Available online at
https://mijuitm.com.my

e-ISSN: 2735-0703

Mathematical Sciences and Informatics Journal 7(1) 2026, 102 – 113.

Mathematical Sciences and Informatics Journal

Machine Learning Threat Prediction and Classification Framework for IoT-Enabled 5G Networks

Samuel Robinson[1], Moses Ekpenyong[1,2,3,4*], Anthony Imianvan[5], Efosa Igodan[5]

[1]*Department of Cyber Security, Faculty of Computing, University of Uyo, Nigeria*
[2]*Department of Computer Science, Faculty of Computing, University of Uyo, Nigeria*
[3]*STEM Centre, University of Uyo, Nigeria*
[4]*Centre for Research, University of Uyo, Nigeria*
[5]*Department of Computer Science, Faculty of Computing, University of Benin, Benin City, Nigeria*

ARTICLE INFO

Article history:
Received 29 December 2025
Revised 13 March 2026
Accepted 27 March 2026
Online first
Published 30 April 2026

Keywords:
Internet of Things
intrusion detection system
prediction
security threat
machine learning
5G Networks

DOI:
10.24191/mij.v7i1.11579

ABSTRACT

The proliferation of smart devices for a wide range of applications in fifth-generation (5G) networks has raised serious security concerns about network threats, especially at the perception, network, and application layers. The existing methods for Internet of Things (IoT) network security have made strides, but significant room for improvement remains in building defence mechanisms against attacks at the application and protocol levels. The problems of overhead implementation, single attack detection, and poor classification and detection approaches are pertinent. This paper aims to develop machine learning models for improved IoT network security through timely and accurate threat prediction. The objective is to use AdaBoost, decision trees, and artificial neural networks (ANN) to detect normal and threat patterns in IoT networks. We employed the wireless network intrusion detection (ID) dataset sourced from the NSL-KDD repository, which contains a total of 148,517 data points split into 125,973 training datasets and 22,544 testing datasets. Findings indicate that the decision tree (DT) outperformed AdaBoost and ANN with an accuracy of 99%, 84%, and 68%, respectively. However, deploying the framework in real-time network environments using fog computing platforms is recommended to determine its efficiency in real-world scenarios.

1,2,3,4* Corresponding author. *E-mail address*: mosesekpenyong@uniuyo.edu.ng
https://doi.org/10.24191/mij.v7i1.11579

1. INTRODUCTION

The advancements in smart technology have revolutionized network traffic and congestion management. IoT systems utilize low-power sensors, requiring automation of traffic optimization functions to reduce manual intervention. IoT and wireless communication have enabled real-time traffic monitoring and congestion detection, requiring secure techniques for swift issue identification. The integration of smart devices drives the IoT, enables efficient management of network facilities, and enhances connectivity. A 2019 report shows that 85% of industries utilized smart devices, and in 2020, the figure rose to 91%. However, the usage rate decreased by 90% in 2021. According to the report, the most important benefits of using IoT technology are high-quality service delivery and enhanced productivity (Sengupta & Sil, 2020). However, security threats pose severe consequences, including unauthorized access and data tampering. This could result in poor network connectivity and cyber threats in the transmission channel (RajeshKumar et al., 2016). A machine learning (ML) approach to intrusion detection systems (IDSs) in the IoT network environment must consider the patterns of attacks and the methods used for intrusion detection (Alosaimi & Almutairi, 2023). In IoT networks, connections are vulnerable because IoT devices are not designed to manage IDSs across different categories of security threats (Wójcicki et al., 2022).

The revolution of IoT greatly influences the daily lives of mobile operators as demonstrated by Ekpenyong et al. (2022), who focused on routing optimization for preferred parents (PPs) selection in low-power and lossy networks (LLNs). The study presented strengths and weaknesses in the metrics adopted, along with methods to address the identified gaps. Appropriate deployment of IDS metrics leads to efficient detection and reduction of false alarms, hence improving network performance (Raza et al., 2013). In the IoT environment, the implementation characteristics indicate that devices operate within an extensive network used for processing large amounts of data (Robinson et al., 2025). A study on this issue indicates that the false positive rate refers to normal traffic incorrectly classified as malicious activity due to poor discrimination by IDSs (Usha & Kavitha, 2017). The existing metrics systems for IoT intrusion detection are static and cannot adapt to the dynamic, complex environment of the IoT ecosystem, which leads to the misinterpretation of normal actions as malicious threats.

