SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

An Improved Anomaly-based Intrusion Detection System for IoT Applications using Machine Learning Methods

Shirin Muataz Mohammed Sideek[1], Nashwan Saleh Ali[1], Wijdan Younus Abed[1], and Mustafa Sabah Taha[2]*

[1]General Directorate of Education in Ninawa, Ministry of Education, 41006 Ninawa, Iraq
[2]Missan Oil Training Institute, Ministry of Oil, 62001 Missan, Iraq

ABSTRACT

The emergence of the Internet of Things (IoT) aimed to enhance people's way of life by providing a range of smart, networked applications across multiple industries. Due to security vulnerabilities, devices operating in an IoT context encounter several problems. Although several strategies have been proposed to enhance the security and privacy of IoT devices, further work is still required. Machine learning (ML) has become a permanent fixture as a method for efficiently identifying anomalies in IoT networks. Hence, this study focusses on the challenges posed by heterogeneous IoT systems. It proposes a novel hybrid multi-algorithm system that uniquely combines four complementary ML algorithms to enhance anomaly detection in IoT. Unlike existing approaches that rely on single datasets or computationally intensive deep learning (DL), this study introduces a lightweight, yet highly effective framework that combines k-nearest neighbour (KNN), decision tree (DT), random forest (RF), and stacking classifier (SC) algorithms trained on an integrated multi-source dataset to address real-world IoT heterogeneity. The training and testing of the proposed system were conducted using the comprehensive NetFlow-University of Queensland-Network Intrusion Detection System (NF-UQ-NIDS) dataset, which uniquely combines four benchmark datasets: UNSW-NB15, BoT-IoT, ToN-IoT, and CSE-CIC-IDS2018, enabling superior generalisation across diverse IoT environments. The system achieved 99.9% and 96% accuracy rates in binary and multi-class classifications, outperforming state-of-the-art approaches while maintaining computational efficiency suitable for resource-constrained IoT devices.

Keywords: Binary classifications, information security, Internet of Things, intrusion detection system, machine learning, multi-classifications

ARTICLE INFO

Article history:
Received: 02 March 2025
Accepted: 11 June 2025
Published: 25 February 2026

DOI: https://doi.org/10.47836/pjst.34.1.18

E-mail addresses:
shirinmuataz@gmail.com (Shirin Muataz Mohammed Sideek)
nashwansaleh55@gmail.com (Nashwan Saleh Ali)
wjdanywns2@gmail.com (Wijdan Younus Abed)
timimymustafa@gmail.com (Mustafa Sabah Taha)
* Corresponding author

e-ISSN: 2231-8526

INTRODUCTION

The IoT is gaining popularity in many information and communication technology (ICT) systems, including wearable devices, automated transportation systems (Oladimeji et al., 2023; Yaseen et al., 2021), military and intelligence (Sulyman & Henggeler, 2022), smart city applications (Altamimi et al., 2020), and smart power systems (Al-Turjman et al., 2022), as a result of the introduction of new service paradigms in numerous sectors by technological innovation. IoT operates by utilising devices equipped with sensors, which enable the seamless transmission of data from these devices to the cloud for further analysis.

The analysed dataset is then used to generate control decisions that are relevant to cyber-physical systems (Koohang et al., 2022). The latest data suggests that there are approximately 26 billion linked and functional IoT gadgets globally (Koohang et al., 2022). In a study given by Cvitić et al. (2021), it was claimed that many more devices will be connected to IoT by 2025, with the number expected to be up to 75 billion. Numerous businesses rely on different IoT systems to increase efficiency and safety. IoT-based solutions can be used by manufacturers to analyse huge volumes of data gathered by the sensors built into their machinery.

This enables the efficient prevention and prediction of urgent situations, such as engine failures and other mishaps. Manufacturers can also rely on these decisions to greatly enhance productivity and safety (Khanna & Kaur, 2020; Quy et al., 2022).

The IoT can be categorised into four abstraction layers: the first layer is the physical layer, which involves collecting data through IoT sensors; the second layer is the network layer that facilitates the transfer of data between devices for processing (this layer can utilise cloud or edge communications); the third layer is the processing layer that uses cloud computing to implement numerous computational tasks; the application layer, the last layer, comes from the end users' devices (Kaur et al., 2022).

These four layers are vulnerable to security risks (Ahanger et al., 2022). Hence, much effort has recently been pushed towards improving the security of IoT devices (Rajaan et al., 2025). Devices that are connected to the IoT generate, collect, and process data, which frequently includes sensitive data.

These devices are therefore extremely susceptible to serious security risks that attackers may use against them. Therefore, it is essential to protect the accuracy of the data that IoT devices acquire in real-time, and achieving this feat requires building efficient anomaly detection models that could detect these threats in real-time and make excellent decisions automatically (Yang & Zhang, 2023).

ML employs both malicious and anomalous IoT data to train detection models, thereby playing an important role in the detection of anomalous and malicious network traffic. Numerous ML algorithms are used in the literature to identify malicious data (Alghanmi et al., 2022; Xu et al., 2023). These methods, however, are predicated on the essential premise that the training data is homogeneous, meaning it is taken from similar sources and belongs to the same data types, such as pixels. In simpler terms, these systems are not explicitly created to handle the diverse types of data commonly used in practical IoT systems. Hence, it became essential to come up with a system that can effectively detect anomalies obtained from dynamic and heterogeneous environments; this can be achieved by integrating multiple ML algorithms.

While various ML approaches have been proposed for IoT intrusion detection, existing solutions face three critical limitations: (i) most studies focuss on single-algorithm approaches or simple ensemble methods that cannot effectively capture the diverse attack patterns in heterogeneous IoT environments; (ii) evaluation is typically conducted on single, homogeneous datasets that fail to represent real-world IoT network diversity; and (iii) the trend toward complex ML models creates computational overhead unsuitable for resource-constrained IoT devices. Therefore, this paper addresses these gaps through three novel contributions:

This study's contributions are grounded in a thorough review of recent literature, which revealed specific limitations in existing intrusion detection system (IDS) solutions for IoT. The identified research gap served as the foundation upon which the proposed framework was conceptualised and developed.

1. Novel hybrid multi-algorithm architecture - A unique four-algorithm hybrid framework was introduced, where DT, KNN, and RF serve as complementary base learners, with SC acting as an intelligent meta-learner. This specific combination is novel because: (i) it leverages the linear decision boundaries of DT, distance-based classification of KNN, and ensemble strength of RF; (ii) SC optimally combines their predictions rather than simple voting; and (iii) the four-algorithm synergy specifically addresses IoT attack pattern diversity.

2. Comprehensive multi-dataset integration approach - Unlike previous studies using single datasets, this study employed the NF-UQ-NIDS dataset comprising four different benchmark datasets (NF-BoT-IoT, NF-UNSW-NB15, NF-ToN-IoT, NF-CSE-CICIDS-2018). This approach is novel because it: (i) trains models on heterogeneous data sources representing diverse IoT environments; (ii) ensures robustness across different attack vectors and network configurations; and (iii) provides the first comprehensive evaluation framework for IoT intrusion detection.

