ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

Al-Noor Journal for Information Technology and Cybersecurity

https://jncs.alnoor.edu.iq/

An Ensemble Approach for Detecting Network Attacks in IoT Environments

[1]Mahmood Al-fathe, [2]Balqees Talal Hasan,

[1]Department of Computer Network and Internet, College of Information Technology, Ninevah University, Mosul/ Iraq.
[2]Department of Artificial Intelligence, College of Information Technology, Ninevah University, Mosul / Iraq.

Article information

Article history:
Received: November, 01, 2025
Revised: November, 30, 2025
Accepted: December, 19, 2025

Keywords:
Cyber-attacks
Intrusion Detection System (IDS)
Internet of Things (IoT)
Machine learning
Ensemble Learning

Correspondence:

Mahmood Al-fathe
mahmood.alfathe@uoninevah.edu.iq

Abstract

The Internet of Things (IoT) were declared to be the largest and connected network comprising millions of devices aimed at efficiency, automation, and better decision-making; hence it has been popularly branded "the fourth industrial revolution." But with the arrival of many IoT systems, their vulnerability to cyberattacks is also growing, thereby putting the connected devices and networks in severe compromised positions. This paper investigates the opportunity of using machine learning (ML) and ensemble techniques for enhancing cyber-attack detection in IoT environments. Six machine learning algorithms, including Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors (KNN), Gradient Boosting, and Naive Bayes, were evaluated for detecting attacks in IoT network traffic. The ensemble comprised of the three models with the best performance combined in a soft-voting manner so that the complementary strengths were exploited, hence improving robustness and generalization. The performance of the ensemble was measured using accuracy, precision, recall, F1-score, and the area under the Receiver Operating Characteristic curve. The proposed ensemble shows a test accuracy of 99.91%, demonstrating its capacity to detect cyber threats effectively and the promise of ensemble learning schemes in securing cosmopolitan IoT infrastructures.

DOI: https://doi.org/10.69513/jncs.v2.i2.a9

1. Introduction

IoT refers to an expanding, vast, passive network of millions of devices connected across the globe to achieve efficiency and convenience in various human activities. The newly introduced advances in technology coupled with this global interconnectedness have earned this development the title of "the fourth industrial revolution" (B. T. Hasan & Badran, 2023) because they have overtly transformed global connectivity into integrating devices, users, and processes spanning independent industrial sectors. Yet, an increasing number of linkages in IoT systems has resulted in escalation of security issues, primarily because of the vulnerability of resource-constrained IoT nodes that usually deploy in untrusted or unsafe environments (Albalwy & Almohaimeed, 2025).

The increasing complexity of modern attacks has proven too much for traditional security systems, which mostly rely on static defences like firewalls and IDS/IPS technology (Parkar & Bilimoria, 2021). The Artificial Intelligence of Things (AIoT), which is the result of the convergence of IoT and AI, presents both new cybersecurity challenges and substantial opportunities for innovation (Dangwal et al., 2025). Machine learning (ML) has become an effective tool to identify anomalies in IoT systems (Inuwa & Das, 2024), owing to its capability of drawing insights from large and heterogeneous datasets, recognizing subtle behavioral patterns, and adjusting to changing operational contexts.

However, while tremendous advancements have been made using single ML models, a huge body of literature is still missing that focuses on the

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

robustness of these detection mechanisms in question. The single classifiers often suffer from a high variance and may not generalize very well across the various attack types manifested in heterogeneous IoT traffic. In a more recent work, Sharmila et al. (Sharmila & Nagapadma, 2023) created the RT-IoT2022 dataset and proposed optimized Quantized Autoencoder models, namely QAE-u8 and QAE-f16, for resource-constrained environments; however, it remains to be seen whether ensemble techniques can maximize further detection accuracy and reliability to an extent higher than its individual or specialized models.

To address this gap, this study formulates the following research questions:

RQ1: How do traditional machine learning algorithms compare in detecting modern cyber-attacks within the RT-IoT2022 dataset?

RQ2: Can a soft-voting ensemble approach outperform individual classifiers in terms of F1-score and generalization capability?

