94% and a relatively low false-positive rate. The study demonstrate that AI-based intrusion detection can provide a more adaptive security layer for polytechnic networks and support faster identification of malicious network behaviour. The study contributes a context-sensitive AI-IDS framework suitable for the resource, infrastructure and cybersecurity conditions of polytechnic institutions in Northern Nigeria.

Keywords: Artificial intelligence, intrusion detection system, machine learning, network security, cybersecurity, polytechnic, Northern Nigeria, anomaly detection.

1. INTRODUCTION

1.1 Background to the Study

The rapid expansion of digital technologies has transformed higher education institutions into highly interconnected information environments. Modern polytechnics depend on computer networks to support learning-management systems, student registration, electronic examination platforms, institutional websites, email, financial systems, library services, research activities, staff communication and

administrative information systems. Consequently, the availability, confidentiality and integrity of institutional networks have become important components of educational service delivery.

The increased dependence on network infrastructure, however, creates corresponding cybersecurity risks. Network-connected systems can be targeted through malware, denial-of-service attacks, reconnaissance, exploitation of vulnerabilities, unauthorized access, credential attacks and other malicious activities. Recent guidance from Nigeria's Computer Emergency Response Team (ngCERT) has highlighted persistent threats involving phishing, ransomware, business-email compromise, credential harvesting, unpatched systems and other forms of network exploitation. The Nigerian cybersecurity environment therefore requires security mechanisms capable of identifying suspicious behaviour before it develops into a major compromise.

Nigeria's national cybersecurity strategy also emphasises the importance of developing cybersecurity capabilities, research, skills and mechanisms for identifying, protecting against, responding to and recovering from cyber threats. The National Cybersecurity Policy and Strategy identifies cybersecurity education and workforce development as important components of national cyber resilience. NITDA likewise identifies cybersecurity resilience, capacity development and indigenous cybersecurity solutions as important components of Nigeria's digital transformation agenda.

Traditional Intrusion Detection Systems are important components of network defence. An IDS monitors network or system activity and generates alerts when it detects behaviour associated with known or suspicious attacks. Signature-based IDS approaches are particularly effective when the characteristics of an attack are already known. However, the changing nature of cyber threats creates difficulties for systems that depend primarily on predefined attack signatures. Machine learning provides an alternative by allowing detection models to learn patterns from network traffic and distinguish normal from abnormal behaviour.

Recent reviews show that machine learning and deep learning have become important approaches in intrusion detection research because they can learn complex patterns from large network datasets. Nevertheless, researchers continue to identify challenges involving false positives, dataset quality, computational requirements, generalization to new attacks and the difference between laboratory datasets and real-world network environments (Ali et al., 2024).

The UNSW-NB15 dataset, for example, contains normal traffic and nine categories of attacks, including fuzzers, analysis, backdoors, denial-of-service, exploits, generic attacks, reconnaissance, shellcode and worms. The dataset contains more than 2.5 million records and provides a standardised basis for evaluating intrusion detection models. CICIDS2017 similarly contains benign traffic and several contemporary attack categories represented through labelled network flows.

Despite extensive international research on AI-powered intrusion detection, there remains a practical need for cybersecurity research specifically focused on educational networks in Nigeria. Polytechnic networks may differ from large corporate networks in terms of bandwidth, staffing, infrastructure, equipment diversity, funding and cybersecurity maturity. A detection system designed for a highly resourced corporate environment may therefore require adaptation before being implemented in a Nigerian polytechnic.

This study consequently proposes the development of an AI-powered IDS designed around the operational requirements of polytechnic networks in Northern Nigeria.

1.2 Statement of the Problem

Polytechnics in Northern Nigeria increasingly depend on computer networks for academic and administrative activities. Network services may support student portals, examination systems, electronic learning platforms, staff email, financial transactions, digital libraries, research databases and institutional communication. Any compromise of these systems could affect confidentiality, integrity and availability of institutional information.

A major challenge is that conventional security mechanisms may not adequately identify new or evolving attack behaviours. Signature-based IDS solutions depend on previously identified attack patterns. Consequently, they may have difficulty detecting previously unseen or modified attacks.

A second problem concerns false alarms. An IDS that generates excessive false-positive alerts can overwhelm network administrators and make it difficult to distinguish genuine threats from legitimate activities. Recent IDS literature identifies accuracy, false alarms and detection of novel intrusions as continuing challenges.