3. Computational efficiency innovation – This study demonstrates that superior performance (99.9% binary, 96% multi-class accuracy) can be achieved using lightweight ML algorithms instead of computationally intensive DL approaches. This contribution is significant because: (i) it challenges the complexity paradigm in IoT security; (ii) it enables deployment on resource-constrained IoT devices; and (iii) it provides practical solutions for real-world IoT implementations.

This study aims to achieve the following objectives: (1) to design a lightweight hybrid intrusion detection model tailored for heterogeneous IoT environments; (2) to evaluate the model's performance using an integrated multi-dataset approach; and (3) to ensure computational efficiency suitable for resource-constrained IoT devices.

Based on these objectives, the study addresses the following research questions:

1. How effective is a hybrid ML architecture (DT, KNN, RF, SC) in detecting anomalies across diverse IoT attack patterns?
2. Can integrating multiple benchmark datasets improve the generalisation and robustness of IDS models?
3. To what extent can lightweight ML models achieve high detection accuracy compared to DL methods in IoT environments?

Guided by these questions, the study tests the following hypotheses:

H1 : The proposed hybrid ML model will outperform single-algorithm models in anomaly detection accuracy across heterogeneous IoT datasets.

H2 : Lightweight ML models can achieve comparable or superior accuracy to DL models while maintaining lower computational complexity.

To position this study within the broader context of existing research, it is necessary to critically examine the recent developments in IoT-based intrusion detection systems. The following section presents a detailed literature review, highlighting the strengths and limitations of current ML- and DL-based approaches, the datasets commonly used, and the unresolved challenges that motivate the present research.

LITERATURE REVIEW

To establish a comprehensive understanding of the current state of IDS in IoT environments, a structured literature review was conducted using a combination of academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. The search was guided by key terms including IoT intrusion detection, ML for IDS, DL IoT security, anomaly detection in IoT, hybrid ML IDS, and lightweight IDS models. The selection criteria focussed on peer-reviewed journal articles and conference proceedings published between 2020 and 2024 to ensure the relevance and currency of findings. A total of 22 studies were selected, comprising both ML-based and DL-based approaches. These studies were critically examined to identify technical limitations, algorithmic trends, dataset usage, and evaluation strategies to extract the existing research gap that this paper aims to address.

This section covers the review of studies in the field of IDS in IoT. First, a DL-based model that achieved 99% network anomaly detection accuracy has been developed by Vibhute et al. (2024). The work focussed mainly on the real-time detection of network anomalies using a CNN model trained on the modern UNSW-NB15 dataset. They proposed a two-step method for detecting network problems, involving using traditional ML (RF) to select important features, while DL (CNN) is used to classify the selected features into two groups. The proposed method was employed to enhance the accuracy and effectiveness of detecting unusual network traffic using the UNSW-NB15 dataset.

Ferrag et al. (2020) used the DT ML model to compare the binary classification efficiency of different models based on the commonly used Canadian Institute of Cybersecurity-Intrusion Detection System (CIC-IDS) and BoT-IoT datasets. The model recorded an anomaly detection accuracy of 96% but the study failed to consider the model's false alarm rate. In another study, Jiang et al. (2020) The researchers discussed the process of selecting suitable ML algorithms, utilising the CICIDS-2017 dataset, and employing seven distinct ML algorithms. However, the major focuss of the study was anomaly detection using different ML algorithms rather than comparing their accuracy and effectiveness in network intrusion detection.

Kunhare et al. (2020) suggested the use of a swarm optimisation technique during the selection of important features for the ML algorithm to ensure the reduction of computational complexity. The models’ testing phase achieved 99% accuracy for binary classification using the RF classifier. However, ML algorithms often exhibit high rates of false alarms, which is a major bottleneck to the use of ML algorithms for real-time anomaly detection.

Many scholars have also proposed numerous DL methods for IDS. For instance, DL-based IDS was proposed by Awajan (2023) based on a probability distribution-based attack classification method and a four-layer deep, fully connected architecture. The suggested method's average anomaly detection accuracy rate was 93.21%. Nonetheless, the study recognised that a significant restriction is still the requirement for a lightweight version of the model to guarantee effective and quick intrusion detection. A DL model for anomaly-based intrusion detection in IoT networks was presented by Saba et al. (2022). The model was trained and validated on the National Infrastructure Database (NID) dataset with 25,192 records. Using 20% of the training dataset, the model showed a remarkable overall accuracy of 99.51% throughout the validation process. The performance evaluation was conducted using a confusion matrix on the BoT-IoT dataset, achieving 95.55% accuracy across various network attack categories. Hence, the model was considered suitable for IoT networks.

A study presented by Awajan (2023), authors have been developed by the authors as a communication protocol independent framework in order to minimise deployment complexities. Its performance has been rigorously evaluated through experimental analysis under both simulated and real-world intrusion scenarios, where reliable results have been demonstrated. The system has been shown to effectively detect Blackhole, Distributed Denial of Service (DDoS), and Opportunistic Service, Sinkhole, and Wormhole attacks, achieving an average detection accuracy of 93.74%. Furthermore, the intrusion detection system (IDS) has been reported to obtain mean precision, recall, and F1-scores of 93.71%, 93.82%, and 93.47%, respectively. By employing deep learning methodologies, an average detection rate of 93.21% has been maintained, which has been considered satisfactory for enhancing the overall security of Internet of Things (IoT) networks.

Altulaihan, Almaiah, and Aljughaiman (2024) proposed an intrusion detection system (IDS) defence mechanism designed to enhance the security of IoT networks against Denial-of-Service (DoS) attacks through the integration of anomaly detection and machine learning (ML) techniques. The IDS employs anomaly detection to continuously monitor network traffic and identify deviations from established normal profiles. To achieve this, four supervised classification algorithms were applied: Decision Tree (DT), Random Forest (RF), K-Nearest Neighbour (kNN), and Support Vector Machine (SVM). In parallel, two feature selection methods—Correlation-based Feature Selection (CFS) and Genetic Algorithm (GA)—were utilised and their performances comparatively analysed. The IoTID20 dataset, one of the most recent benchmark datasets for detecting anomalous activities in IoT environments, served as the training and testing foundation for the models. The findings indicated that DT and RF classifiers, particularly when combined with GA-based feature selection, yielded the most effective detection performance. Furthermore, evaluations of additional metrics, including training and testing times, revealed that DT achieved superior efficiency.