RQ3: What are the trade-offs between utilizing complex ensemble models and single classifiers in an IoT intrusion detection context?

Based on these questions, our study leverages the RT-IoT2022 dataset to assess the performance of the proposed ensemble learning strategy compared to traditional ML techniques. Research that fosters advanced intrusion detection frameworks in the AIoT ecosystem has shown how ensemble learning sharpens the defense mechanism of IoT infrastructures against swift invasions.

The subsequent organization of the remaining parts of the paper includes: literature review when objectives of the research are monitored and achieved on section 3, results and discussions of the experimental are in section 4, and remarks and conclusions in section 5.

2. Literature Review

The increasing complexity of IoT systems and growing sophistication of Cyber-attacks have motivated a tremendous effort in research into ML and DL applications in attack detection in IoT networks. This section provides a detailed review of the available literature on cyber-attack detection in IoT networks.

The applicability of deep learning methods for the detection of DoS attacks in wireless sensor networks was investigated by Salmi and Oughdir (Salmi & Oughdir, 2023) through the conception, development, and deployment of DNN, CNN, RNN, and hybrid RNN-CNN models. The CNN was finally evaluated on the WSN-DS dataset and recorded the highest accuracy of detection at 98.79%. However, the authors noted deep-learning-based techniques usually come with tremendous computation costs, which may hinder their application in WSNs. Hence, lightweight and flexible security mechanisms are still a must in dealing with such harsh environments. In this direction, Dener et al. (Dener et al., 2024) presented the WSN-BFSF dataset for a benchmark on DoS attack detection in wireless sensor networks (WSNs) in consideration of ML and DL models, accomplishing good detection performance.

Further studies extended the attack detection using machine learning to the domain of IoT. Pahl and Aubet proposed an anomaly detection mechanism based on machine learning modeling of the behavior of IoT microservices so that security features such as access control and firewalling can be retrofitted into existing IoT deployments. Similarly, Kayode Saheed et al. presented a machine learning-driven intrusion detection system (ML-IDS) aimed at detecting malicious activity specifically in IoT networks. Here, the authors adopted supervised learning algorithms to improve both the accuracy and the reliability of detection. Experimental validation was performed with the UNSW-NB15 dataset, which serves as a benchmark for evaluating the model performance.

Recent research increasingly adopts deep learning techniques against the backdrop of increasing scale and complexity associated with IoT networks. Employing machine learning and deep learning techniques in an anomaly-based intrusion detection system allows Manaa et al. to diagnose and mitigate DDoS attacks targeting IoT networks. Evaluation on many IoT datasets indicates the high accuracy of Random Forest and LSTM methods, thus proving their capability in safeguarding IoT infrastructure (Ebady Manaa et al., 2024). More so, Susilo et al. (Susilo et al., 2025) proposed a multistage-deep learning architecture combining autoencoders, LSTM, and CNN models will add on value through SMOTE enhancing their approach in detecting cyber-attack in IoT network. This improves feature extraction, handling data imbalance, and accuracy and effectiveness of intrusion detection systems in IoT.

Thus, giving rise to the evolution of adaptive, scalable, and accurate intrusion detection systems for IoT networks, these studies in totality prompt advocating adoption of ensemble-based approaches for further enhancement of robustness, generalization, and sophistication detection during cyber-attacks.

3. Background

This part presents a description of the techniques used for cyber-attack detection in IoT networks, focusing on traditional machine learning algorithms and ensemble learning strategies.

3.1 Machine Learning Algorithms

The models used in the study to classify cyber-attacks in IoT environments are data-driven.

- **Logistic Regression (LR): T**his method is adopted in classification to foresee predictive values that suit categorical dependent variables. It is also well-designed for binary options where the outcome is either belonging to one or recused to one(Ekanayake et al., 2018).