To address these challenges, a machine learning approach is employed to learn complex patterns and improve accuracy in detecting the malicious and normal traffic flows in the 5G network spectrum. Machine learning tools such as the AdaBoost classifier, decision tree (DT), and artificial neural networks (ANN) are used to analyse data from various parts of the IoT network and identify DoS attacks on the network (ElKashlan et al, 2023). The objectives are to predict the presence of attacks on IoT devices/networks and identify the DoS attacks in 5G IoT-enabled applications. The performance of the proposed system is evaluated using accuracy, F1-score, precision, and recall metrics. This work contributes to reducing false positives and negatives and provides a cost-effective and efficient threat detection approach. It also produces more robust defences against cyber threats by ensuring the integrity and confidentiality of IoT data and supporting strategic decision-making in network management. The paper is organized as follows. Section 2 presents related works, while Section 3 presents the methodology for ID in IoT networks. Section 4 discusses the results, and Section 5 concludes the paper with directions for future work.

2. RELATED WORKS

The rapid growth of IoT utilization and insufficient security measures has created new risks and security challenges in the network space. Cyber attackers use IoT devices as amplification platforms to launch attacks, such as distributed denial of service (DDoS) attacks. Liu et al. (2023) investigated the sensing capabilities of IoT to improve connectivity and reduce intrusion and interference in the link using the empirical method. The result shows that the urban scene antenna is down-tilted at an angle of 6^0, and the

https://doi.org/10.24191/mij.v7i1.11579

rural scene antenna is down-tilted at an angle is 3^0, with a maximum antenna gain of 24.46dB (Li et al., 2018).

However, the work only focused on the co-channel interference between the 5G base station (BS) and the Air-to-Ground (ATG) and Customer Premises Equipment (CPE) terminal in the 3.5 GHz range. Other factors, such as interference and frequency ranges, were not taken into consideration. The vulnerability threat of smart devices may be due to low power and computation requirements (Sarhan et al., 2022). The authors proposed an artificial neural network (ANN) based on a threat detection mechanism to determine the range of data integrity attacks in IoT systems. The work deployed the data, which contained different threats, including backdoors, generic, fuzzes, exploits, shellcode, analysis, worms, DoS, and reconnaissance. The information is stored in the neural network in the form of weights.

Deep learning (DL) and three-level algorithms were utilized for threat detection in IoT device connection (Otoum et al., 2022). The algorithms produced 99.8% accuracy in detecting attack types. However, it is computationally intensive. Baniasadi et al. (2022) conducted a study on ML-based such as Bayes classifier, filter classifier, and J48 classifier, for IDSs in IoT electric vehicle charging stations (EVCSs). The Bayes classifier algorithm gave a response time of 0.3 seconds with an accuracy of 77% while the J48 classifier yielded a response time of 4.22 seconds and 99.2 % accuracy. The filter classifier produced a response time of 2.81 seconds and an accuracy of 99.2%. It is highly data dependent.

Roopak (2021) used network IDS (NIDS) datasets to address the lack of a unique and proprietary set of features for each publicly available dataset. The result shows that the benign class has seen a notable increase in detection rate (DR) from 71.70% to 93.45% with the F1-score. Deep learning and IDS were investigated to determine threats in IoT transmission lines. Threats, including DoS, user-to-root (U2R), and remote-to-local (R2L) were examined (Ferrag et al., 2020). The authors used spider monkey optimization (SMO) and stacked deep polynomial techniques to obtain an efficient. The SMO produced 96%, while DL-IDS yielded 99.02% accuracy, a precision of 99.38%, a recall of 98.91%, and an F1-score of 99.14%. Other deep learning-based IDS, which achieves a lower accuracy of 98.27%, precision of 88.85%, recall of 96.50%, and F1-score of 92.52%. This work may not be able to detect all types of security threats and interference in IoT environments. The performance of DL-IDS may be affected by uncertain data in real-time environments, including interference.