Sharma et al. (2023) created a generative adversarial network (GAN)-based deep neural network (DNN) model that was trained on the UNSW-NB15 dataset. The generation of synthetic data that imitates minor attacks was done using the GAN model. This method sought to resolve the class problem in the dataset's cross-validation. The model's evaluation revealed an astounding 91% attack detection accuracy rate. Additionally, Saheed et al. (2023) presented a novel method for identifying intrusion attacks in IoT networks, which relies on a Gray Wolf Optimiser (GWO)-based ensemble learning strategy. The study also suggested a classification phase engine and a traffic analyser as two core components of the voting GWO ensemble model. The suggested model combines the probability averages of the basic learners using a voting approach. Secondly, it was suggested that dimensionality be decreased by combining feature extraction and feature selection algorithms. Thirdly, the ensemble models' parameters were optimised using GWO. The method combined several learners to create an ensemble of learners and utilised the most accurate intrusion detection datasets available. Feature dimensionality was reduced by combining principal component analysis (PCA) and information gain (IG). For classification, a new GWO ensemble learning technique that combined a multilayer perceptron, KNN, RF, and DT was also used. Using the BoT-IoT dataset, the performance metrics of the model were 99.98% for accuracy, 99.97% for DR, 99.94% for precision, 99.99% for rate of change (ROC), and 1.30 % for false acceptance rate (FAR). The model also recorded the following metrics on the UNSW-NB15 dataset: 100% for accuracy, 99.9% for DR, 99.59% for precision, 99.40% for ROC, and 1.50 % for FAR.

The global market for IoT devices is growing steadily, and by the end of 2025, there will be an estimated 50 billion linked devices. According to Saheed et al. (2023), with the increasing number of connected devices come serious security issues for these connected devices. These issues are yet to be addressed properly, as they cannot be properly handled using the existing traditional network security mechanisms. Hence, scholars have proposed and developed several network IDS that could handle these network attacks effectively. Intrusion detection systems are built with a feature selection stage that is considered the most important stage.

Although this feature selection step is quite labour-intensive and time-consuming, numerous ML techniques have been developed to enhance it, thereby improving IDS performance. However, the detection rates and accuracy of these methods are subpar. For feature selection, this research suggests a novel hybrid autoencoder and modified particle swarm optimisation (HAEMPSO), while for classification tasks in IDS, it suggests a DNN. The UNSW-NB15 and BoT-IoT datasets, which are suitable for the IoT environment, are utilised in an experimental study after the DNN parameters are optimised using the PSO with a modified inertia weight.

Upon a critical synthesis of the reviewed literature, it is evident that despite substantial progress in IoT-based intrusion detection, existing models suffer from significant limitations, including over-reliance on homogeneous datasets, a lack of robust multi-algorithmic frameworks, and excessive computational complexity that is unsuitable for low-resource IoT devices. These gaps underscore the absence of a lightweight, hybrid, and scalable intrusion detection solution capable of handling the heterogeneous and dynamic nature of real-world IoT environments. This research addresses this critical void by proposing a novel hybrid architecture, multi-dataset integration strategy, and a computationally efficient detection approach that directly stems from the empirical deficiencies identified in literature. Thus, the research contribution is not theoretical speculation but a direct response to concrete limitations observed across recent academic and practical studies.

METHODOLOGY

The implementation of the proposed system consisted of multiple phases; first, the four datasets (NF-BoTIoT, NF-UNSWNB15, NF-ToNIoT, and NF-CSE CICIDS2018) were in .csv file format and followed the same steps. Second, exploratory data analysis (EDA) was conducted to better understand the dataset. Third, the data was pre-processed to identify important features. Then, feature selection was conducted, followed by binary classification and multiclass classification. The last phase was the performance evaluation using various metrics and a comparison of the results. An overview of these phases is illustrated in Figure 1.

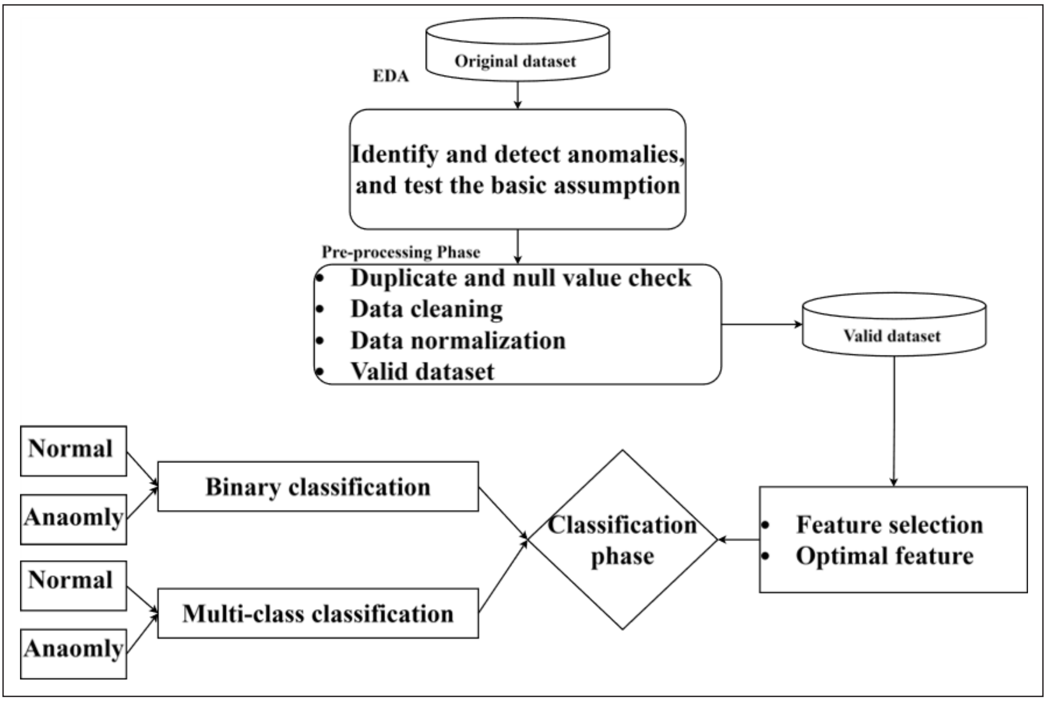

Figure 1. An overview of the phases followed in this work
Note. EDA = Exploratory data analysis

Dataset

The limited capability of network-based intrusion detection system (NIDS) has made its real-world usage in IoT networks troublesome. To address the limitation of the existing IDS, Sarhan et al. (2021) offered a solution by proposing five NIDS datasets based on NetFlow. These datasets have a usable and consistent feature set, unlike those that only target specific types of attacks. The database was created using benchmark NIDS datasets such as NF-BoT-IoT, NF-UNSWNB15, NF-ToN-IoT, and NF-CSE CICIDS2018. The original packet captured files from these datasets were converted into the NetFlow format. NetFlow is a widely used format in practical scenarios and is extensively deployed in production networks due to its excellent scaling properties (Awad et al., 2022).

Table 1
Description of the dataset

Dataset	Total data	Training dataset	Testing dataset
NF-BoT-IoT	600,100	480,080	120,020
NF-ToN-IoT	1,379,274	1,103,419	275,855
NF-CSE-CIC-IDS2018	8,392,401	6,713,920	1,678,481
NF-UNSW-NB15	1,623,118	1,298,494	324,624
NF-UQ-NIDS	11,994,893	9,595,914	2,398,979

Note. NF-BoT-IoT = Net Flow- Botnet - Internet of Things, NF-ToN-IoT = Net Flow- Telemetry of Networks in the Internet of Things, NF-CSE-CIC-IDS2018 = Network Flow - Communications Security Establishment - Canadian Institute for Cyber security - Intrusion Detection System 2018, NF-UNSW-NB15 = Net Flow - University of New South Wales - New Benchmark 2015, NF-UQ-NIDS = Network Flow - University of Queensland - Network Intrusion Detection System

The list of utilised datasets in this work is shown in Table 1. The recently released dataset showcases the benefits of using shared dataset feature sets. Over time, the size and diversity of NIDS datasets are expected to increase. These datasets will include flows from different attacks and network configurations.

