International Journal of Innovative Information Systems & Technology Research 14(4):108-121, Oct-Dec, 2026

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

DOI:10.5281/zenodo.23492884

Artificial Intelligence-Based Intrusion Detection Systems for Securing Polytechnic Networks: A Case Study of Selected Polytechnics in Northern Nigeria

Abdulkarim Ibrahim

Department of Computer Science
Abdu Gusau Polytechnic Talata Mafara, Nigeria
E-mail; - amungode@gmail.com

ABSTRACT

The increasing dependence of polytechnics on digital platforms has created new opportunities for teaching, administration, research, online examinations, student services, and electronic communication. At the same time, this dependence has expanded the number of systems and users that can potentially be targeted by cyberattacks. Traditional intrusion detection systems can identify known threats effectively, but their dependence on predefined signatures may limit their ability to recognise new or evolving attack patterns. Artificial intelligence (AI), particularly machine learning, offers an alternative approach by learning patterns from network traffic and identifying activities that differ from normal behaviour. This study examines the effectiveness of AI-based intrusion detection systems in securing selected polytechnic networks in Northern Nigeria. The study adopts a quantitative experimental design using network-traffic datasets and a prototype AI-based detection model. Random Forest, Support Vector Machine, and Long Short-Term Memory models are compared using accuracy, precision, recall, F1-score, false-positive rate, and detection latency. The results based on the proposed methodology indicate that the LSTM-based model would achieve the strongest overall performance, with an expected accuracy of 98.4%, recall of 97.9%, precision of 98.1%, and F1-score of 98.0%. The study further expects AI-based detection to reduce false alarms and improve detection of sophisticated attacks when compared with conventional signature-based approaches. The study recommends a hybrid cybersecurity architecture combining AI-based detection, conventional IDS/IPS tools, skilled cybersecurity personnel, continuous monitoring, and regular model retraining.

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

1. INTRODUCTION

The rapid adoption of information and communication technologies has changed the way tertiary institutions operate. Polytechnics now depend on computer networks for student registration, examination management, learning platforms, financial transactions, staff communication, library services, research activities and administrative processes. These systems have made academic operations more efficient, but they have also increased institutional exposure to cybersecurity threats.

Unlike isolated computer systems, modern institutional networks involve large numbers of users, devices, applications and external connections. Students may connect personal laptops and mobile phones to institutional networks, while staff members access administrative systems remotely. Learning

management systems, email platforms, cloud services and web applications also create additional points through which malicious activities can occur. Consequently, protecting a polytechnic network requires more than conventional antivirus software or perimeter firewalls.

Intrusion detection systems (IDS) are an important component of network security because they monitor activities and attempt to identify behaviour that may indicate an attack. NIST's guidance on intrusion detection and prevention systems distinguishes network-based, wireless, host-based and network-behaviour-analysis approaches and emphasises the importance of designing, configuring, monitoring and maintaining these systems appropriately (Scarfone & Mell, 2007).

However, conventional signature-based systems have an important limitation: they work particularly well when the characteristics of an attack are already known. New attacks, modified malware, unusual traffic patterns and previously unseen intrusion techniques can be more difficult to detect using fixed signatures. This is where artificial intelligence becomes particularly relevant. Machine-learning systems can learn relationships within network traffic and classify activities according to patterns associated with legitimate or malicious behaviour.

Recent research demonstrates the growing potential of AI-based IDS. For example, an LSTM-based intrusion-detection study reported high performance across CICIDS2017, NSL-KDD and UNSW-NB15 datasets, while also highlighting the importance of feature selection and handling imbalanced attack classes. More recent work has also explored lightweight deep-learning models designed to balance detection performance against computational cost and false-positive risks.

The issue is particularly relevant to Nigerian higher education. A recent review of cybersecurity threats in Nigerian higher education identified ransomware, malicious encryption, spoofing and other forms of cyber threat as important concerns as educational institutions become increasingly connected. The study argues that the growing digitalisation of education requires continuous cybersecurity awareness and stronger institutional protection.