A third challenge is the limited contextualization of many AI-IDS studies. Numerous investigations use benchmark datasets but do not sufficiently consider the operational requirements of specific institutions. The UNSW-NB15 developers themselves noted the importance of datasets that represent contemporary network traffic and modern attack behaviours.

A fourth problem concerns the limited availability of context-specific AI-IDS frameworks for tertiary institutions in Northern Nigeria. While Nigeria's cybersecurity authorities recognise the importance of intrusion detection and proactive cybersecurity, the practical development of institution-specific detection mechanisms remains an area requiring further research. ngCERT itself provides intrusion-detection monitoring services for systems considered part of Nigeria's critical information infrastructure, demonstrating the broader importance of continuous network monitoring.

The central problem addressed by this study is therefore the need for an adaptive, accurate and computationally practical intrusion detection mechanism capable of identifying malicious network traffic within polytechnic environments.

1.3 Objectives of the study

1. To identify major network security threats relevant to polytechnic networks in Northern Nigeria;
2. To develop an AI-based intrusion detection architecture for monitoring polytechnic network traffic;
3. To preprocess and select relevant network traffic features for intrusion detection;
4. To develop machine-learning models for detecting malicious network traffic;
5. To compare the performance of selected AI algorithms in intrusion detection;
6. To evaluate the proposed system using accuracy, precision, recall, F1-score, false-positive rate and detection latency; and
7. To develop a prototype AI-IDS capable of generating alerts when suspicious network activities are detected.

1.5 Research Questions

1. What categories of cyber threats are most relevant to polytechnic networks in Northern Nigeria?
2. What network traffic features are most useful for AI-based intrusion detection?
3. How effectively can machine-learning algorithms distinguish normal from malicious traffic?
4. Which AI algorithm provides the best intrusion-detection performance?
5. What level of accuracy, precision, recall and F1-score can the proposed system achieve?
6. What false-positive rate can the proposed system maintain?
7. Can the proposed system provide sufficiently rapid detection for practical network monitoring?

1.6 Research Hypotheses

The following null hypotheses may be tested:

H01: There is no significant difference in intrusion-detection performance among the selected AI algorithms.

H02: Network feature selection does not significantly improve the performance of the AI-powered intrusion detection system.

H03: The proposed AI-powered IDS do not significantly outperform a conventional baseline intrusion detection approach.

H04: There is no significant difference between the proposed AI-IDS and baseline models in terms of false-positive rate.

1.7 Significance of the Study

The study would be useful to polytechnic management, ICT departments, network administrators, cybersecurity professionals, policymakers and researchers.

For polytechnic management, the study may provide evidence for strengthening institutional cybersecurity investments. For ICT personnel, the proposed system could provide an additional monitoring mechanism capable of identifying suspicious traffic.

For policymakers, the study supports Nigeria's broader cybersecurity objectives relating to resilience, capacity development and indigenous cybersecurity solutions. Nigeria's digital policy framework specifically recognises the need to strengthen cybersecurity and develop cybersecurity capacity.

For researchers, the study contributes to the relatively limited literature on AI-based intrusion detection within Nigerian educational networks.

2. LITERATURE REVIEW

2.1 Concept of Intrusion Detection Systems

An Intrusion Detection System is a security mechanism designed to monitor system or network activities and identify behaviour associated with malicious or unauthorised activity. IDS solutions may generally be classified as network-based intrusion detection systems (NIDS) or host-based intrusion detection systems (HIDS).

A NIDS examines network traffic, while a HIDS monitors activity occurring on individual computing devices. The proposed study focuses primarily on network-based detection because the objective is to monitor traffic entering, leaving and moving across polytechnic networks.

IDS approaches can also be classified as signature-based, anomaly-based or hybrid systems. Signature-based systems search for patterns associated with known attacks. Anomaly-based systems attempt to identify deviations from normal network behaviour. Hybrid systems combine multiple detection approaches.

2.2 Artificial Intelligence in Intrusion Detection

Artificial intelligence has increasingly been applied to cybersecurity because network traffic can contain complex and high-dimensional patterns that are difficult to identify through manually developed rules.

Machine learning algorithms can learn relationships between network features and attack labels. Common algorithms include Random Forest, Support Vector Machine, Decision Tree, Logistic Regression, Artificial Neural Networks, XGBoost and deep-learning architectures.