EDA

This analysis involves using graphical methods and descriptive statistics to understand the intricacies buried within datasets (Da Poian et al., 2023). Its main aims are to uncover the most profound understanding of the dataset, to recognise any disassociated or outlier elements, and to validate foundational assumptions. Additionally, it acts as a strong preliminary stage before other statistical approaches are executed. Also, in the context of unsupervised learning, Baseline models must be built to understand data deeply before moving on to the next phases, such as predictive or supervised learning. EDA is the process of describing and classifying repetitive phenomena, determining essential correlation structures for predictions, and evaluating the relevance of factors that account for the most considerable changes in lower-dimensional representation space. Besides, EDA has great importance for anomaly detection, including outliers, which are attributed to poor-quality data. One of the EDA techniques is calculating the percentage share of the four datasets within the NF-UQ-NIDS dataset. Figure 2 illustrates the percentage distribution for each dataset within the NF-UQ-NIDS dataset. The Network Flow - Communications Security Establishment - Canadian Institute for Cyber security - Intrusion Detection System 2018 (NF-SCE-CIC-IDS2018) dataset makes up 64.64% of the total dataset. The NF-UNSW-NB15 dataset represents 16.21% of the dataset, whereas the NF-ToN-IoT dataset contributes 12.65%, and the NF-BoT-IoT dataset comprises 6.50%.

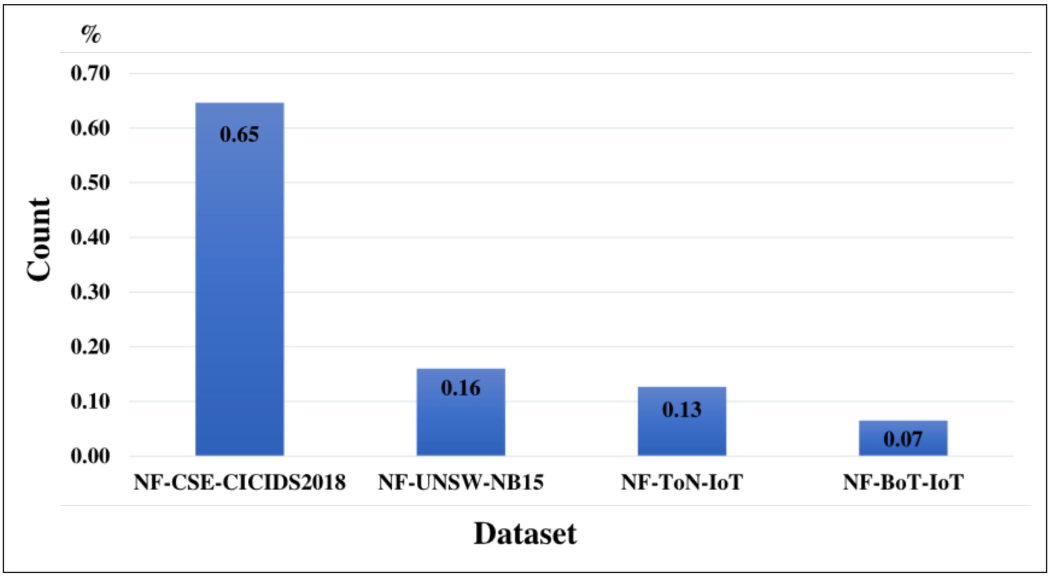

Figure 2. NetFlow-University of Queensland-Network Intrusion Detection System (NF-UQ-NIDS) dataset and the percentage of its component datasets

Note. NF-BoT-IoT = Net Flow- Botnet - Internet of Things; NF-ToN-IoT = Net Flow- Telemetry of Networks in the Internet of Things; NF-CSE-CIC-IDS2018 = Network Flow - Communications Security Establishment - Canadian Institute for Cyber security - Intrusion Detection System 2018; NF-UNSW-NB15 = Net Flow - University of New South Wales - New Benchmark 2015; NF-UQ-NIDS = Network Flow - University of Queensland - Network Intrusion Detection System

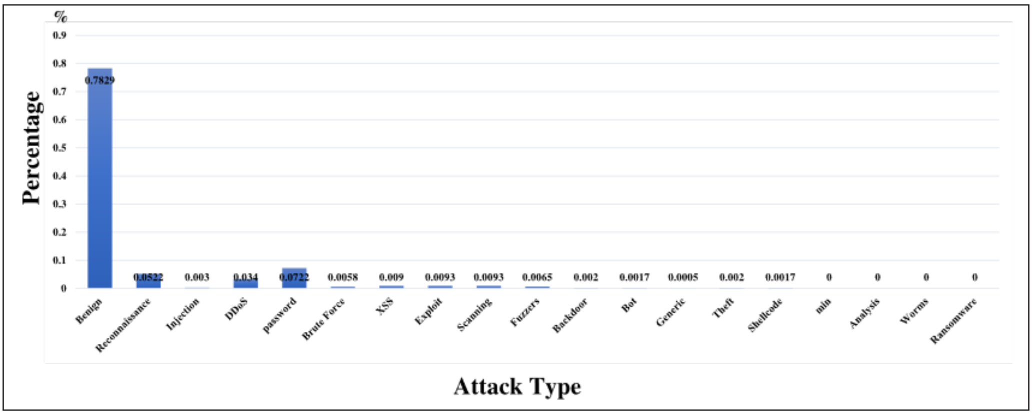

Figure 3. Percentage of each attack type in the dataset

Note. DDoS = Distributed Denial of Service; XSS = cross-site scripting

Figure 3 introduces another possibility of EDA by showing how often attacks were recorded in the dataset. This visualisation accurately and clearly illustrates the distribution of each attack type. By studying this figure, one can understand the most common and the least common attack types in the dataset. This information is crucial in categorising different types of attacks based on their nature and frequency in the dataset. Benign attacks are the most common type of attack, constituting 78.29% of the total attacks. Following these are reconnaissance assaults and injection attacks, which constitute 5.22 and 5.03%, respectively. On the other hand, there are less common forms of attacks, like distributed denial-of-service (DDoS), DoS, password attacks, and cross-site scripting (XSS).

Data-preprocessing

In this work, dataset preparation has been carried out in parallel with the data analysis workflow to ensure the reliability and accuracy of the data. The duplicate and null value check method (Walling & Lodh, 2024) was applied using the panda's library tools to check for repeated or null entries within the data. The strategy used for replacing or handling null values depends on the specific context; for instance, if there are repeated entries, these can be fully discarded or their values can be set to a constant, such as the mean or median. Data cleaning procedures (Gaber et al., 2022), such as removing rows that are repeated and setting some blank values, are bespoke approaches that can help mitigate this issue.