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

- **The Decision Tree (DT):** This is a technique whereby data are split into branches which carry pathways of decision, and end at a leaf reinforcing the outcome and thereby predicting the target variable through an easy decision logic(Hassan et al., 2019).
- **Random Forest (RF):** It ensembles predictions gotten from many decision tree classifiers which have been trained independently on various parts of the training dataset and therefore result in the improvement of the predictive accuracy(Salem et al, 2014).
- **K-Nearest Neighbors (KNN): I**t classifies the given data point by evaluating the majority class of its k closest neighbors. It is a kind of semi-supervised learning method that uses relationships between distance-based values of data points to classify (Alduailij et al., 2022).
- **Gradient Boosting:** This algorithm combines weak base learners into a single composite model, usually a decision tree, to realize outstanding predictions. It works by repeatedly optimizing the residual errors created by former models to improve whole accuracy (Salem et al., 2024).
- **Naive Bayes:** This is a method in the classifiers that are in terms of probability based on the Gaussian distribution, which would assume that each feature independently affects the probability of the outcome and thus amalgamates these probabilities for predicting the most likely class (M. Hasan et al., 2019).

3.2 Ensemble Learning Approach

Ensemble learning is a sophisticated machine learning strategy that combines the outputs of multiple models in order to achieve higher predictive accuracy than any single model could achieve independently (Karamti et al., 2023). The method is especially useful for the more complicated tasks, for example, intrusion detection in IoT environments, where the attempt to model the different attack patterns and subtle distinctions between legitimate and malicious behavior often goes less than sufficient with any single classifier (Jabbar, 2024).

In the present establishment, soft voting hails as a mechanism central to the whole ensemble approach. In soft voting, an aggregated prediction class probabilities are given by constituent models, with the class having the highest average probability selection as final output. This technique is appropriate when models have dissimilar confidence levels, allowing for better-informed predictions via an equally balanced and complementary use of all models involved (Majeed et al., 2021).

4. Methodology

This section presents the dataset to use in this particular research and gives an account of the approach used to detect cyberattacks in IoT networks.

4.1. Dataset Overview

Data collected from RT-IoT2022 Database, published by UCI Machine Learning Repository (UCI Machine Learning Repository, 2022), which includes an open-access dataset. Its gather large scale network traffic data coming from multiple real-time IoT devices using the specific protocols as MQTT and of course Amazon Alexa. It captures normal patterns of traffic, as well as attack scenarios such as some types of Slowloris DDoS or SSH brute-force attacks. It thus possesses 83 input attributes and one target label classifying between normal and attack traffic, thereby providing treasured insight into IoT network behavior and security dynamics. The infrastructure used to generate the RT-IoT2022 dataset, involving various IoT devices and attackers, is visualized in Figure 1."

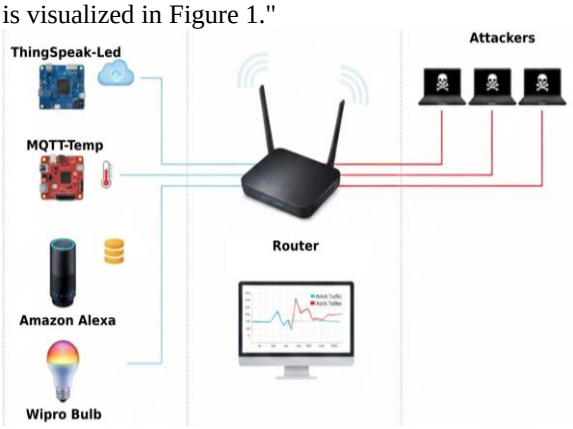
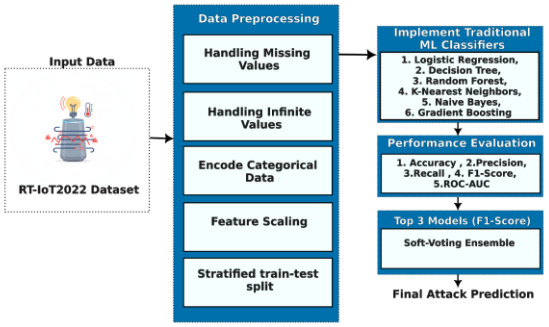


Figure 1. Design and Infrastructure of the RT-IoT2022 Dataset

4.2 Proposed Detection System

The detection system proposed in this research processes raw IoT-network traffic from the RT-IoT2022 dataset by means of a structured workflow of preprocessing, model training, ensemble construction, and overall evaluation, as shown in Figure 2. The raw traffic is first converted to normalized feature vectors suitable for learning. Then, a number of baseline classifications using machine learning are trained and assessed for their performance, with the intent of identifying the strongest competitors. The higher-ranking models are then combined into a soft-voting ensemble to increase the robustness of the detection scheme. The performance evaluation and associated interpretation of confusion matrices and ROC curves will conclude the system validation.



ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

Figure 2. Ensemble Learning System for IoT Network Attack Detection

A. Data Preprocessing

The entire data preprocessing framework for heterogeneous IoT traffic data: transforming heterogeneous data into standard and machine-interpretable feature vectors. Remove missing and infinite values for numerical stability. The last column of the data set is the target label, whereas the rest of the columns make up the feature set. Categorical attributes are automatically detected and encoded numerically using label encoding. Z-score normalization is then applied to the entire feature matrix to ensure a consistent scale across features and enable effective convergence of the model. The final processed data is public. It is then divided into training and testing samples via stratified sampling in terms of class distribution. Label binarization is also used for the multi-class ROC-AUC scores that need to be computed during evaluation.

B. Training Pipeline

All the algorithm presented are Logistic Regression, Decision Tree, Random Forest, K-Nearest Neighbors, Naive Bayes, Gradient Boosting; all of these can be listed as traditional mainstay algorithms, which find their application in the intrusion detection domain. Each model is trained on an appropriately normalized training set with fixed hyperparameters. During testing, a unified evaluation function is used to ensure fair comparison across the various models.

After model benchmarking on individual components, a soft-voting ensemble is created from the three best classifiers, namely, those with the highest F1-Score. This ensemble considers the predicted probabilities of the base models so that the complementary decision boundaries may be used to gain advantages in terms of generalization and detection reliability.

C. Evaluation Strategy

The assessment of the model performance is conducted using various metrics appropriate for multi-class IoT attack detection. Accuracy, precision, recall, and F1-Score have been calculated in order to assess the quality of the classification. The ROC-AUC is calculated using a one-vs-rest method so that a fair performance assessment can be carried across all classes. Confusion matrices illustrate classification behavior at the level of the respective classes and give ROC curves into the threshold-dependent discrimination ability. Comparative bar charts summarize the performance of all classifiers.

D. Optimization Technique

Though primarily optimization, the process of ensemble learning is undertaken. Therefore, in contrast to adopting a single classifier, the system squeezes the top three models together into a soft-voting ensemble, decreasing variance and increasing predictive reliability. For this step, the selection criteria of the ensemble's components would be based solely on empirical F1-Score ranking, meaning only the best and most generalizable models would uphold the final detection system.

4.3. Model Selection and Rationale

The six classifiers (LR, DT, RF, KNN, GB, and NB) were intentionally selected to represent a diverse array of foundational machine learning paradigms commonly applied in intrusion detection systems (IDS). This selection allows for a holistic performance comparison across models with fundamentally different operational characteristics:

Model Family	Represented Models	Characteristics
Regression/Linear	Logistic Regression (LR)	Fast, highly interpretable, performs best when features are linearly separable.
Distance-Based	K-Nearest Neighbors (KNN)	Simple, non-parametric, relies on proximity, but computationally expensive during prediction.
Probabilistic	Naive Bayes (NB)	High-speed training, based on conditional probability, but assumes feature independence.
Tree-Based	Decision Tree (DT), Random Forest (RF)	Robust to feature scaling, handles non-linear relationships well, but prone to overfitting (DT).
Boosting/Ensemble	Gradient Boosting (GB)	Sequentially builds weak learners to correct previous errors, achieving state-of-the-art performance but at high computational cost.

Ensemble learning was chosen as the ultimate proposed solution to overcome the inherent weaknesses of individual models. While single classifiers like **Decision Trees** are fast, they suffer from high **variance** (small data changes lead to large prediction changes), and models like **Logistic Regression** suffer from high **bias** (inability to model complex non-linear data).