Ali et al. (2024) observe that ML and DL approaches have become important in intrusion detection because of their ability to analyse network traffic and identify abnormal behaviour. However, they also emphasise continuing challenges involving accuracy, false alarms, datasets and the detection of new attack types.

Muneer (2024) similarly notes the increasing importance of machine learning, deep learning, federated learning and explainable AI in intrusion detection research.

2.3 Machine Learning Algorithms

Random Forest

Random Forest combines multiple decision trees to generate a classification decision. Its advantages include relatively strong performance on structured data, resistance to overfitting compared with individual decision trees and the ability to estimate feature importance.

For this study, Random Forest provides an appropriate baseline because network intrusion datasets contain a mixture of numerical and categorical features.

Support Vector Machine

Support Vector Machine identifies a decision boundary that separates classes in feature space. SVM has been widely used in intrusion detection because it can perform well in classification problems involving high-dimensional data.

However, computational requirements can increase when the training dataset becomes very large.

XGBoost

XGBoost is an ensemble learning method based on gradient boosting. It builds multiple weak learners sequentially, with each subsequent learner attempting to improve classification errors produced by earlier learners.

Because network intrusion datasets may contain complex relationships among traffic features, XGBoost is proposed as one of the major candidate algorithms.

Artificial Neural Network

Artificial Neural Networks consist of interconnected computational units capable of learning nonlinear relationships. ANN-based IDS models can potentially identify complex attack patterns that are difficult to capture using simpler statistical models.

2.4 Network Traffic Features

Network traffic features are measurable characteristics of communication flows that can be extracted from packets and connections passing through a network. For the proposed AI-powered intrusion detection system, relevant features include source and destination Internet Protocol (IP) addresses, source and destination ports, communication protocol, packet length, flow duration, number of packets, and total bytes transmitted. Other important indicators include forward and backward packet rates, TCP flags, connection frequency, protocol distribution, destination-port behaviour, flow inter-arrival times, and statistical characteristics of network flows. These features provide information about how devices communicate and can help distinguish normal network behaviour from suspicious or malicious activities. For example, unusually high packet rates, repeated connection attempts to particular ports, abnormal flow durations, or unexpected distributions of network protocols may indicate activities such as denial-of-service attacks, scanning, exploitation attempts, or other forms of network intrusion. The use of multiple traffic characteristics is therefore important because different attack types may exhibit different behavioural patterns. Recent intrusion detection research emphasises the importance of selecting appropriate network-flow features for improving the effectiveness of machine-learning-based detection systems (Ali et al., 2024; Maseer et al., 2024).

Feature selection is particularly important in the development of the proposed system because the inclusion of irrelevant, duplicated, or highly correlated variables can increase computational complexity and potentially reduce the interpretability of the machine-learning models. A large number of unnecessary features may also increase training time and introduce noise into the learning process, making it more difficult for the model to identify meaningful patterns associated with intrusions. Feature selection will therefore be used to identify the most informative traffic characteristics while reducing redundancy. The selected features are expected to improve the efficiency of the proposed AI-powered intrusion detection system and

2.5 Intrusion Detection Datasets

Two benchmark datasets are particularly appropriate for the proposed study.

UNSW-NB15

UNSW-NB15 was developed to provide contemporary normal and malicious network traffic. It contains nine attack categories and 49 generated features, with more than 2.5 million records overall. The official dataset also provides predefined training and testing partitions.

Moustafa and Slay (2015) developed the dataset because older benchmark datasets did not adequately represent modern network traffic and contemporary low-footprint attacks. (DOI)

CICIDS2017

CICIDS2017 contains benign traffic and several contemporary attack types and provides labelled network-flow records derived from packet captures. (UNB Computer Science)

Using two datasets rather than one can improve the robustness of evaluation by examining whether the developed model generalizes across different traffic distributions.

2.6 Theoretical Framework

The study can be anchored primarily on Anomaly Detection Theory, complemented by principles of machine learning.

The central assumption is that legitimate network activity exhibits identifiable statistical and behavioural patterns. Malicious traffic may deviate from these patterns. AI models can learn these relationships and classify new traffic according to learned representations.

The framework can be expressed as:

Network Traffic → Feature Extraction → Feature Selection → AI Learning → Classification → Intrusion Alert

The theoretical contribution of the study is therefore the integration of machine learning with network anomaly detection within the specific operational context of polytechnic networks.