Initially, the dataset was validated to look for missing values and duplicate entries. Importantly, the selected dataset had no missing values and no duplicates. This confirms that the dataset is complete and contains no redundant information. After this, the dataset undergoes normalisation processes. Normalisation (Aljebreen et al., 2023) is the process of standardising data to a standard range (Equation 1). This facilitates further comparison and analysis of the data. Completion of these pre-processing steps ensures that the dataset is accurate, reliable, and ready for any further analysis or advanced modelling work.

$$x\ normalized = \frac{x - x\ minimum}{x\ maximum - x\ minimum} \qquad [1]$$

where the minimum value maps to 0, while the maximum value maps to 1, respectively.

The dimensions of the data in this study were compared before and after selecting the top 6 attacks (these top 6 attacks are regarded as the most common or important attacks in the dataset). This selection focusses on attacks that are both prevalent and pose a critical threat to the security of internet-connected devices. Ensuring optimal system performance requires analysing the data and applying the system while considering these six attacks. Dimension comparison measures the data across several predefined scopes to assess their sizes. Here, the specific focuss of the analysis was on how the matrices X and Y shifted in relation to each other and what residual changes occurred spatially after separating the six key attacks. This technique helps understand how identifying these attacks impacts the size of the data and whether there are meaningful changes in dimensions afterward.

Table 2 illustrates the dimension comparison results before and after the selection of the top 6 attacks.

Table 2
Dimension comparison before and after selecting the top 6 attacks

Data	Before	After
X shape	(9156325, 10)	(8806358, 10)
Y shape	(9156325)	(8806358)

The Employed ML Algorithms

The envisioned system in this study aims to enhance the cybersecurity of IoT appliances by detecting intrusion and anomaly traffic. Moreover, it attempts to resolve issues related to the protection of such devices. The application of some ML algorithms, such as DT, KNN, SC, and RF algorithms, to intrusion detection is covered in this paper.

As a member of the family of supervised learning algorithms, the DT algorithm is a unique kind of supervised learning framework since it can be used for both classification and regression tasks (Lin et al., 2022). The DT algorithm was employed in this study due to its capacity to create training systems that can precisely predict the class or value of the target variables. This is achieved by acquiring knowledge from previous data (training data) and inferring straightforward decision rules. The DT algorithm functions by recursively dividing the data into progressively smaller subsets until each subset becomes homogeneous. The DT is constructed by identifying the optimal split at each node. This optimal split is determined by minimising the impurity of the resulting subsets.

Another non-parametric ML technique that is frequently applied to both regression and classification problems is the KNN algorithm (Uddin et al., 2022). Before predicting the new instance's label based on the labels of its k nearest neighbours, it first determines which k instances in the training set are the most like the new instance. Furthermore, it categorises the new data points by comparing their resemblance to the previously recorded data points. Since the data behaviour is dynamic, the Euclidean distance is frequently used in this article to find the nearest neighbour**.** Equation 2 illustrates the calculation of the Euclidean distance (d).

$$d = sqrt[(x_2 - x_1)^2 + (y_2 - y_1] \qquad [2]$$

where d is the distance between (x_1, y_1) and (x_2, y_2), sqrt refers to the square root, (x_1-y_1) are the coordinates of one point, and (x_2-y_2) are the coordinates of the other point, respectively.

The SC refers to a stacking technique that utilises classification systems (Khan & Byun, 2022). The main concept of an SC, as discussed in this paper, involves utilising a combination of diverse classifiers to enhance the accuracy of the ultimate predictions. Typically, the base classifiers are trained on different subsets of the data or with different hyperparameter settings. The SC algorithm was utilised in this study for three reasons: firstly, improving the predictive power of the proposed system is beneficial; additionally, stacking can help mitigate the issue of overfitting. To avoid overfitting the proposed system to the training dataset, each classifier can be trained on a distinct subset of the data. Additionally, stacking can be employed as a technique to enhance the interpretability of the proposed system.

Sheykhmousa et al. (2020) have discussed the RF algorithm as one of the supervised learning ML algorithms. Classification and regression trees (CART) tasks can be performed using ML techniques. The RF classifier consists of several DTs, each trained on distinct portions of a dataset. The classifier aggregates the average values obtained through each DT's predictions to boost its accuracy concerning the dataset.

Table 3
The all-in-one computer specification was utilised in this study

Hardware	Specification
Operating system	Windows 10 Pro.
Central processing unit	10th Intel i7-10700
Random access memory	32 GB
Hard desk	1 TB SSD
Wireless	Wi-Fi 6; Bluetooth 5
Ethernet	RJ45
Software libraries	Python, Scikit Learn, Numpy, and TensorFlow

Note. SSD = Solid-state drive

Experimental Environment and the Evaluation Metrics

In this study, the experiments were performed with an all–in–one computer that has the following specifications Table 3.

Several metrics, including accuracy, precision, recall, and F1, have been widely used in the literature to measure the performance of binary and multi-classifier anomaly detection models in IoT (Kaur et al., 2022; Awajan, 2023). Equations 3-6 represent some of the performance evaluation metrics used in IoT studies.

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \quad [3]$$

$$Precision = \frac{TP}{TP + FP} \quad [4]$$

$$Recall = \frac{TP}{TP + FN} \quad [5]$$

$$F - Measure = 2\, Precision \cdot Recall\, Precision + Recall \quad [6]$$

where TN = true negatives, TP = true positives, FN = false negatives, FP = false positives, and F = false positives, respectively.

RESULTS AND DISCUSSION

This study strives towards improving the security features of IoT devices through an ML-based IDS that hybridises DT, KNN, SC, and RF algorithms. The suggested system was trained and validated on the NIDS dataset (consisting of UNSW-NB15, BoT-IoT, ToN-IoT, and CSE-CIC-IDS2018 datasets) using 10-fold cross-validation. The dataset was portioned into 80% for the training phase and 20% for the testing phase. In ML, classification is a supervised learning technique in which a computer programme learns from existing data and creates new observations or categories. The classification process in this study involves dividing a given NIDS dataset into separate and distinct classes. It can be applied to both organised and unstructured data. Two types of classification tasks have been used in this study, which are binary classifications (Rizvi et al., 2023) and multi-classification models (Du et al., 2023).

i. Binary classification: It involves two distinct class labels; in most cases, one class represents the standard or typical condition, while the other class represents the abnormal or aberrant condition. Within the context of this paper, binary classification refers specifically to the task of distinguishing between two scenarios: an attack and a non-attack situation.

ii. Multi-classification: It involves more than two class labels multi-class classification, unlike binary classification, classifies instances into several pre-defined classes rather than differentiating between normal and abnormal results.

The accuracy of the KNN algorithm for binary classification in this study was 99.3%, just slightly below the accuracy of the RF algorithm (99.8% accuracy) and the DT algorithm (99.8% accuracy). With a score of 99.9%, the SC technique showed the highest degree of accuracy. The SC approach achieved the best accuracy of 96% in the multi-classification model, followed by the RF algorithm (95.6%) and the KNN algorithm (94%). At 93%, the DT algorithm's accuracy rate was the lowest among all the models. These results demonstrate the effectiveness of various ML algorithms in accurately identifying patterns and anomalies in IoT security. Figures 4 and 5 show the accuracy of metric-based binary and multi-classification models for the four ML algorithms employed in this work.