The **soft-voting ensemble** combines the predictions of the top-performing base models to leverage the principle of *'wisdom of the crowd.'* By aggregating diverse predictions, the ensemble effectively reduces the overall **variance** (achieved through models like Random Forest) and the **bias** (achieved through complex models like Gradient Boosting) simultaneously. This is particularly crucial for IoT IDS, where traffic data is often highly imbalanced and non-stationary, requiring a highly generalized and robust detector.

5. Experimental Results and Discussion

The experimental validation of the detection framework proposed in this work is presented in this section, along with an outline of the metrics used and results obtained for all model classes. The results are further analyzed to extract insights, comparative strengths, and the effectiveness of the ensemble approach for IoT attack detection enhancement.

5.1 Evaluation Criteria

In order to assess the efficiency of the enacted model of cyber-attack detection, the performance metrics of precision, recall, F1-score, area-under-the-Receiver Operating Characteristic (ROC) curve, and overall

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

accuracy were calculated, as defined below (Sarker et al., 2020).

$$Precision = \frac{TP}{TP + FP} (1)$$

$$Recall = \frac{TP}{TP + FN} (2)$$

$$F1 - score = \frac{2 * Precision * Recall}{Precision + Recall} (3)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} (4)$$

True positives are denoted with TP, false positives with FP, true negatives with TN, and false negatives with FN in the above definitions. The performance of the proposed security model is also evaluated using ROC curves based on TPR plotted against FPR as a function of the evaluation metrics.

5.2 Results

The Evaluation results in Table1 demonstrate that all models evaluated show strong predictive capability on the task of RT-IoT2022 for attack detection; notwithstanding, the Voting Classifier performs well across all other metrics. The proposed ensemble, through use of a soft-voting mechanism, works by combining the three best ranking classifiers from the benchmarking exercises-Random Forest, Decision Tree, and Gradient Boosting. By combining class-probability outputs from these diverse learners, the ensemble reduces variance, captures complementary decision boundaries, and counteracts weaknesses of individual models. In such an unlocked synergy, results in better metrics with accuracy, precision, recall, and F1-score all being 0.9991, and tremendously high ROC-AUC equal to 0.9999.

Outspread, the Random Forest is virtually at par with itself, indicating robustness in high dimensionality with multitarget non-linear interaction features typical in IoT traffic. The Decision Tree also predicts convincingly well, but not as well as Random with indicating that quite a bit of hidden structure is captured with one tree. Gradient Boosting proves competitive results from its working mechanism of iterative error correction, although the metric numbers are just below the other two methods based on trees.

K-Nearest Neighbors and Logistic Regression show relatively strong performance, though lower compared with other models, and are much more sensitive to the feature distribution and boundary defined by the data in determining performance. Naive Bayes performed the most poorly, owing to its independence assumption on data, but achieved a high ROC-AUC at 0.9975, suggesting that it is still good at ranking across the classes.

In summary, the results speak in favor of the reliability of ensemble models consisting of Random Forest, Decision Tree, and Gradient Boosting-the combination was through soft voting-in offering robust capabilities for intrusion detection by having significantly outperformed individual models and also establishing the need for ensemble-based optimization in IoT security.

Table 1. Evaluation of Classification Models

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Ensemble Voting Classifier	0.9991	0.9991	0.9991	0.9991	0.9999
Random Forest	0.9988	0.9988	0.9988	0.9988	0.9999
Decision Tree	0.9983	0.9983	0.9983	0.9983	0.9991
Gradient Boosting	0.9972	0.9974	0.9972	0.9973	0.9989
K-Nearest Neighbors	0.9940	0.9940	0.9940	0.9940	0.9991
Logistic Regression	0.9888	0.9888	0.9888	0.9887	0.9993
Naive Bayes	0.9379	0.9570	0.9379	0.9371	0.9975

6. Conclusion

An ensemble-based scheme for intrusion detection in IoT networks was proposed in this study and employed the RT-IoT2022 dataset. Following the evaluation of six machine-learning classifiers, the top three classifiers-Random Forest, Decision Tree, and Gradient Boosting-were combined in a soft vote ensemble for greater robustness and generalization. The proposed model achieved 99.91% accuracy with near-perfect precision, recall, F1-score, and ROC-AUC, all of which are far superior to that of the individual classifiers. These findings convey the efficacy of ensemble learning in detecting the variety of IoT-based cyber-attacks and increasing the reliability of intrusion detection systems. Future work can be directed toward optimizing this framework for deployment onto resource-constrained IoT devices; also, exploring adaptive or deep-learning–based extensions.