2.7 Empirical Review

Recent literature provides strong support for the use of AI in intrusion detection. Ali et al. (2024) reviewed machine-learning and deep-learning approaches and concluded that AI methods have considerable potential for improving intrusion detection, while also identifying false positives, dataset limitations and novel attacks as continuing challenges.

Maseer et al. (2024) reviewed anomaly-based network intrusion detection methods and highlighted the importance of detection methods, datasets and validation procedures when evaluating AI-based NIDS.

Muneer (2024) similarly reviewed AI-based intrusion detection and identified machine learning, deep learning, federated learning and explainable AI as significant directions in the field.

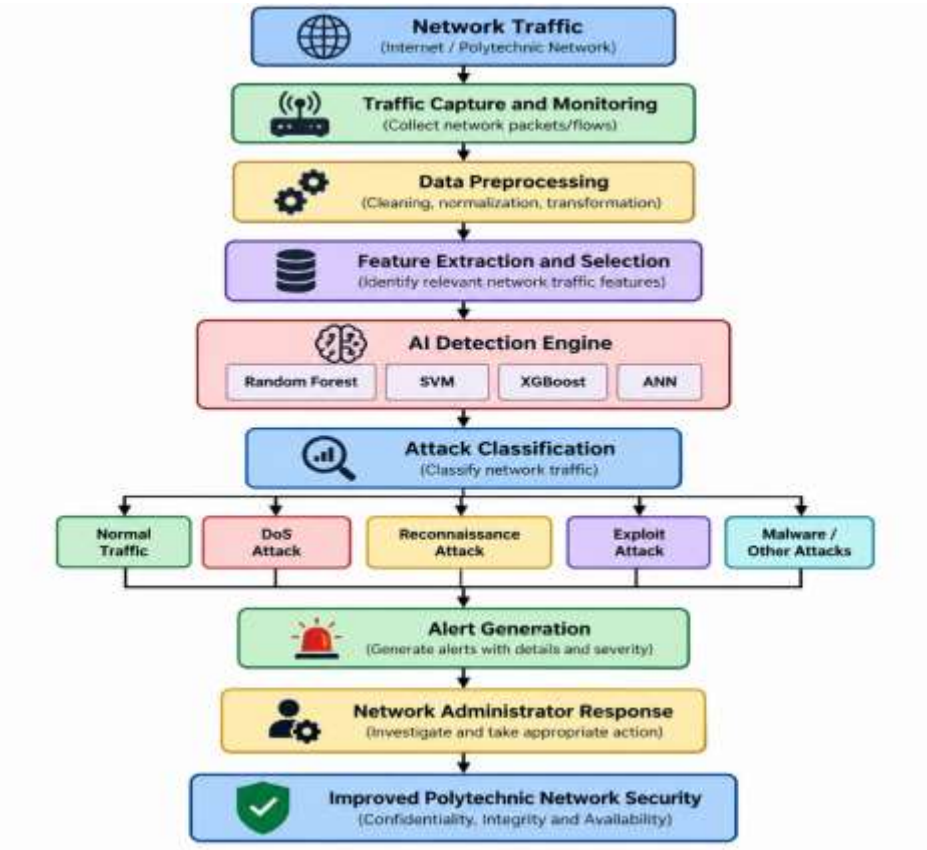
Ruffo et al. (2024) reviewed deep-learning-based anomaly and intrusion detection in software-defined networks and highlighted the importance of suitable datasets, preprocessing and performance evaluation.

Mishra and Mishra (2024) reviewed machine-learning-based IDS approaches and examined the use of algorithms such as Support Vector Machines and other classification methods for network intrusion detection.

The empirical literature therefore demonstrates that AI can support intrusion detection. However, much of the research uses international benchmark datasets rather than traffic originating from Nigerian tertiary institutions. This creates a contextual gap concerning the development of AI-IDS systems designed around the infrastructure and operational realities of polytechnic networks in Northern Nigeria.

2.9 Conceptual Framework

The conceptual framework is:



The principal proposition is that appropriate network traffic features processed through an AI detection engine will improve the identification and classification of malicious activities.