Examining the four evaluation criteria mentioned earlier in equations (3, 4, 5, and 6) will lead to the presentation of the individual results for each ML algorithm. These result tables include binary classification, classification based on a confusion matrix, and multiple classification models. For the multi-classification model, Table 4 presents the evaluation metrics of the KNN algorithm

Table 4
The results of the multi-classification model using the k-nearest neighbour algorithm

Metric type	Value
Precision	0.9386477533273871
Recall	0.9419731875598999
F1 Score	0.939868420746709

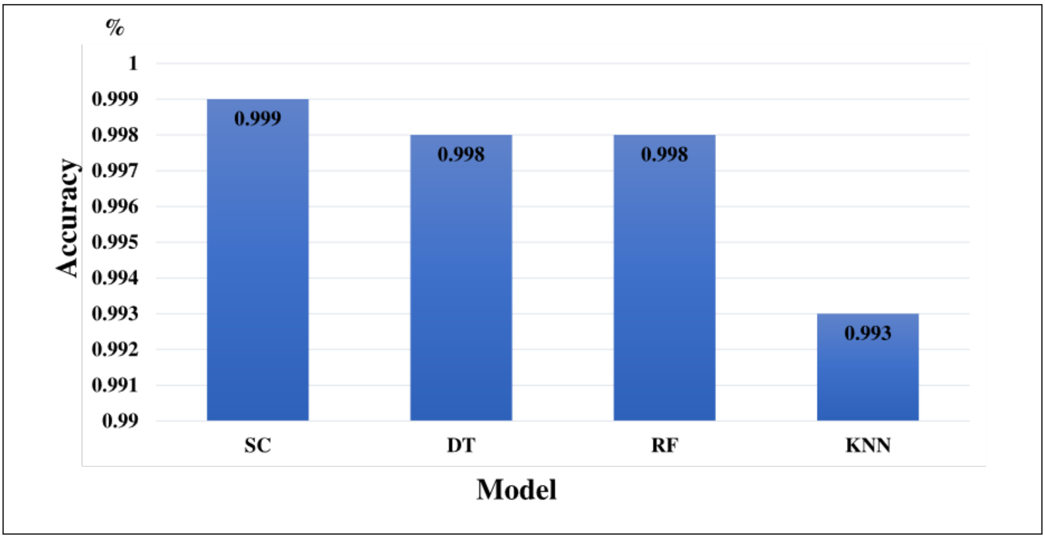

Figure 4. The accuracy metric-based binary classification model for ML algorithms
Note. ML = Machine learning; SC = Stacking classifier; DT = Decision ree; RF = Random forest; KNN = k-nearest neighbour

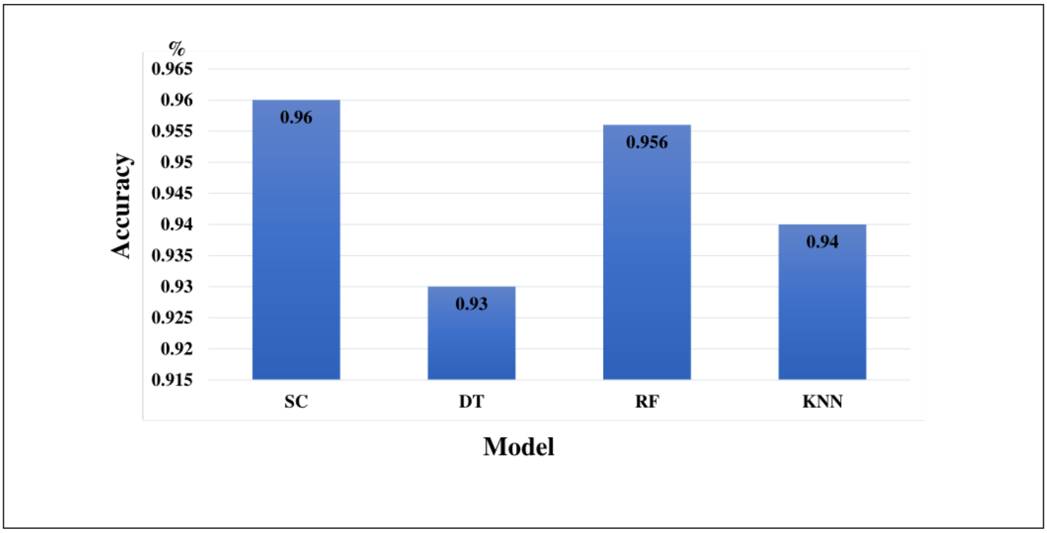

Figure 5. The accuracy metric-based multi-classification model for ML algorithms
Note. ML = Machine learning; SC = Stacking classifier; DT = Decision tree; RF = Random forest; KNN = K-nearest neighbour

while its prediction performance in the multi-class classification model is presented in Table 5 as a confusion matrix. Table 6 presents the assessment metrics of the KNN's for the binary classification model.

Table 5
The confusion matrix of predicting each class in the multi-classification model using the k-nearest neighbour algorithm

	Class 1	**Class 2**	**Class 3**	**Class 4**	**Class 5**	**Class 6**
Class 1	1428244	908	684	3032	689	37
Class 2	837	36311	9750	920	11279	1710
Class 3	868	11409	36509	989	262	2
Class 4	2864	4703	1548	86116	53	0
Class 5	827	10638	218	26	70218	10396
Class 6	88	6519	98	12	20835	1673

Table 6
The results of the binary classification model using the k-nearest neighbour algorithm

Metric type	**Value**
Precision	0.9816024785423058
Recall	0.9852721269050715
F1 Score	0.9834338794451865

Table 7
The results of the multi-classification model using the decision tree algorithm

Metric type	**Value**
Precision	0.9351291425814838
Recall	0.934990166198066
F1 Score	0.9347700943355706

Table 8
The confusion matrix of predicting each class in the multi-classification model using the decision tree

	Class 1	**Class 2**	**Class 3**	**Class 4**	**Class 5**	**Class 6**
Class 1	1432513	51	193	783	52	2
Class 2	15	32735	12107	978	12281	2691
Class 3	146	13423	35308	1065	75	22
Class 4	763	5241	1100	88180	0	0
Class 5	29	16727	134	0	57501	17932
Class 6	1	9303	18	0	19368	535

Table 9
The results of the binary classification model using the decision tree algorithm

Metric type	**Value**
Precision	0.996534334796682
Recall	0.99686582559708
F1 Score	0.9967000526343892

Table 10
The results of the multi-classification model using the stacking classifier algorithm

Metric type	**Value**
Precision	0.955886879731435
Recall	0.9579758265617122
F1 Score	0.9545949378591999

In the same way, Tables 7, 8, and 9 show the results of the DT algorithm for the multi-classifications, the confusion matrix, and the binary classification models using the four-evaluation metrics. Table 6 expresses the results of the evaluation metrics of the DT algorithm for the multi-classification model. A confusion matrix, presented in Table

7, illustrates how well the DT algorithm predicts each class in a multi-class classification model. Table 8 presents the evaluation metrics of DT for the binary classification model.