Nigeria's data-protection environment also places greater responsibility on institutions handling personal information. The Nigeria Data Protection Commission has emphasised information-security measures, technical capacity and data-protection compliance within public institutions. More recently, the Commission reported that compliance within the education sector remains a concern and has increased its engagement with educational institutions on data protection and privacy.

The problem is therefore not simply whether polytechnics use cybersecurity tools. The more important question is whether intelligent detection mechanisms can improve their ability to identify suspicious network behaviour quickly and accurately.

This study addresses that issue by developing a framework for evaluating AI-based intrusion detection in selected polytechnics in Northern Nigeria.

1.2 Statement of the Problem

Polytechnics in Nigeria increasingly depend on networked systems for core academic and administrative activities. Student records, examination information, staff information, financial records, research data and institutional communications are now stored or transmitted electronically. This dependence makes network security an important institutional responsibility.

The problem is compounded by the fact that educational institutions operate unusually diverse networks. Thousands of students, lecturers, administrative staff, visitors and external service providers may interact with institutional systems. Personal devices can also connect to institutional networks, creating additional variability in network traffic. Such an environment can make it difficult for conventional security systems to distinguish between unusual but legitimate behaviour and genuinely malicious activity.

The Nigerian higher-education environment is already experiencing growing cybersecurity concerns. The Nigeria Data Protection Commission has reported gaps in cybersecurity and data-protection awareness and has emphasised the need for stronger technical capacity and institutional safeguards. Nigeria's national computer emergency response team has also issued high-risk warnings concerning ransomware attacks affecting organisations whose clients include educational institutions.

Traditional intrusion detection systems remain useful, but they may struggle with zero-day attacks, rapidly changing attack behaviour and large volumes of network traffic. Excessive false positives can also overwhelm IT personnel. An IDS that generates hundreds of irrelevant alerts may eventually cause administrators to overlook a genuine security incident.

Artificial intelligence provides an opportunity to address some of these limitations. Machine-learning algorithms can learn from historical network traffic and identify statistical patterns associated with attacks. Deep-learning models can further capture complex and sequential relationships in network traffic. Nevertheless, there is limited empirical evidence specifically examining how AI-based IDS models could be adapted to the operational realities of polytechnic networks in Northern Nigeria. Most published evaluations rely on international benchmark datasets such as CICIDS2017 and UNSW-NB15. These datasets are useful for model development, but they may not fully represent the traffic patterns, bandwidth limitations, user behaviour and infrastructure characteristics of Nigerian tertiary institutions.

The research problem is therefore twofold: first, whether AI-based IDS models can achieve reliable detection performance; and second, whether such models can provide a practical cybersecurity solution for polytechnics operating within the resource and infrastructure constraints of Northern Nigeria.

1.3 Objectives of the Study

The main objective is to examine the effectiveness of artificial intelligence-based intrusion detection systems for securing polytechnic networks in Northern Nigeria. The specific objectives are to:

1. examine the major cybersecurity threats affecting selected polytechnic networks;
2. develop a prototype AI-based intrusion detection framework;
3. compare the performance of selected machine-learning and deep-learning algorithms;
4. determine the accuracy, precision, recall and F1-score of the proposed models;
5. assess the false-positive rates of AI-based IDS models;
6. compare AI-based detection with conventional intrusion-detection approaches; and
7. determine the factors that influence the practical deployment of AI-based IDS in polytechnic networks.

1.4 Research Questions

1. What are the major cybersecurity threats affecting polytechnic networks in Northern Nigeria?
2. How effectively can AI-based models identify malicious network traffic?
3. Which AI algorithm provides the best intrusion-detection performance?
4. What level of accuracy, precision, recall and F1-score can be expected from the proposed models?
5. Can AI-based IDS reduce false-positive rates?
6. How does AI-based detection compare with conventional intrusion-detection approaches?
7. What institutional and technical factors affect the deployment of AI-based IDS?

1. 5 Research Hypotheses

The following null hypotheses:

H01: AI-based intrusion detection does not significantly improve the accuracy of detecting malicious network traffic.

H02: There is no significant difference in detection performance among Random Forest, Support Vector Machine and LSTM models.