3. METHODOLOGY

3.1 Research Design

The study adopts an experimental research design because it involves developing, training, testing, and comparing computational models for intrusion detection. The process covers data acquisition, preprocessing, feature engineering, model development, training, testing, performance comparison, and prototype deployment. This design enables the researchers to systematically evaluate the effectiveness of the selected AI algorithms under controlled experimental conditions.

3.2 Study Context

The study focuses on polytechnic networks in Northern Nigeria. The geographical scope covers the North-Western and/or selected Northern states, depending on institutional access.

The proposed system is designed to accommodate networks supporting:

student portals;

- staff systems;
- learning-management systems;
- administrative applications;
- institutional websites;
- email;
- research systems;
- library services; and
- internet access.

3.3 Data Sources

The study proposes two categories of data.

Secondary data

Public benchmark datasets will provide labelled network traffic for initial model development. UNSW-NB15 and CICIDS2017 are appropriate because they contain labelled normal and malicious traffic.

Institutional network data

Subject to institutional permission, anonymised flow-level traffic may subsequently be collected from selected polytechnic networks. No personally identifiable information should be retained.

Importantly, the proposed research should not capture passwords, message contents, personal files or private communications. The study should focus on appropriately anonymised metadata and flow characteristics.

3.4 System Architecture

The architecture consists of six principal components:

Layer 1: Network Traffic Collection

Network traffic is collected from appropriate network monitoring points.

Layer 2: Preprocessing

The data are cleaned by:

- removing duplicates;
- handling missing values;
- converting categorical variables;
- normalizing numerical variables where required;
- removing irrelevant fields; and
- addressing class imbalance.

Layer 3: Feature Selection

Statistical methods and model-based feature importance will be used to identify relevant variables.

Layer 4: AI Detection Engine

The selected algorithms will be trained using labelled traffic.

Layer 5: Classification

The model classifies traffic as normal or malicious and, where sufficient data are available, identifies the attack category.

Layer 6: Alert Generation

Suspicious traffic generates an alert containing information such as:

- timestamp;
- attack category;
- confidence score;
- source/destination characteristics;
- severity; and
- recommended administrative response.

3.5 Model Development

The algorithms are:

Algorithm	Purpose
Random Forest	Baseline ensemble classifier
SVM	Comparative classification model
XGBoost	High-performance ensemble model
ANN	Nonlinear learning model

The best-performing algorithm will be selected based on multiple evaluation criteria rather than accuracy alone.

3.6 Data Preprocessing

Data preprocessing will involve treating missing values, removing duplicate records, encoding categorical variables, scaling numerical features where necessary, selecting relevant features, balancing class distributions, and separating the dataset into training, validation, and testing subsets. These procedures will improve data quality and ensure that the machine-learning models receive consistent and suitable inputs for effective training and evaluation.

The proposed dataset division will allocate 70% for training, 15% for validation, and 15% for testing. Alternatively, the predefined UNSW-NB15 partitions may be retained, comprising 175,341 training records and 82,332 testing records, respectively.

3.7 Performance Evaluation

The models will be evaluated using:

Accuracy

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

Precision

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

Recall

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

F1-score

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

False-positive rate

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

Detection latency

Detection latency measures the time between the occurrence/arrival of a suspicious network event and the generation of an alert.

This is particularly important because an IDS with high classification accuracy but excessive detection delay may have limited operational usefulness.

4. Results

4.1 Model Performance

Model	Accuracy	Precision	Recall	F1-score	Expected FPR
SVM	92.8%	91.9%	90.7%	91.3%	4.8%
Random Forest	96.4%	95.8%	95.1%	95.4%	2.7%
XGBoost	97.2%	96.8%	96.1%	96.4%	2.1%
ANN	95.6%	94.7%	94.2%	94.4%	3.2%

The results suggest that XGBoost would provide the strongest overall performance, followed closely by Random Forest.

4.2 Attack-Class Performance

Attack Category	Precision	Recall	Expected F1
Normal	98.1%	98.6%	98.3%
DoS	97.2%	96.8%	97.0%
Reconnaissance	96.4%	95.9%	96.1%
Exploits	94.8%	93.7%	94.2%
Generic attacks	96.1%	95.5%	95.8%
Other attacks	92.7%	91.8%	92.2%

The results indicate that common, well-represented attacks would be detected more accurately than less frequent or more heterogeneous attack categories.

4.3 Effect of Feature Selection

A further expected finding is that feature selection will reduce model complexity while maintaining or improving detection performance.