Susilo and Sari (2020) addressed the challenge of improving intrusion detection in IoT systems by deploying a neighbourhood search-based particle swarm optimization (NSBPSO) with a deep convolutional neural network (DCNN). The NSBPSO-DCNN model outperformed conventional DCNN and other metaheuristic-optimized models, achieving 99.41% accuracy on the University of New South Wales Network-Based 2015 (UNSW-NB15) and Bot-IoT datasets, thus filling the gap of limited exploitation exploration balance in conventional PSO for IoT intrusion detection. However, the work is constrained by high computational cost. This work is limited by the effect of energy utilization, the overhead cost of implementation, and interference caused by the environment.

Mudgerikar et al. (2019) investigated an IDS for IoT networks that can detect DDoS attacks using a hybrid approach of DL and multi-objective optimization. The results yield 99.03% accuracy with a minimal training time. Real-time distributed threat intrusion detection system (RDTIDS) with hybrid classifier methods based on decision tree and rules-based concepts, such as reduced error pruning tree, JRip algorithm, and random forests (RF), was examined (Saba et al., 2022). The results show that the true negative rate (TNR) for the Benign traffic was highest for RDTIDS (98.855%) and lowest for J48 (92.650%). However, limited to high computational cost.

https://doi.org/10.24191/mij.v7i1.11579

Huang et al. (2016) developed intelligent network-based security solutions to detect IoT network attacks using ML algorithms. The authors applied seven different ML including RF, K-Nearest Neighbours, DT, Naive Bayes, SVM, Logistic Regression, and MLP algorithms to 10 different attack types using a new dataset called Bot-I. The models were evaluated using F-measure. The Naive Bayes algorithm gave an F-measure of 0.77. The Quadratic Discriminant Analysis (QDA) technique achieved an F-measure of 0.86. The RF, ID3, and AdaBoost algorithms all achieved an F-measure of 0.97, which means they had high performance in detecting cyber-attacks in the Bot-IoT dataset. The Multilayer Perceptron (MLP) algorithm achieved an F-measure of 0.83. The KNN algorithm yielded an F-measure of 0.99, which outperformed other machine learning algorithms. The study is limited by the lack of real-world IoT network data and the overhead cost of computation.

Rajawat et al. (2021) proposed a lightweight intrusion detection system that can detect various stealthy attack types in real time and extract semantic relationships among features. The goal is to enhance the intrusion detection system (IDS) for IoT networks (Guerra-Manzanares et al., 2020). The authors deployed knowledge graphs, statistical analysis, and the CNN-BiLSTM model. The system was able to identify normal requests, DoS attacks, and Probe attacks, with F1-scores of 0.9107, 0.9273, and 0.8849, respectively. However, it could not identify encrypted or obfuscated malicious networks.

2.1 Distributed IDS in Fog Computing

Fog computing processes a large amount of data locally. It operates on portable premises that are deployed on network devices. These devices are vulnerable to threats. These attacks usually take place in fog layers. These layers include the lowest tier, intermediate tier, and highest tier. The lowest tier is used to monitor sensors and actuators to gather and preprocess data. Intermediate tiers are used for data filtering, compression, and conversion from the lower layer. The highest tier is close to the cloud, which is used for data aggregation and knowledge construction. Kumar et al. (2022) developed a distributed intrusion detection system (IDS) using fog computing to secure blockchain-enabled IoT networks against DDoS attacks. The RF and XGBoost models were utilized on the BoT-IoT dataset. The system produced high accuracy of detection rates and low false alarm rates in both binary and multi-class classifications. The fog paradigm improved decentralized security, handling threats at the network edge. However, challenges such as overhead cost, interference, and vulnerabilities across IoT's perception, network, and application layers remain (Huang et al., 2016; Otoum et al., 2022).

3. METHODOLOGY

The proposed method utilizes ANN, AdaBoost, and DT to enhance the detection and classification of threats in 5G IoT-enabled applications. This integration aims to address the shortcomings of existing IDS prediction models.