The ML-based SC algorithm behaved differently, as shown in Tables 10, 11, and 12 for multi-classifications, the confusion matrix, and binary-classification models using the four evaluation metrics. Table 10 expresses the results of the evaluation metrics of the SC algorithm for the multi-classification model. A confusion matrix, seen in Table 11, illustrates how well the SC algorithm predicts each class in a multi-class classification model. The SC algorithm's evaluation metrics for the binary classification model are shown in Table 12.

Tables 13, 14, and 15 demonstrate the performance of the ML-based RF system for multi-classification, confusion matrix, and binary classification models using the four-evaluation metrics. Table 13 presents the evaluation metrics of the RF algorithm for the multi-classification model. Table 14 displays a confusion matrix that evaluates the accuracy of the RF algorithm in the prediction of the different classes within a multi-class classification model. For the binary classification model, the evaluation metrics of the SC algorithm are shown in Table 15.

The performance of the proposed model in this work was benchmarked against several recent models to ensure improvement in model development. Tables 16 and 17 present a comparative study of the accuracy-based binary and multi-classification models, comparing the results of this model with the references (Bhavsar et al., 2023; Saba et al., 2022; Sharma et al., 2023).

Table 11
The confusion matrix of predicting each class in the multi-classification model using the stacking classifier algorithm

	Class 1	**Class 2**	**Class 3**	**Class 4**	**Class 5**	**Class 6**
Class 1	1432572	33	64	885	38	2
Class 2	24	38100	4603	3931	13239	910
Class 3	217	4737	40604	4140	340	1
Class 4	1113	2494	2909	88767	1	0
Class 5	36	6441	183	17	82394	3252
Class 6	2	2470	88	3	21843	4819

Table 12
The results of the binary classification model using the stacking classifier algorithm

Metric type	**Value**
Accuracy	0.9987026421813325
Precision	0.9967028236651778
Recall	0.9963226093909264
F1 Score	0.996512680260854

Table 13
The results of the multi-classification model using the random forest algorithm

Metric type	Value
Precision	0.9479355325129594
Recall	0.9560255315476542
F1 Score	0.9499312815098315

Table 14
The confusion matrix of predicting each class in the multi-classification model using the random forest algorithm

	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	1430309	230	254	2488	313	0
Class 2	1360	46807	19	93	12528	0
Class 3	1623	13461	34546	126	283	0
Class 4	4067	5692	71	85449	5	0
Class 5	764	4825	24	0	86710	0
Class 6	122	4820	9	0	24274	0

Table 15
The results of the binary classification model using the random forest algorithm

Metric type	Value
Precision	0.996534334796682
Recall	0.99686582559708
F1 Score	0.9967000526343892

Table 16
Comparative assessment of the proposed system's performance against recently developed algorithms on binary classification tasks

Reference	Accuracy (%)
The proposed system	99.90
Bhavsar et al. (2023)	99.00
Saba et al. (2022)	99.51
Sharma et al. (2023)	84.00

Table 17
A comparative study between the proposed system's result and the state-of-the-art using the metric accuracy-based multi-classification performance

Reference	Accuracy (%)
The proposed system	96.00
Bhavsar et al. (2023)	88.00
Saba et al. (2022)	95.55
Sharma et al. (2023)	83.90

The findings of this study directly addressed the proposed research questions and validated the stated hypotheses. All predefined objectives were successfully achieved, confirming that the proposed model effectively bridged the identified research gap.

The proposed hybrid ML framework contributes theoretically by extending ensemble strategies in heterogeneous IoT environments. Practically, it offers a deployable, low-complexity solution suitable for real-world IoT security challenges, enhancing system resilience without high computational costs.

RESEARCH CHALLENGES

While the proposed hybrid multi-algorithm intrusion detection system demonstrates superior performance, several challenges, and limitations must be acknowledged to provide a comprehensive evaluation framework and guide future research directions.

1. The NF-UQ-NIDS dataset exhibits significant class imbalance, as evidenced in Figure 3, where benign traffic constitutes 78.29% of the dataset while critical attack types

like DDoS, DoS, and password attacks represent much smaller proportions. This imbalance presents several challenges for real-world deployment.

2. In actual IoT deployments, the ratio of malicious to benign traffic may differ significantly from our training dataset, potentially affecting model generalisation. Attack patterns in production environments may be sparser or concentrated than represented in the benchmark datasets. While we selected the top 6 attack types to focuss on the most significant threats, reducing the dataset from 9,156,325 to 8,806,358 samples, this approach may inadvertently exclude emerging or less common attack vectors that could be critical in specific IoT deployments.
3. The benchmark datasets used in NF-UQ-NIDS were collected between 2015 and 2018, potentially limiting their relevance to current threat landscapes. IoT attack techniques have evolved significantly since dataset collection, with new vulnerabilities and attack methods emerging regularly. Furthermore, IoT communication protocols and security mechanisms have advanced, potentially affecting the applicability of historical attack patterns to modern IoT infrastructures. This temporal gap between training data and current deployment environments represents a significant challenge for maintaining detection effectiveness over time.

CONCLUSION AND FUTURE DIRECTIONS

This study aimed to design an efficient and lightweight IDS model for heterogeneous IoT environments using a hybrid ML architecture and a multi-dataset evaluation strategy. The methodology enabled robust, reproducible results that confirmed the research assumptions and closed the identified gap.

The experimental outcomes demonstrated high binary and multi-class classification accuracy with low computational demand, validating the proposed contributions. The study thus makes a meaningful contribution to IoT security literature and practical deployment frameworks.

It is recommended to further explore adaptive ensemble models across broader and more diverse IoT datasets and to investigate integration into industrial IoT infrastructures. Future research should examine collaborative learning mechanisms and scalability testing.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge Rachis Systems Sdn. Bhd. (Malaysia) for their generous funding and continuous support in advancing this research.