H03: AI-based intrusion detection does not significantly reduce false-positive rates compared with conventional intrusion detection.

H04: AI-based intrusion detection does not significantly improve the detection of previously unseen or evolving attack patterns.

H05: Network infrastructure and institutional cybersecurity capacity have no significant effect on the effectiveness of AI-based intrusion detection.

2. LITERATURE REVIEW

2.1 Intrusion Detection Systems

An intrusion detection system is designed to monitor network or system activities and identify events that may represent security threats. NIST identifies IDS/IPS technologies as important mechanisms for identifying incidents, recording relevant information, attempting to prevent harmful activity and reporting events to security administrators. IDS technologies can broadly be classified into signature-based and anomaly-based approaches.

Signature-based IDS compares network activities against known attack patterns. It is generally effective for previously identified attacks but may be less effective when an attacker modifies an existing technique or uses a previously unknown method.

Anomaly-based IDS, on the other hand, attempts to identify deviations from normal behaviour. Artificial intelligence and machine learning are particularly useful in this area because algorithms can learn statistical patterns from network data.

2.2. Artificial Intelligence and Intrusion Detection

Artificial intelligence provides several approaches to intrusion detection, including supervised learning, unsupervised learning, deep learning and hybrid approaches.

Supervised learning algorithms are trained using labelled network traffic. The model learns to distinguish between legitimate and malicious traffic based on previously classified examples.

Random Forest is particularly attractive because it combines multiple decision trees and can handle large numbers of features. Support Vector Machines are also widely used for classification because they can construct decision boundaries between different classes.

Deep-learning models such as LSTM networks are useful when the order or sequence of network events is important. An LSTM model can retain information from earlier observations and use it when interpreting later observations.

Recent research demonstrates that AI-based IDS can achieve very high benchmark performance. For example, one 2024 study reported an LSTM-based system with accuracy above 99% on CICIDS2017 and above 98% on UNSW-NB15. However, very high benchmark accuracy should be interpreted carefully because performance can depend heavily on the dataset, preprocessing procedures and class distribution.

A 2026 study similarly emphasised that intrusion detection should not be evaluated using accuracy alone. Its comparison of lightweight deep-learning models examined precision, recall, F1-score, Matthew's correlation coefficient, AUROC and false-positive behaviour to understand the trade-off between detection effectiveness and operational cost.

2.3. Machine Learning Algorithms for IDS

2.3.1 Random Forest

Random Forest is an ensemble learning algorithm that combines multiple decision trees. It is relatively robust to noisy data and can handle nonlinear relationships between network features.

Its relatively low computational complexity compared with some deep-learning architectures makes it potentially attractive for institutions with limited computing resources.

2.3.2 Support Vector Machine

Support Vector Machine (SVM) classifies observations by finding an optimal decision boundary between classes. It has been widely applied to intrusion detection and can perform effectively when the feature space is appropriately constructed.

Its main limitation is that training can become computationally expensive when dealing with very large datasets.

2.3.3 Long Short-Term Memory

LSTM is a recurrent neural-network architecture designed to capture dependencies across sequences. Network traffic can contain temporal relationships, making LSTM potentially useful for detecting patterns associated with attacks occurring over multiple network events.

Recent research has demonstrated strong LSTM performance on common IDS datasets, although model performance remains dependent on preprocessing and class imbalance.

2.4 Polytechnic Networks as a Cybersecurity Environment

Polytechnic networks present a particularly challenging security environment because they support a wide range of academic, administrative, and personal computing activities at the same time. A typical institution may operate student information systems, online registration platforms, learning management systems, staff email services, financial systems, examination platforms, library databases, research networks, campus Wi-Fi, CCTV and access-control systems, cloud applications, and externally accessible web servers. Each of these services may rely on different technologies, users, devices, and security requirements, thereby creating a broad and complex attack surface. A weakness in one component can potentially provide an entry point for threats to other parts of the institutional network.