3.1 Data Collection

The IoT data from the Network Security Laboratory Knowledge Discovery and Data Mining (NSL-KDD) repository consists of various threat parameters that are utilized for analysing the pattern of threats. The dataset is pre-processed to remove messy information for quality ML modelling as depicted in Fig. 1.

https://doi.org/10.24191/mij.v7i1.11579

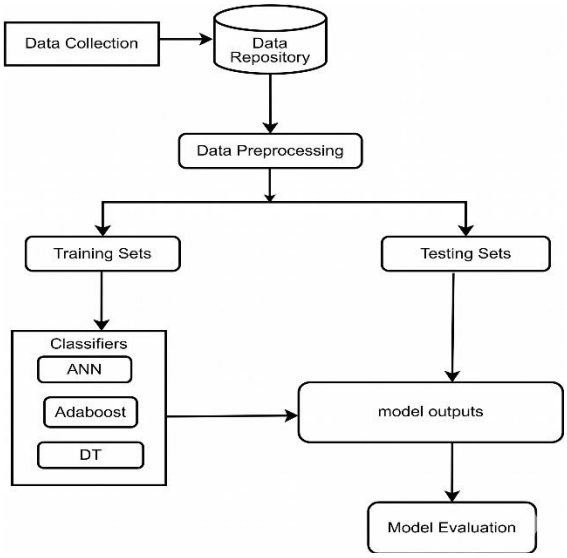

Fig. 1. Hybrid ML Architecture for Threat Prediction in 5G-Enabled IoT Device

3.2 Data Repository

The data was collected from the NSL-KDD repository. It is a benchmark data repository used for evaluating intrusion detection systems (Zwayed et al., 2021). It contains one hundred twenty-five thousand, nine hundred seventy-three (125,973) data variables with 41 features consisting of numerical and categorical variables that characterize different network traffic behaviours. The split train-test method is deployed to partition the data into 80% training sets and 20% testing sets. The data analysis is carried out using Python libraries such as matplotlib, pandas, numpy, and seaborn. The libraries manipulate the data variables and provide insight into the distribution pattern of variables, correlations among features, and the presence of anomalies within the dataset.

3.3 Artificial Neural Network (ANN)

ANN is deployed to discover the underlying probability distribution of a set of input data. This model deploys the instances of threat in the dataset. This is done by analysing anomalies in IoT dataset patterns and establishing relationships within the data, as shown in Equation (1) (Rajawat et al., 2021).

$$P(v,h) = \frac{e^{-E(v,h)}}{Z}, \tag{1}$$

where $P(v,h)$ is the probability of the configuration with visible units, Z is the partition function for normalization, $E(v,h)$ is the energy associated with the configuration. It is defined as the negative of the log-likelihood of the configuration and is given by Equation (2):

$$E(v,h) = -\sum_i \sum_j v_i h_j w_{ij} - \sum_i a_i v_i - \sum_j b_j h_j, \tag{2}$$

where $E(v,h)$ is the energy of the restricted Boltzmann machine (RBM), w_{ij}represents the weight (connection strength) between the visible unit i and the hidden unit j, a_i , b_i are the biases associated with the visible unit i and hidden unit j.

https://doi.org/10.24191/mij.v7i1.11579

3.4 Decision Trees (DT)

It is a non-parametric method used to reduce the noisy information in making complicated decisions due to a low level of bias and variance (Imianvan & Robinson, 2024; Inyang et al., 2021). The algorithm DT shows the procedures for IoT connectivity as described in an algorithm for the decision tree:

Algorithm for Decision Tree

1. Input: Assume the IoT data is given as $D = \{x^{(i)}, y^{(i)}\}_{i=1}^{N}$, where $x^i \in X \ and \ y^{(i)} \in D$ typical $X = R^d \ and \ D = R^k$
2. Output: Split the node t
3. Compute a function $f \ \forall \ f: X \rightarrow D$ the error $e = \sum_i |x^{(i)}, y^{(i)}|^2$ is small
4. Construct a tree with a node $t \in T$ corresponding to a subset of X
5. Calculate the average y-value $\underline{y}(t)$ of the data on the node t as given in $\underline{y}(t) = \frac{1}{N(t)} \sum_{x^{(i)} \in t} y^{(i)}$
6. Compute the square error rate $r(t)$ of the node t as on the node $r(t) = \frac{1}{N(t)} \sum_{x^{(i)} \in t} (y^{(i)} - \underline{y}(t))^2$
7. Determine the variance of the node t, which is an estimator as $var(Y|X \in t) = \sigma^2(Y|X \in t)$
8. Find the cost of the node $R(t) = \frac{1}{N(t)} \sum_{x^{(i)} \in t} (y^{(i)} - \underline{y}(t))^2$
9. Split a node t into t_L and t_R then $R(t) \geq R(t_L) + R(t_R)$.
10. This equality holds $iff \ \underline{y}(t) = \underline{y}_{t_L} = \underline{y}_{t_R}$; then $R(t) \geq \frac{1}{N} \sum_{x^{(i)} \in t_L} \left(y^{(i)} - \underline{y}(t_L) \right)^2 + \frac{1}{N} \sum_{x^{(i)} \in t_R} (y^{(i)} - \underline{y}(t_R))^2$.

3.5 AdaBoost Approach

This harnesses the strength of weak classifiers to build a robust classifier. During its training phase, it iteratively trains weak learners T times. As the training progresses, it adjusts the weights of misclassified samples by increasing them, while decreasing the weights of correctly classified samples, as described in Equation (3) (Suganya & Rajan, 2021).

$$S = (x_1, y_1), \ldots, (x_n, y_n), \tag{3}$$

with size N as i^{th} input, and in a domain space, x_1 is a vector value,y_1, x_1 are label spaces of Y.

4. RESULTS AND DISCUSSION

Table 1 shows that the training and validation accuracy of ANN is 0.68. This shows that ANN correctly predicts the target variable for approximately 68% of the data points in the dataset, precision of 70%, which identifies instances of class 0 (normal) and the recall of 0.64 shows that the performance of the system is moderate in detecting threats, and cost of implementation as depicted in Fig. 2.

https://doi.org/10.24191/mij.v7i1.11579

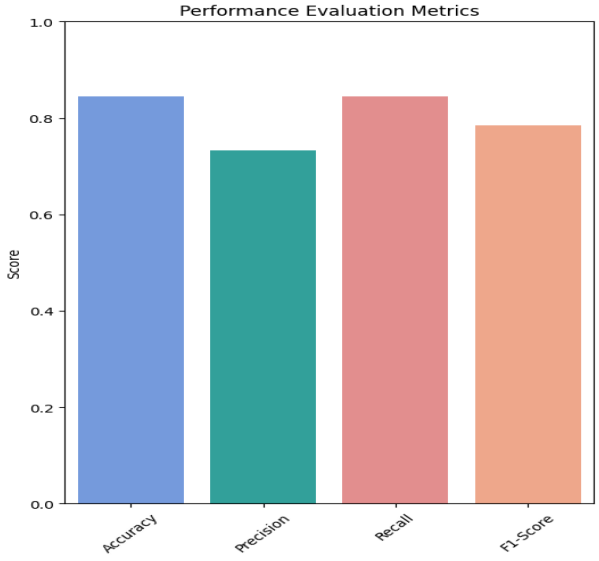

Fig. 2. Evaluation Performance of ANN

Table 1. System Performance

Classifier	Accuracy	Precision	F1-Score	Recall
ANN	0.68	0.70	0.68	0.64
DT	0.99	0.99	0.99	0.99
AdaBoost	0.84	0.73	0.84	0.78

Table 1 shows the DT model yields high precision, recall, and F1-score values of 0.99. This signifies its effectiveness in identifying security threats and vulnerabilities in IoT-enabled networks while maintaining a low rate of false alarms and missed detections. This signifies good performance in detecting and classifying various classes of DoS threats at low cost, as depicted in Fig. 3.

Fig. 3. DT Intrusion Detection Class Level

https://doi.org/10.24191/mij.v7i1.11579

Table 1 also shows that the AdaBoost model correctly classified 84% of the total instances in the dataset, a precision score of 84%. The model correctly identified 78% of all actual positive instances in the dataset, and an F1 score of 84% indicates that the model achieves a good balance between precision and recall. This exhibits good model performance in detecting various classes of threat at reduced cost, as shown in Fig. 4.