REFERENCES

Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). A state-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks*, *206*, 108771. https://doi.org/10.1016/j.comnet.2022.108771

Alghanmi, N., Alotaibi, R., & Buhari, S. M. (2022). Machine learning approaches for anomaly detection in IoT: An overview and future research directions. *Wireless Personal Communications*, *122*, 2309-2324. https://doi.org/10.1007/s11277-021-08994-z

Aljebreen, M., Alohali, M. A., Saeed, M. K., Mohsen, H., Al Duhayyim, M., Abdelmageed, A. A., Drar, S., & Abdelbagi, S. (2023). Binary chimp optimisation algorithm with ML-based intrusion detection for secure IoT-assisted wireless sensor networks. *Sensors*, *23*(8), 4073. https://doi.org/10.3390/s23084073

Altamimi, A. S. H., Al-Dulaimi, O. R. K., Mahawish, A. A., Hashim, M. M., & Taha, M. S. (2020). Power minimisation of WBSN using an adaptive routing protocol. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(2), 837-846. https://doi.org/10.11591/ijeecs.v19.i2.pp837-846

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors, 24*(2), 713. https://doi.org/10.3390/s24020713

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3677. https://doi.org/10.3390/s24020713

Awad, M., Fraihat, S., Salameh, K., & Al Redhaei, A. (2022). Examining the suitability of NetFlow features in detecting IoT network intrusions. *Sensors, 22*(16), 6164. https://doi.org/10.3390/s22166164

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers, 12*(2), 34. https://doi.org/10.3390/computers12020034

Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things, 3*, 5. https://doi.org/10.1007/s43926-023-00034-5

Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2021). Novel approach for detection of IoT-generated DDoS traffic. *Wireless Networks, 27*, 1573-1586. https://doi.org/10.1007/s11276-019-02043-1

Da Poian, V., Theiling, B., Clough, L., McKinney, B., Major, J., Chen, J., & Hörst, S. (2023). Exploratory data analysis (EDA) machine learning approaches for ocean world analog mass spectrometry. *Frontiers in Astronomy and Space Sciences, 10*, 1134141. https://doi.org/10.3389/fspas.2023.1134141

Du, J., Yang, K., Hu, Y., & Jiang, L. (2023). NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning. *IEEE Access, 11*, 24808-24821. https://doi.org/10.1109/ACCESS.2023.3254915

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), 44. https://doi.org/10.3390/fi12030044

Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. *Physical Communication, 52*, 101685. https://doi.org/10.1016/j.phycom.2022.101685

Jiang, K., Wang, W., Wang, A., & Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access, 8*, 32464-32476. https://doi.org/10.1109/ACCESS.2020.2973730

Kaur, J., Jaskaran, Sindhwani, N., Anand, R., & Pandey, D. (2022). Implementation of IoT in various domains. In N. Sindhwani, R. Anand, M. Niranjanamurthy, D. C. Verma, & E. B. Valentina (Eds.), *IoT based smart applications* (pp. 165-178). Springer. https://doi.org/10.1007/978-3-031-04524-0_10

Khan, P. W., & Byun, Y.-C. (2022). Multi-fault detection and classification of wind turbines using stacking classifier. *Sensors, 22*(18), 6955. https://doi.org/10.3390/s22186955

Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: A comprehensive review. *Wireless Personal Communications, 114*, 1687-1762. https://doi.org/10.1007/s11277-020-07446-4

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management, 62*, 102442. https://doi.org/10.1016/j.ijinfomgt.2021.102442

Kunhare, N., Tiwari, R., & Dhar, J. (2020). Particle swarm optimisation and feature selection for the intrusion detection system. *Sādhanā, 45*, 109. https://doi.org/10.1007/s12046-020-1308-5

Lin, L., Di, L., Zhang, C., Guo, L., Di, Y., Li, H., & Yang, A. (2022). Validation and refinement of cropland data layer using a spatial-temporal decision tree algorithm. *Scientific Data, 9*, 63. https://doi.org/10.1038/s41597-022-01169-w

Oladimeji, D., Gupta, K., Kose, N. A., Gundogan, K., Ge, L., & Liang, F. (2023). Smart transportation: An overview of technologies and applications. *Sensors, 23*(8), 3880. https://doi.org/10.3390/s23083880

Quy, V. K., Hau, N. V., Anh, D. V., & Ngoc, L. A. (2022). Smart healthcare IoT applications based on fog computing: Architecture, applications, and challenges. *Complex and Intelligent Systems, 8*, 3805-3815. https://doi.org/10.1007/s40747-021-00582-9

Rajaan, R., Singh, B., & Choudhary, N. (2025). Advancements in IoT anomaly detection: Leveraging machine learning for enhanced security. *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence, 189*, 367-389. https://doi.org/10.2991/978-94-6463-700-7_30

Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2023). Deep learning-based network intrusion detection system for resource-constrained environments. In S. Goel, P. Gladyshev, A. Nikolay, G. Markowsky, & D. Johnson (Eds.), *International Conference on Digital Forensics and Cyber Crime* (pp. 355-367). Springer. https://doi.org/10.1007/978-3-031-36574-4_21

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*, 107810. https://doi.org/10.1016/j.compeleceng.2022.107810

Saheed, Y. K., Usman, A. A., Sukat, F. D., & Abdulrahman, M. (2023). A novel hybrid autoencoder and modified particle swarm optimisation feature selection for intrusion detection in the Internet of Things network. *Frontiers in Computer Science, 5*, 997159. https://doi.org/10.3389/fcomp.2023.997159

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2021). NetFlow datasets for machine learning-based network intrusion detection systems. In Z. Deze, H. Huang, R. Hou, S. Rho, & N. Chilamkurti (Eds.), *International Conference on Big Data Technologies and Applications* (pp. 117-135). Springer. https://doi.org/10.1007/978-3-030-72802-1_9

Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly-based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering, 107*, 108626. https://doi.org/10.1016/j.compeleceng.2023.108626

Sheykhmousa, M., Mahdianpari, M., Ghanbari, H., Mohammadimanesh, F., Ghamisi, P., & Homayouni, S. (2020). Support vector machine versus random forest for remote sensing image classification: A meta-analysis and systematic review. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 13*, 6308-6325. https://doi.org/10.1109/JSTARS.2020.3026724

Sulyman, A. I., & Henggeler, C. (2022). Physical layer security for military IoT links using MIMO-beamforming at 60 GHz. *Information, 13*(2), 100. https://doi.org/10.3390/info13020100

Uddin, S., Haque, I., Lu, H., Moni, M. A., & Gide, E. (2022). Comparative performance analysis of k-nearest neighbour (KNN) algorithm and its different variants for disease prediction. *Scientific Reports, 12*, 6256. https://doi.org/10.1038/s41598-022-10358-x

Vibhute, A. D., Khan, M., Patil, C. H., Gaikwad, S. V., Mane, A. V., & Patel, K. K. (2024). Network anomaly detection and performance evaluation of convolutional neural networks on UNSW-NB15 dataset. *Procedia Computer Science, 235*, 2227-2236. https://doi.org/10.1016/j.procs.2024.04.211

Walling, S., & Lodh, S. (2024). Network intrusion detection system for IoT security using machine learning and statistical-based hybrid feature selection. *Security and Privacy, 7*(6), e429. https://doi.org/10.1002/spy2.429

Xu, H., Sun, Z., Cao, Y., & Bilal, H. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Soft Computing, 27*, 14469-14481.https://doi.org/10.1007/s00500-023-09037-4

Yang, M., & Zhang, J. (2023). Data anomaly detection in the Internet of Things: A review of current trends and research challenges. *International Journal of Advanced Computer Science and Applications, 14*(9). https://doi.org/10.14569/IJACSA.2023.0140901

Yaseen, N. A., Hadad, A. A.-A., & Taha, M. S. (2021). An anomaly detection model using principal component analysis technique for medical wireless sensor networks. In *International Conference on Data Science and Its Applications* (pp. 66-71). IEEE. https://doi.org/10.1109/ICoDSA53588.2021.9617547