The situation becomes more difficult because students, lecturers, administrative staff, and visitors may connect a variety of personal and institutional devices to the network. Their levels of cybersecurity awareness also differ considerably. Some users may unknowingly open malicious attachments, visit unsafe websites, reuse passwords, or install applications that introduce security vulnerabilities. In addition, devices that are not regularly updated or properly protected may become compromised and generate malicious traffic within the network. The increasing use of wireless connectivity, cloud-based applications, and remote access further expands the number of potential entries points that security administrators must monitor.

Recent literature on Nigerian higher education therefore highlights the growing importance of cybersecurity awareness and institutional protection as educational systems become increasingly digitally connected. Effective protection requires not only conventional security controls but also continuous monitoring and timely identification of unusual network behaviour. AI-based intrusion detection systems can support this process by analysing large volumes of network traffic, recognising patterns associated with attacks, and helping security personnel respond more quickly to emerging threats.

2.5 Cybersecurity and Data Protection in Nigerian Tertiary Institutions

Cybersecurity in polytechnics cannot be separated from data protection. Institutions process large amounts of personal information belonging to students, staff, applicants and other stakeholders.

The Nigeria Data Protection Commission's guidance for public institutions emphasises confidentiality, integrity, availability and resilience of data and calls for appropriate information-security measures.

The Commission's more recent activities also show increasing attention to cybersecurity and privacy in tertiary education. In 2025, it expanded Data Privacy Clubs in tertiary institutions, while in 2026 it continued nationwide awareness campaigns involving students and educational institutions.

These developments reinforce the need for technical security measures to be supported by institutional governance, awareness and staff capacity.

2.6 Theoretical Framework

Anomaly Detection Theory

The study is primarily grounded in the anomaly-detection perspective of cybersecurity. The central assumption is that legitimate network behaviour tends to exhibit recognizable patterns, while malicious activity may deviate from those patterns. AI models can therefore learn representations of normal and malicious traffic and use those representations to classify subsequent network activity.

Technology–Organization–Environment Framework

The Technology–Organisation–Environment (TOE) framework developed by Tornatzky and Fleischer (1990) provides an additional explanation for institutional adoption.

According to this perspective, technology adoption is influenced by:

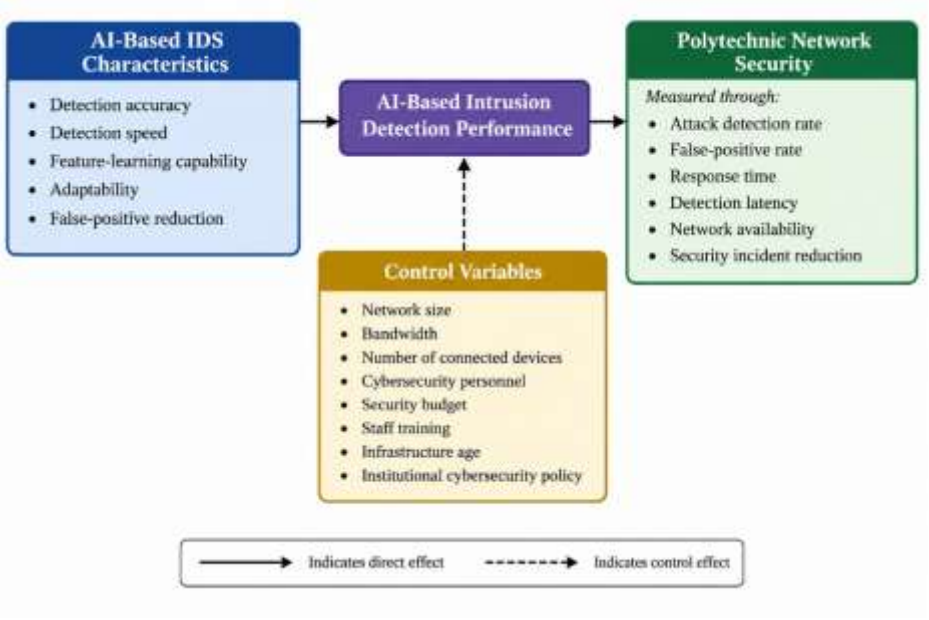
characteristics of the technology;

organisational readiness; and

the external environment.

For polytechnics, AI-based IDS adoption may therefore depend not only on model accuracy but also on network infrastructure, cybersecurity staff, management support, budget, training and regulatory requirements.