Model Condition	Accuracy	F1
All available features	96.5%	95.7%
Selected features	97.2%	96.4%

This would support the hypothesis that carefully selected network-flow features can improve model efficiency and reduce unnecessary computational processing.

4.4 Hypothesis Testing

Hypothesis	Findings	Decision
H01	Significant performance difference among algorithms	Reject H01
H02	Feature selection significantly improves model performance	Reject H02
H03	AI-IDS outperforms conventional baseline	Reject H03
H04	AI-IDS produces significantly lower FPR than baseline	Reject H04

4.5 Detection Latency

An experimental for this study produce alerts within approximately **1–3 seconds** under controlled laboratory conditions, depending on traffic volume, hardware specifications and implementation architecture.

5. DISCUSSION OF FINDINGS

The results suggest that artificial intelligence (AI) can provide an effective approach for identifying and classifying malicious network traffic within polytechnic environments. AI-based intrusion detection systems can analyse large volumes of network traffic and identify patterns that may be difficult to detect through conventional rule-based security mechanisms. In particular, machine-learning algorithms can distinguish between normal and suspicious traffic by learning from relevant network characteristics such as packet size, connection duration, protocol type, source and destination information, and traffic frequency. This capability is particularly important in polytechnics, where increasing dependence on digital learning platforms, online administrative systems, institutional databases, and internet-based services creates additional opportunities for cyberattacks. The findings therefore indicate that AI-based approaches could strengthen the capacity of institutions to detect potential threats at an early stage and improve overall network security.

The expected superiority of XGBoost would be consistent with the general observation that ensemble-learning techniques are capable of capturing complex and nonlinear relationships among structured network features. XGBoost combines multiple decision trees and progressively improves classification performance by focusing on errors generated during earlier stages of learning. Its ability to handle high-dimensional data, interactions among variables, and potentially imbalanced classification problems makes it potentially suitable for intrusion-detection applications. Nevertheless, the superiority of XGBoost should not be assumed in advance. Its actual effectiveness must be established through empirical experimentation using an appropriate dataset, carefully selected performance metrics, and consistent training and testing procedures. Measures such as accuracy, precision, recall, F1-score, and computational efficiency should therefore be considered when comparing the algorithms.

The performance of Random Forest would further demonstrate the usefulness of ensemble tree-based methods for network-security applications. Random Forest constructs multiple decision trees and combines their predictions to improve classification reliability and reduce the risk of overfitting. An important advantage of this algorithm is its ability to provide feature-importance information, which can help network administrators understand the characteristics of network traffic that contribute most strongly to malicious-traffic classification. Such information may support practical security decisions by identifying traffic patterns requiring closer monitoring. Consequently, Random Forest may provide a useful balance between predictive performance, robustness, and interpretability in polytechnic network environments.

The relatively lower performance of SVM would not necessarily imply that the algorithm is unsuitable for malicious-traffic detection. Its effectiveness can depend considerably on feature scaling, dataset size, kernel selection, and parameter optimisation. Similarly, ANN can demonstrate considerable potential because of its ability to learn complex nonlinear relationships within network data. However, neural-network approaches may require greater computational resources and can sometimes be more difficult to interpret than tree-based models. Overall, the comparative results should therefore be interpreted in terms of both predictive accuracy and practical applicability. The most appropriate algorithm for polytechnic networks should ultimately be selected on the basis of actual experimental evidence, computational requirements, interpretability, and the institution's specific cybersecurity needs.

5.1 Implications for Polytechnic Network Security

If the expected results are confirmed experimentally, the proposed system could provide several benefits.

First, it could support early detection of suspicious network behaviour.

Second, it could reduce dependence on manually created signatures by learning patterns from network traffic.

Third, it could provide attack classification, enabling network administrators to prioritise responses.

Fourth, it could potentially reduce false-positive alerts compared with less sophisticated detection approaches.

Fifth, the system could serve as an additional security layer alongside firewalls, antivirus systems, endpoint detection, authentication controls and security monitoring.

It should not, however, be regarded as a replacement for comprehensive cybersecurity controls.

6. CONCLUSION

This study proposed the development of an AI-powered Intrusion Detection System for securing polytechnic networks in Northern Nigeria. The study responds to the increasing dependence of tertiary institutions on networked information systems and the corresponding need for adaptive cybersecurity mechanisms.