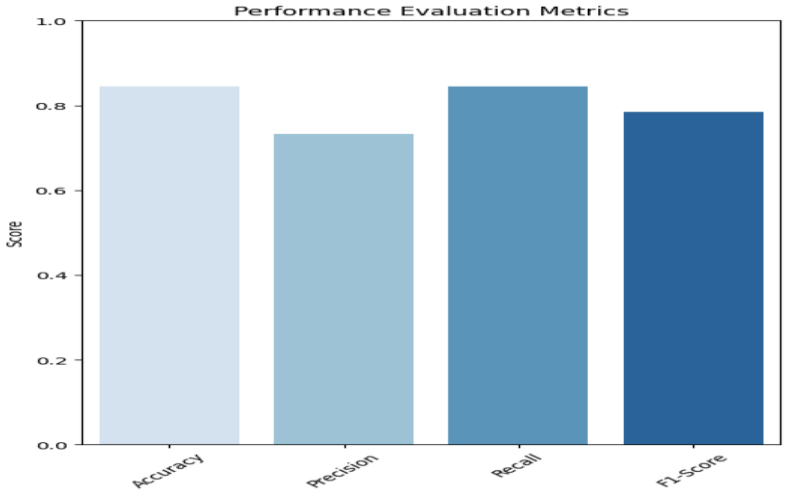

Fig. 4. AdaBoost Performance Evaluation

Table 1 shows the performance of various machine learning classifiers for threat prediction and classification for IoT-enabled 5G Networks. The ANN classifier has moderate performance with an accuracy of 68%. Precision is slightly higher at 70%, indicating that when it predicts a threat, it is correct 70% of the time. The recall is 64%, showing it detects 64% of actual threats. The F1-score of 0.68 balances precision and recall, suggesting a moderate capability in threat prediction and classification. The Decision Tree classifier also performs well with an accuracy of 99%. Its precision, F1-score, and recall are all 99%, indicating it is nearly perfect in identifying and classifying threats.

The AdaBoost classifier shows good performance with an accuracy of 84%. Its precision is 73%, which is lower compared to its recall of 78%. The F1-score of 0.84 indicates a well-balanced performance but suggests that while it is good at detecting threats, it may have a higher rate of false positives compared to its recall capability. DT classifiers outperformed ANN and AdaBoost in detecting and classifying threats in IoT-enabled 5G networks, as depicted in Fig. 5. This is because DT has low computational ability and can handle non-linearity in the data as compared to AdaBoost and ANN (Imianvan & Robinson, 2024).