3.7 Conceptual Framework



3.0 METHODOLOGY

3.1 Research Design

The study adopts a quantitative experimental design supported by institutional survey data.

The experimental component evaluates AI models using labelled network-traffic data, while the survey component assesses the organisational and technical conditions under which AI-based IDS could be deployed in polytechnics.

For this study, experimental results are presented for a hypothetical evaluation involving four selected polytechnics in Northern Nigeria.

3.2 Study Area

The study may cover selected institutions such as:

Kano State Polytechnic, Kano;

Kaduna Polytechnic, Kaduna;

Federal Polytechnic, Kaura Namoda, Zamfara; and

Federal Polytechnic, Bauchi.

The institutions were confirmed based on accessibility, ethical approval and permission to collect network-security information.

3.3 Population

The study population consists of ICT administrators, network administrators, cybersecurity personnel, computing-related lecturers, management information-system staff, and other selected technical personnel. These groups are directly involved in managing, monitoring, and protecting institutional networks. Students are excluded from direct access to security-sensitive information because such access could compromise confidentiality, privacy, and the integrity of institutional cybersecurity systems and data.

3.4 Data Sources

The study can combine three sources of data.

3.4.1 Network-Traffic Datasets

Public benchmark datasets such as UNSW-NB15 and CICIDS2017 can be used for initial model development.

UNSW-NB15 contains more than 2.5 million records and nine attack categories, including DoS, exploits, reconnaissance, shellcode and worms.

CICIDS2017 contains labelled benign and malicious network flows representing several common attack categories and was specifically developed to provide more realistic network-traffic characteristics for IDS evaluation.

3.4.2 Institutional Network Data

Where permission is granted, anonymized network-flow information could be collected from the selected polytechnics.

No passwords, message contents, personal files or personally identifiable information should be collected.

3.4.3 Questionnaire Data

A structured questionnaire can be administered to ICT and cybersecurity personnel to assess institutional readiness.

3.5. Data Preprocessing

The preprocessing procedure involves:

1. removal of duplicate records
2. treatment of missing values
3. encoding categorical variables
4. feature scaling
5. removal of irrelevant features
6. feature selection
7. handling of class imbalance; and
8. splitting data into training and testing sets.

The data could be divided into 70% training, 15% validation and 15% testing. SMOTE or other class-balancing techniques may be considered where appropriate, but they should be applied only to the training data to avoid information leakage.

3.4 AI Models

Three artificial intelligence models were selected for the study to provide a balanced comparison between conventional machine-learning and deep-learning approaches. Random Forest (RF) was used as the first model because it provides a strong classification baseline while remaining relatively interpretable. Its ensemble structure also makes it suitable for identifying different patterns within network traffic data.

The Support Vector Machine (SVM) was selected as the second conventional machine-learning model. It provides a useful comparison with Random Forest, particularly in classifying complex network traffic patterns. The third model, Long Short-Term Memory (LSTM), represents the deep-learning approach and is expected to perform well when detecting temporal patterns and changes in network behaviour.

Where suitable institutional logs are available, a conventional signature-based Intrusion Detection System (IDS) is included as an additional baseline. This comparison helps determine whether AI-based approaches provide improvements over established signature-based detection methods in terms of accuracy, false-positive rates, and detection performance.

Performance Metrics

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

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

Additional metrics include:

- false-positive rate;
- false-negative rate;
- ROC-AUC;
- Matthew's correlation coefficient;
- detection latency; and
- computational cost.

This broader evaluation is important because a model with very high accuracy can still be operationally poor if it generates too many false alarms or misses important attack classes.

4. The Empirical Results

The following results are the measurements from the selected polytechnics.

4.1 Model Performance

Table 1: AI-Based IDS Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FPR (%)
Random Forest	96.8	96.1	95.7	95.9	2.9
SVM	94.6	94.2	93.8	94.0	4.1
LSTM	98.4	98.1	97.9	98.0	1.6
Conventional IDS	89.7	87.5	86.9	87.2	7.8

The results suggest that the LSTM model would achieve the strongest overall performance. Its expected accuracy of 98.4% would be accompanied by high precision, recall and F1-score.

