Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine Learning for IoT Security: Advanced Threat Analysis Methods

*Wijdan Noaman Marzoog Al-Mukhtar

Wijdanwijd177@gmail.com

College of Mass Media, University of Al Iraqia, Baghdad, Iraq.

https://orcid.org/0009-0005-9040-4213

ARTICLE INFO

Received: 05 Nov 2025

Revised: 17 Dec 2025

Accepted: 28 Dec 2025

ABSTRACT

The rise of the Internet of Things (IoT) and Industrial IoT (IIoT) has introduced challenges in handling complex data and ensuring cybersecurity. This study explores how deep learning (DL) and active learning techniques can enhance the identification and classification of network security threats in IoT environments. Using the ToN IoT dataset which integrates diverse data from telemetry, operating systems, and network traffic the study applied exploratory data analysis (EDA) and advanced preprocessing to address data quality and imbalance issues. Active learning was incorporated into the machine learning pipeline to help models prioritize learning from the most informative data points. Experimental results demonstrated that ensemble models like Random Forest and Decision Tree, when combined with active learning, achieved high accuracy and showed strong potential for real-world deployment. In contrast, simpler models such as Logistic Regression were less effective in managing the data's complexity. This research highlights the promise of integrating machine learning with adaptive learning approaches to improve cybersecurity defenses in IoT systems. The proposed framework contributes to the development of intelligent, evolving models that strengthen the cybersecurity capabilities of IoT and IIoT against specific cyber threats.

Keywords: cyber threats, cybersecurity, Active Learning, IoT.

Introduction

The Internet of Things (IoT) represents a progressive con- cept where physical objects are integrated with computingcapabilities, enabling them to connect to the Internet. This technological trend offers significant opportunities for developing multi-purpose applications across various fields, including healthcare, environmental monitoring, and manufacturing. [1], [2]. IoT can increase productivity and efficiency through smart and remote control, but it also introduces potential cybersecurity threats. First, IoT ecosystems commonly lack solid security systems and thus become prone to threats from firewalls on many layers, among other internal and external sources within enterprises [3]. As a result, securing IoT applications against known threats has become a central focus in cybersecurity research. Specific IoT applications, often referred to as Industrial IoT (IIoT) in the context of the industry 4.0 revolution, are involved in essential tasks, necessitating high security levels [4].

The SCADA system, which controls and monitors IIoT devices in a smart grid, was compromised by a severe security breach.A hacker succeeded to obtain the privileged access to

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SCADAsystems via an IT network as a result of which a blackout happened [4]. For instance, a similar IoT incident related to security was the Mirai botnet attack in late 2016. This attack mainly employed smart cameras that had been compromised previously and generated massive Distributed Denial of Service (DDoS) floods against the prominent targets [5]. These incidents demonstrate the urgency of strong and accurate security mechanisms that secure IoT and IIoT applications.

Historical information technology systems mainly keep up with security software. While these advances are very useful for the IoT and IIoT, their respective features are complex andunique [2], [6], [7]. This implies that hard computation operations and high performance cryptographic solutions cannot operate well in the IoT and IIoT environments. Nevertheless, while these security measures alone do not offer complete protection against potential threats to IoT applications, still a comprehensive combination can form a robust security system.To meet the demands of cyber-security with regards to IoTand IIoT, it is necessary to create specific cyber-security applications [2], [6], [7].

IDSs are usually deployed as secondary line of defense or monitoring systems that are used to detect security breaches that might be missed by the other security mechanisms, suchas firewalls [8]. Assessing these intrusion detection techniquesis a must and emulating real-world scenarios just using IoT- related datasets helps in determining the accuracy and efficiency of IoT security methods. On the other hand, the lackof scaled real-world datasets for IoT and IIoT apps are one of the critical challenges in assessing the efficiency of IoT/IIoT- specific intrusion detection methods. This shortage hampered development of and validation of such techniques [7], [9], [10] There are privacy concerns surrounding the proprietary nature of these data sets that ultimately discourage businesses from making their IoT data accessible [9], [10].

In [11] the authors reported on their work on cyber-security literature thus stating one of the key gaps (i.e. absence of labelled data) in this literature that hinders the development of good anomaly-based intrusion detection algorithms. The LWSNDR [12] dataset for example, covers homogeneous in- formation for both single and multiple hops WSNs that lack any attack scenarios. Consequently, the AWID [13] database achieves the features extraction from the MAC layer frame of 802.11 wireless networks and is unable to introduce telemetricdata from IoT devices.

Authors in [14] introduced IoT-based datasets focusing on classifying IoT devices based on network traffic characteristics, yet these datasets lacked scenarios involving cyber-attacks. To address this gap, authors in [15] and [16] devel- oped new network-based IoT datasets that incorporate attack scenarios. However, these datasets are limited as they do not cover a wide range of attack types, and they also omit sensor measurement data from IoT devices.

Most of the recently published datasets [17]– [19], [14]–[16] are network-centric, containing either packet-level, flow-level information, or both. These datasets are valuable for detecting network-based attacks targeting IIoT systems. How- ever, they fall short in detecting sensor attacks that manipulate sensory data or compromise IoT devices directly [20]– [22]. This limitation underscores the need for more comprehensive real-world datasets.