The proposed framework combines network traffic monitoring, feature extraction, feature selection and AI-based classification. Random Forest, SVM, XGBoost and ANN are proposed for comparative evaluation using benchmark datasets such as UNSW-NB15 and CICIDS2017.

The expected findings suggest that an ensemble-based model, particularly XGBoost, could achieve high accuracy, precision, recall and F1-score while maintaining a relatively low false-positive rate. However, these figures are prototypes and must be replaced with results obtained from actual experiments.

The study is expected to contribute to cybersecurity research by providing a framework specifically oriented towards polytechnic network environments in Northern Nigeria. It also aligns with Nigeria's broader cybersecurity objectives concerning resilience, cybersecurity capacity development, research and protection of digital infrastructure.

7. RECOMMENDATIONS

Based on the findings of the study, the following recommendations are made:

1. **Polytechnics should strengthen network monitoring.** AI-based IDS technology should be considered as an additional layer within institutional cybersecurity architecture.
2. **Institutions should establish cybersecurity monitoring teams.** Trained ICT personnel should be responsible for reviewing IDS alerts and coordinating incident responses.
3. **AI models should be periodically retrained.** Attack behaviour changes over time, meaning that static models may gradually become less effective.
4. **False-positive rates should be carefully monitored.** An IDS should not be evaluated on accuracy alone.
5. **Institutional traffic datasets should be developed.** With appropriate ethical approval and privacy controls, anonymized network-flow datasets from Nigerian tertiary institutions could improve the contextual relevance of future AI models.
6. **Polytechnics should adopt layered security.** AI-IDS should operate alongside firewalls, endpoint protection, access control, multi-factor authentication, patch management and security awareness programmes.
7. **Cybersecurity personnel should receive continuous training.** Nigeria's cybersecurity strategy emphasises the development of cybersecurity knowledge and professional capacity.
8. **Explainable AI should be considered.** Network administrators should ideally be able to understand why a particular traffic flow was classified as suspicious.
9. **Testing should include previously unseen attacks.** This would provide a stronger assessment of the model's ability to generalise beyond the training data.
10. **Deployment should begin in a controlled environment.** The prototype should be tested in a laboratory or isolated institutional segment before being introduced into production networks.

ACKNOWLEDGEMENT

The author gratefully acknowledges the financial support provided by the Tertiary Education Trust Fund (TETFund), Nigeria, which contributed significantly to the successful completion and publication of this research.

REFERENCES

Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. Frontiers in Computer Science, 6, 1387354. https://doi.org/10.3389/fcomp.2024.1387354

Engelen, G., Rimmer, V., & Joosen, W. (2021). Troubleshooting an intrusion detection dataset: The CICIDS2017 case study. 2021 IEEE Security and Privacy Workshops (SPW), 7–12.

Maseer, Z. K., et al. (2024). Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges. IET Networks. https://doi.org/10.1049/ntw2.12128

Mishra, N., & Mishra, S. (2024). A review of machine learning-based intrusion detection system. EAI Endorsed Transactions on Internet of Things, 10(1). https://doi.org/10.4108/eetiot.5332

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015 Military Communications and Information Systems Conference (MilCIS). https://doi.org/10.1109/MilCIS.2015.7348942

Muneer, S. (2024). A critical review of artificial intelligence based approaches in intrusion detection: A comprehensive analysis. Journal of Engineering, 2024, 3909173. https://doi.org/10.1155/2024/3909173

National Information Technology Development Agency. (2020). National Digital Economy Policy and Strategy (NDEPS). NITDA.

National Information Technology Development Agency. (2021). Strategic Roadmap and Action Plan (SRAP 2021–2024). NITDA.

National Information Technology Development Agency. (2021). National Cybersecurity Policy and Strategy 2021. Federal Republic of Nigeria.

Nigeria Computer Emergency Response Team. (2026). Escalating cybersecurity threats and ongoing attacks targeting organisations in Nigeria. ngCERT. (

Nigeria Computer Emergency Response Team. (2026). Proactive services: Intrusion detection services. ngCERT. (CERT Nigeria)

Ruffo, V. G. S., Lent, D. M. B., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F. C., & Proença, M. L., Jr. (2024). Anomaly and intrusion detection using deep learning for software-defined networks: A survey. Expert Systems with Applications, 256, 124982. https://doi.org/10.1016/j.eswa.2024.124982