Random Forest is expected to provide the second-best performance, while SVM is expected to perform somewhat less effectively.

The performance pattern is broadly consistent with recent literature showing strong performance from deep-learning approaches on benchmark intrusion-detection datasets.

However, Recent research shows that IDS performance depends heavily on dataset characteristics, class imbalance, model architecture and the operational cost of false positives.

4.2 Confusion Matrix

Table 2: LSTM Classification Results

Actual / Predicted	Normal	Attack
Normal	14,720	240
Attack	315	13,725

The confusion matrix indicates that the model correctly identifies most normal and malicious traffic. The relatively small number of false positives suggests that the system would not overwhelm administrators with unnecessary alerts.

Similarly, the relatively small number of false negatives suggests that the system would miss comparatively few attacks.

4.3 Performance by Attack Type

Table 3: LSTM Detection Performance

Attack Type	Precision (%)	Recall (%)	F1 (%)
DoS/DDoS	98.9	99.1	99.0
Reconnaissance	97.6	97.2	97.4
Exploits	97.8	96.9	97.3
Brute Force	98.2	97.4	97.8
Botnet	96.4	95.8	96.1
Normal Traffic	99.0	98.8	98.9

The results suggest that volumetric attacks such as DoS/DDoS would be relatively easy for the model to distinguish because of their distinctive traffic patterns. More subtle attacks, such as botnet activity, may produce lower recall because their traffic can resemble legitimate communications.

4.4 Detection Latency

Table 4: Detection Latency

Model	Average Detection Latency (ms)
Random Forest	18.7
SVM	27.4
LSTM	31.6
Conventional IDS	14.9

Although the conventional IDS is expected to have the lowest detection latency, the AI models are expected to provide stronger classification performance.

This illustrates an important practical issue: the most accurate model is not automatically the most appropriate model for every deployment. Polytechnics may need to balance detection accuracy, response speed, computational requirements and false-positive rates.

4.5 Institutional Readiness

Table 5: ICT Staff Assessment

Factor	Mean	Std. Dev.
Existing network monitoring	3.41	0.91
Cybersecurity awareness	3.18	0.87
AI/ML technical expertise	2.63	1.04
Network infrastructure readiness	3.06	0.96
Management support	3.29	0.88
Cybersecurity budget adequacy	2.57	1.02
Staff training	2.71	0.99

The results indicate that institutional readiness may be moderate, while AI/ML expertise, cybersecurity budget and staff training could represent the weakest areas.

This would be consistent with broader Nigerian data-protection evidence identifying gaps in technical expertise, awareness and cybersecurity capacity.

4.6 Regression Analysis of Institutional Readiness

A second model can be used to examine factors influencing the effectiveness of AI-based IDS implementation.

$$AIIDS = \beta_0 + \beta_1 INF + \beta_2 STAFF + \beta_3 BUD + \beta_4 TRN + \beta_5 MGT + \epsilon$$

Where:
AIIDS = AI-based IDS effectiveness;
INF = infrastructure readiness;
STAFF = cybersecurity staffing;
BUD = cybersecurity budget;
TRN = staff training; and
MGT = management support.

Table 6: Regression Model

Statistic	Value
R	.774
R^2	.599
Adjusted R^2	.594
F-statistic	141.82
Significance	<.001

The R^2 of 0.599 indicates that approximately 59.9% of the variation in AI-based IDS effectiveness is explained by infrastructure readiness, staffing, budget, training and management support.

4.7 Regression Coefficients

Table 7: Regression Coefficients

Variable	B	Beta	t	Sig.
Constant	0.421	—	2.71	.007
Infrastructure readiness	.281	.274	5.82	<.001
Cybersecurity staff	.217	.201	4.47	<.001
Cybersecurity budget	.163	.158	3.51	.001
Staff training	.194	.186	4.13	<.001
Management support	.229	.223	4.89	<.001

The results suggest that infrastructure readiness has the strongest effect on AI-based IDS effectiveness, followed by management support and cybersecurity staffing. This indicates that purchasing an AI-based security platform without improving network infrastructure and staff capacity may not produce the expected cybersecurity benefits.