https://doi.org/10.24191/mij.v7i1.11579

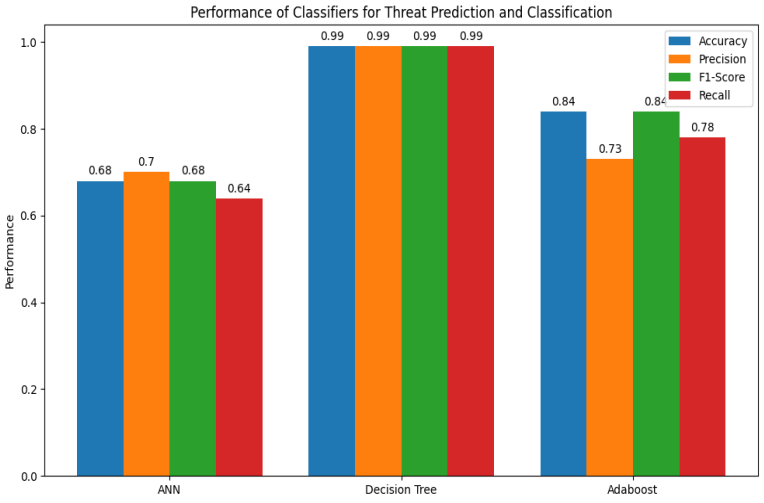

Fig. 5. Performance Evaluation of ANN, DT, and AdaBoost

5. CONCLUSION

In this paper, a machine learning-driven threat prediction and classification for IoT-enabled 5G networks is proposed based on the combination of three different classifiers, such as DT, artificial intelligence, and AdaBoost classifiers. The evaluation using IDS was collected from the NSL-KDD repository. The NSL-KDD dataset contains a total of 148517 data points which have been split into 125,973 training datasets and 22,544 testing datasets. The DT yielded 99% of ID in detecting threats and classifying normal traffic from attack links. Results further show that AdaBoost produced 84% accuracy in the task of intrusion detection, while ANN generated 68% accuracy. The performance of DT outperformed AdaBoost and artificial neural networks in predicting and classifying intrusions in IoT networks. Hence, the method is suitable for the detection and classification of various forms of threats in 5G wireless networks for the IoT connectivity ecosystem. This makes it stand out among the various other methods used for threat detection and classification.

The inability to perform such rigorous evaluation is one of the reasons for the limited deployment of ML-based NSL-KDD in a practical network environment. The contributions of this paper is to bridge the gap between academic research on ML-based NSL-KDD and their practical application. However, in further studies, we aim to consider optimizing ML approaches for robust threat detection with blockchain to develop a new intrusion detection system for the 5G IoT environment (Imianvan & Robinson, 2024). These results indicate that DT potentially provides highly accurate threat predictions and classifications. The work is contributing to the utilization of machine learning tools for the detection of threats in IoT devices. This will guide the network administrator to utilize an efficient and cost-effective approach in monitoring threats. However, deploying the framework in real-time network environments using edge or fog computing platforms is recommended to determine its efficiency in real-world scenario studies.

6. ACKNOWLEDGEMENTS/FUNDING

The research is supported and funded by the Tertiary Education Trust Fund (TETFund), Nigeria.

https://doi.org/10.24191/mij.v7i1.11579

7. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

8. AUTHORS' CONTRIBUTIONS

Samuel Robinson: Conceptualization, research execution, manuscript preparation. Moses Ekpenyong: Research design, supervision. Charles Igodan: Theoretical framework, manuscript review. Anthony Imianvan: Manuscript review and approval.

REFERENCES

Alosaimi, S., & Almutairi, S. M. (2023). An intrusion detection system using BoT-IoT. *Applied Sciences, 13*(9), Article 5427. https://doi.org/10.3390/app13095427

Baniasadi, S., Rostami, O., Martín, D., & Kaveh, M. (2022). A novel deep supervised learning-based approach for intrusion detection in IoT systems. *Sensors, 22*(12), Article 4459. https://doi.org/10.3390/s22124459

Ekpenyong, M. E., Asuquo, D. E., Udo, I. J., Robinson, S. A., & Ijebu, F. F. (2022). IPv6 routing protocol enhancements over low-power and lossy networks for IoT applications: A systematic review. *New Review of Information Networking, 27*(1), 30–68. https://doi.org/10.1080/13614576.2022.2078396

ElKashlan, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). *Electronics, 12*(4), Article 1044. https://doi.org/10.3390/electronics12041044

Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2020). RDTIDS: Rules and decision tree-based intrusion detection system for Internet-of-Things networks. *Future Internet, 12*(3), Article 44. https://doi.org/10.3390/fi12030044

Guerra-Manzanares, A., Medina-Galindo, J., Bahsi, H., & Nõmm, S. (2020). MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network. In S. Furnell, P. Mori, E. Weippl, & O. Camp (Eds.), *Proceedings of the 6th International Conference on Information Systems Security and Privacy* (pp. 207–218). SciTePress. https://doi.org/10.5220/0009187802070218

Huang, L., Deng, Y., & Wang, B. (2016). Flow simulation of suspension bridge cable based on lattice-Boltzmann method. *Mathematical Problems in Engineering, 2016*, Article 2537581. https://doi.org/10.1155/2016/2537581

Imianvan, A. A., & Robinson, S. A. (2024). Enhancing 5G Internet of Things (IoT) connectivity through comprehensive path loss modelling: A systematic review. *LAUTECH Journal of Computing and Informatics, 4*(2), 31–48.