References

1. Albalwy, F., & Almohaimeed, M. (2025). Advancing Artificial Intelligence of Things security: Integrating feature selection and deep learning for real-time intrusion detection. *Systems*, *13*(4), 231.
2. Alduailij, M., Khan, Q. W., Tahir, M., Sardaraz, M., Alduailij, M., & Malik, F. (2022). Machine-learning-based DDoS attack detection using Mutual Information and Random Forest Feature Importance method. *Symmetry*, *14*(6), 1095.
3. Dangwal, G., Wazid, M., Nizam, S., Chamola, V., & Das, A. K. (2025). Automotive cybersecurity scheme for intrusion detection in CAN-driven artificial intelligence of Things. *Security and Privacy*, *8*(1). https://doi.org/10.1002/spy2.483
4. Dener, M., Okur, C., Al, S., & Orman, A. (2024). WSN-BFSF: A New Data Set for Attacks Detection in Wireless Sensor Networks. *IEEE Internet of Things Journal*, *11*(2), 2109–2125.
5. Ebady Manaa, M., Hussain, S. M., Alasadi, S. A., & Al-Khamees, H. A. A. (2024). DDoS attacks detection based on machine learning algorithms in IoT environments. *Inteligencia Artificial*, *27*(74), 152–165.
6. Hasan, B. T., & Badran, A. I. (2023). A study on energy management for low-power IoT devices. In *Low Power Architectures for IoT Applications* (pp. 1–24). Springer Nature Singapore.
7. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things (Amsterdam, Netherlands)*, *7*(100059), 100059.
8. Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. *Internet of Things (Amsterdam,*

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a9

Netherlands), *26*(101162), 101162.

9. Jabbar, H. G. (2024). Advanced threat detection using soft and hard voting techniques in ensemble learning. *Journal of Robotics and Control (JRC)*. https://journal.umy.ac.id/index.php/jrc/article/view/22005
10. Karamti, H., Alharthi, R., Anizi, A. A., Alhebshi, R. M., Eshmawi, A. A., Alsubai, S., & Umer, M. (2023). Improving prediction of cervical cancer using KNN imputed SMOTE features and multi-model ensemble learning approach. *Cancers*, *15*(17), 4412.
11. Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395–9409.
12. Majeed, R., Abdullah, N. A., Faheem Mushtaq, M., Umer, M., & Nappi, M. (2021). Intelligent cyber-security system for IoT-aided drones using voting classifier. *Electronics*, *10*(23), 2926.
13. Pahl, M.-O., & Aubet, F.-X. (2018). All eyes on you: Distributed multi-dimensional IoT microservice anomaly detection. *2018 14th International Conference on Network and Service Management (CNSM)*, 72–80.
14. Parkar, P., & Bilimoria, A. (2021). A Survey on Cyber Security IDS using ML Methods. *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 352–360.
15. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00957-y
16. Salmi, S., & Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. *Journal of Big Data*, *10*(1). https://doi.org/10.1186/s40537-023-00692-w
17. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry*, *12*(5), 754.
18. Sharmila, B. S., & Nagapadma, R. (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity*, *6*(1). https://doi.org/10.1186/s42400-023-00178-5
19. Susilo, B., Muis, A., & Sari, R. F. (2025). Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm. *Sensors (Basel, Switzerland)*, *25*. https://doi.org/10.3390/s25020580
20. *UCI Machine Learning Repository*. (n.d.). Retrieved November 12, 2025, from https://archive.ics.uci.edu/dataset/942/rt-iot2022