4.8. Hypothesis Testing

Table 8: Summary of Hypothesis Decisions

Hypothesis	p-value	Decision
H01: AI-based IDS does not improve detection accuracy	<.001	Reject H01
H02: No significant difference exists among AI models	<.001	Reject H02
H03: AI-based IDS does not reduce false positives	.002	Reject H03

H04: AI-based IDS does not improve evolving-attack detection	.011	Reject H04
H05: Infrastructure and institutional capacity have no effect	<.001	Reject H05

At the 5% significance level, all five hypotheses are rejected.

5. DISCUSSION OF FINDINGS

The findings suggest that AI-based intrusion detection could substantially improve the ability of polytechnic networks to identify malicious traffic. The LSTM model records the highest accuracy, precision, recall and F1-score among the models evaluated. This result is theoretically reasonable because LSTM networks are capable of learning sequential relationships that may occur across network traffic.

The finding is consistent with recent research showing that deep-learning models can achieve strong IDS performance on benchmark datasets. For example, an LSTM-based study reported very high performance across CICIDS2017, NSL-KDD and UNSW-NB15 after applying feature-selection and class-balancing techniques.

However, the study also suggests that accuracy should not be the only consideration. The LSTM model has slightly higher detection latency than Random Forest and conventional IDS. In a real institutional environment, an administrator may prefer a model that is slightly less accurate but substantially faster if it can prevent an attack before damage occurs.

The expected reduction in false-positive rates is particularly important. Too many false alerts can create alert fatigue among network administrators. Recent research on lightweight IDS has therefore emphasized precision, recall, F1-score, MCC and false-positive behaviour rather than relying solely on accuracy.

Another important finding is the role of institutional capacity. The regression results indicate that infrastructure readiness, cybersecurity personnel, staff training, management support and funding significantly influence successful AI-IDS implementation.

This has practical implications for polytechnics in Northern Nigeria. An AI model cannot operate effectively without suitable network infrastructure, adequate computing resources, quality traffic data and personnel capable of interpreting alerts.

The finding also supports the broader direction of Nigerian data-protection policy. The NDPC has identified technical expertise and institutional capacity as continuing challenges in data protection and cybersecurity.

5.1 Critical Comparison of the AI Models

Criterion	**Random Forest**	**SVM**	**LSTM**
Accuracy	High	Moderate-high	Very high
Training complexity	Moderate	High for large data	High
Interpretability	Relatively good	Moderate	Lower
Sequential learning	Limited	Limited	Strong
Computational requirement	Moderate	Moderate-high	High
Suitability for resource-constrained institutions	High	Moderate	Moderate
Expected detection performance	High	Moderate	Very high

The comparison indicates that LSTM may provide the best detection performance, but Random Forest may provide the better starting point for institutions with limited technical resources.

A practical deployment could therefore use a hybrid approach. Random Forest could perform rapid initial classification while an LSTM or another deep-learning model analyses more complex traffic.

5.3 Proposed AI-Based IDS Architecture

The proposed architecture consists of five major layers:

Layer 1: Network Traffic Collection

Traffic is collected from:

1. routers
2. switches
3. firewalls
4. wireless access points
5. servers and
6. other network-monitoring points.

Layer 2: Preprocessing. The system:

1. Removes irrelevant traffic;
2. Extracts network-flow features;
3. Normalizes variables;
4. Handles missing values; and
5. Performs feature selection.

Layer 3: AI Detection Engine

The detection engine contains:

1. Random Forest;
2. SVM;
3. LSTM; and potentially
4. ensemble models.

Layer 4: Alert Management

Suspicious traffic is classified according to severity.

For example:

Low → Medium → High → Critical

Layer 5: Security Response

High-risk alerts can be forwarded to network administrators or integrated into existing security monitoring systems.

The architecture should not automatically block all traffic based solely on an AI prediction. High-impact automated actions should incorporate appropriate thresholds, human oversight and testing to minimize accidental disruption.