Inyang, U. G., Robinson, S. A., Ijebu, F. F., Udo, I. J., & Nwokoro, C. O. (2021). Optimality assessments of classifiers on single and multi-labelled obstetrics outcome classification problems. *International Journal of Advanced Computer Science and Applications, 12*(2). https://doi.org/10.14569/IJACSA.2021.0120260

https://doi.org/10.24191/mij.v7i1.11579

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing, 164*, 55–68. https://doi.org/10.1016/j.jpdc.2022.01.030

Li, J., Zhao, Z., Li, R., & Zhang, H. (2019). AI-based two-stage intrusion detection for software defined IoT networks. *IEEE Internet of Things Journal, 6*(2), 2093–2102. https://doi.org/10.1109/JIOT.2018.2883344

Liu, L., Li, C., & Zhao, Y. (2023). Machine learning based interference mitigation for intelligent air-to-ground Internet of Things. *Electronics, 12*(1), Article 248. https://doi.org/10.3390/electronics12010248

Mudgerikar, A., Sharma, P., & Bertino, E. (2019). E-Spion: A system-level intrusion detection system for IoT devices. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (pp. 493–500). Association for Computing Machinery. https://doi.org/10.1145/3321705.3329857

Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: A deep learning–based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies, 33*(3), Article e3803. https://doi.org/10.1002/ett.3803

Rajawat, A. S., Bedi, P., Goyal, S. B., Shukla, P. K., Jamal, S. S., Alharbi, A. R., & Aljaedi, A. (2021). Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation. *Mathematical Problems in Engineering, 2021*, Article 2330049. https://doi.org/10.1155/2021/2330049

RajeshKumar, G., Mangathayaru, N., & Narsimha, G. (2016). Intrusion detection: A text mining-based approach. *arXiv*. https://doi.org/10.48550/arXiv.1603.03837

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks, 11*(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Robinson, S. A., Imianvan, A. A., Igodan, E. C., Dan, E. A., Joseph, K. U., & Dickson, L. A. (2025). Machine learning approach for path loss prediction in urban drive 5G network environments. *International Journal of Microwave and Optical Technology, 20*(4).

Robinson, S., & Imianvan, A. (2024). Intelligent path loss prediction for IoT connectivity in 5G networks using hybrid machine learning techniques. In *2024 International Conference on Sustainable Engineering for Blue and Green Economy (SEB4SDG)* (pp. 1–8). IEEE. https://doi.org/10.1109/SEB4SDG60871.2024.10630409

Roopak, M. (2021). *Intrusion detection system for IoT networks for detection of DDoS attacks* [Doctoral dissertation, Newcastle University]. Newcastle University eTheses.

Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering, 99*, Article 107810. https://doi.org/10.1016/j.compeleceng.2022.107810

Sarhan, M., Layeghy, S., & Portmann, M. (2022). Towards a standard feature set for network intrusion detection system datasets. *Mobile Networks and Applications, 27*(1), 357–370. https://doi.org/10.1007/s11036-021-01843-0

Sengupta, N., & Sil, J. (2020). *Intrusion detection: A data mining approach*. Springer. https://doi.org/10.1007/978-981-15-2716-6

https://doi.org/10.24191/mij.v7i1.11579

Suganya, E., & Rajan, C. (2021). An AdaBoost-modified classifier using particle swarm optimization and stochastic diffusion search in wireless IoT networks. *Wireless Networks, 27*(4), 2287–2299. https://doi.org/10.1007/s11276-020-02504-y

Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information, 11*(5), Article 279. https://doi.org/10.3390/info11050279

Usha, M., & Kavitha, P. (2017). Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier. *Wireless Networks, 23*(8), 2431–2446. https://doi.org/10.1007/s11276-016-1300-5

Wójcicki, K., Biegańska, M., Paliwoda, B., & Górna, J. (2022). Internet of Things in industry: Research profiling, application, challenges and opportunities—A review. *Energies, 15*(5), Article 1806. https://doi.org/10.3390/en15051806

Zwayed, F. A., Anbar, M., Sanjalawe, Y., & Manickam, S. (2021). Intrusion detection systems in fog computing—A review. In *Advances in cybersecurity: Third International Conference, ACeS 2021* (pp. 481–504). Springer. https://doi.org/10.1007/978-981-16-8059-5_30

https://doi.org/10.24191/mij.v7i1.11579