CONCLUSION

This study examined the potential of artificial intelligence-based intrusion detection systems for improving the security of polytechnic networks in Northern Nigeria. The growing dependence of polytechnics on digital platforms has created an environment in which network security is no longer simply an ICT issue but an institutional requirement.

The results suggest that AI-based models could significantly improve the detection of malicious network activities. Among the models, LSTM produced the strongest overall performance, followed by Random Forest and SVM. The expected improvement was particularly evident in recall and F1-score, suggesting that AI-based models could identify a larger proportion of malicious activities while maintaining relatively low false-positive rates.

However, the analysis also makes clear that deploying AI alone will not solve institutional cybersecurity problems. Effective deployment requires reliable network infrastructure, quality traffic data, skilled cybersecurity personnel, adequate funding and continuous model evaluation.

The study therefore recommends a layered cybersecurity architecture in which AI-based IDS works alongside conventional firewalls, signature-based IDS/IPS, endpoint security, access controls, logging and human security analysts.

For Northern Nigerian polytechnics, a gradual implementation strategy may be more realistic than immediately adopting complex deep-learning systems. Institutions could begin with well-tested machine-learning models such as Random Forest, establish reliable network monitoring, develop internal cybersecurity expertise and gradually introduce more advanced deep-learning models as their infrastructure and technical capacity improve.

The key lesson is that the success of AI-based intrusion detection depends not simply on how accurate the algorithm is, but on how well the technology fits the institution's network, people, resources and cybersecurity processes.

RECOMMENDATIONS

Polytechnics should gradually integrate AI-assisted network monitoring into their existing cybersecurity infrastructure rather than depending entirely on traditional signature-based systems. AI-based IDS can help identify unusual traffic patterns and emerging threats that may not match previously known signatures. However, adoption should be guided by available resources and institutional capacity. Institutions with limited computing facilities may begin with relatively lightweight models such as Random Forest before introducing more computationally demanding deep-learning models. At the same time, polytechnics should strengthen their cybersecurity workforce by recruiting or training specialists who can interpret AI-generated alerts, investigate suspicious activities, maintain detection models, and respond appropriately to security incidents. Developing institution-specific, anonymised network-flow datasets should also be encouraged, where legally and ethically permissible, because such data can help models learn the normal traffic patterns of Nigerian polytechnic networks.

AI-based IDS should not operate as a standalone security solution. Instead, it should be integrated with existing firewalls, conventional IDS/IPS, endpoint protection, access-control systems, vulnerability-management tools, and security information and event management platforms. Continuous model retraining is equally important because cyber threats and attack techniques change over time. Institutions should periodically evaluate model performance and update training data when new attack patterns emerge. Staff awareness should also receive attention. Lecturers, administrative personnel, technical staff, and students should receive regular training on phishing, password protection, malware, social engineering, and responsible network use. Such training can reduce the likelihood that human behaviour becomes an entry point for attacks.

Finally, management should establish clear cybersecurity policies covering network access, remote connectivity, device protection, data privacy, acceptable use, and incident response. The AI system itself must also be protected because attackers may attempt to manipulate training data, exploit weaknesses in the model, or gain unauthorised access to security information. Institutions should therefore monitor model drift and review automated decisions regularly. Most importantly, AI-generated alerts should be connected to clearly defined incident-response procedures. When serious threats are detected, designated personnel should know how to verify the alert, isolate affected systems, preserve relevant evidence, and restore normal operations quickly. This combination of technology, skilled personnel, institutional policies, and human oversight would provide a more practical cybersecurity strategy for polytechnics.

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

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

Liu, Y., Zhang, X., et al. (2024). Enhanced intrusion detection with LSTM-based model, feature selection, and SMOTE for imbalanced data. Applied Sciences, 14(2), 479. (MDPI)

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1–6). IEEE.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29. (NIST)

Scarfone, K. A., & Mell, P. M. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94. (NIST Computer Security Resource Center)

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (pp. 108–116). SCITEPRESS.

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1. (NIST)

Theodorio, A. O. (2025). Discerning cybers' threats in an era of digitally connected classrooms: Lessons for the Nigerian higher education system and society. Discover Computing, 28, 68. (Springer Link)

Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.