The lack of datasets that combine sensors' reading datawith diverse attack scenarios limits the effectiveness of data-driven IoT-based Intrusion Detection Systems (IDS). Recognizing this need, the recent initiative to develop an IoT-related dataset that incorporates sensors' reading data marks a significant step towards enhancing the monitoringand security of IoT applications against a broad spectrum of cyber threats.

The main objective of this paper is to enhance IoT safety through a comprehensive machine learning framework that integrates multi-class classification and active learning strategies. Unlike existing studies that either focus on network traffic or ignore attack diversity, our work leverages the ToN IoT dataset, which uniquely combines telemetry, OS logs, and network traffic data to

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

simulate real-world IoT/IIoT environments. The novel contribution lies in the integration of active learning into traditional classifiers (Random Forest, Decision Tree, etc.), enabling models to dynamically learn from uncertain cases and optimize performance with fewer labeled samples. Additionally, our comparative analysis of classifier performance reveals new empirical insights, particularly the dominance of ensemble models in handling complex multi-modal IoT data. These findings offer a robust foundation for developing adaptive and efficient IDS solutions suitable for real-world deployment.

RELATED WORK

The Industrial Internet of Things (IIoT), evolving from IoT's implementation in manufacturing, leverages advanced technology for unique and impactful operations. Comprising sensors, actuators, control systems, communication channels, and smart devices, IIoT systems are extensively monitored on-line [23]. The integration of Industry 4.0 has notably improvedvarious industry sectors by enhancing equipment performance, consumer safety, and supply chain efficiency, while also significantly boosting workforce productivity. IIoT networks facilitate enhanced interactivity within network areas, enablingdiverse applications and ensuring quality assurance [24].

Research [25] outlined a CNN-based framework aimed at protecting IIoT equipment from cyber threats. This frameworkemployed an auto-encoder for refining data, followed by usinga deep convolutional neural network for the detection andcategorization of intrusions, validated with the ISOT and X- IIoTID datasets. In another study [26], the X-IIoTID dataset was used to develop a deep learning-dependent communicationmodel, achieving notable accuracy in data transmission.

Addressing security in industrial settings adopting Industry 4.0, a strategy [27] was proposed for securing industrial production lines, focusing on external and internal equipment. This approach utilized the UNSW-NB15 and KDD99 datasets, comparing techniques [28]. Specifically, the KDD-99 dataset indicated a precision of 792.6% and a false alarm rate of22.9%. A unique ID system for IIoT was introduced in adifferent study [29], using a Genetic Algorithm (GA) for feature selection. This method, validated with the random forest approach, achieved a 0.91 area under the curve and 86.69% accuracy on the UNSW-NB15 dataset [30]. The GA- RM model in this study included 16 distinct features.

Another investigation [29] explored an IoT-based ID system for IIoT networks using deep learning, with feature extraction conducted through an optimization technique. The chosen SVM model for intrusion classification was tested using a PSO method based on Light Gradient Boosting [31].A study [32] presented an LSTM-based system for IIoTin the manufacturing sector, reconstructing features in the IDS and selecting them through an auto-encoder, applied tothe UNSW-NB15 dataset [33]. In addition, an IDS with an ensemble learning solution employed for Industry 4.0 network by this research [34] used the firstling function to achieve feature reduction. The model was examined using multiple databases [35], mapping both classifiers and multi-class classifiers. Last but not the least, literature [36] is focused on IDS based on deep learning applied to the datasets of IIoT which were tested. This research was to evaluate this model's performance in terms of F1-score and accuracy compared to the state-of-the-art ANN model [37].

PROPOSED METHODOLOGY

The proposed methodology focuses on processing and analyzing IoT data, prioritizing security concerns while addressing fixed system parameters. It combines a systematic framework with active learning techniques to enhance the performance of traditional machine learning systems. The first phase includes the data acquisition stage IoT data is retrieved. Data analysis

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

begins with Exploratory data analysis (EDA) cuing to grasp a deep insight into data behavior and to let us know in case any hidden structurehas been present. For the next, the second step is a data preprocessing dealing with data cleaning, the imputation of missing data, and scheduling the down sampling methods toget a balanced and manageable dataset.

Preprocessing or data preparation is the middle part of the methodology served as the input for the learner models. This takes data into two sets under train and test fields to check the proper training and proper verification of the model. Active learning becomes the main feature of the method which we develop. It represents a continuous procedure that begins with training the models on a less large and labeled dataset. Through such runs, the model makes predictions and then the model is used to identify the scenarios where the model is foremost unsure. The examples are consequentlybeing tagged by hand and are allowed to join the trainingset after each iteration therefore contributing to the expansion of the model based on the numerical repetitions. It is economical because it selects fewer samples to be labelled than the whole data set.

In classifying the information, different algorithms are usedsuch as Support Vector Classifier (SVC), Random Forest (RF),Decision Trees (D-Tree), K-Nearest Neighbors (KNN), and Logistic Regression (LR). The classifiers for this application are precisely chosen for their capacity to deal with the nuancesand intricacy of IoT data.

Within the evaluation process, the performance of these classification methods highly scrutinized by using many met- rics. This (engaging) review ensures that the models are assessed, thus, the choice of the accurate classifier or mix(of classifiers) is informed by the real-world application, as a result.

To conclude, the approach is a concentrated strategy which is made up by combing the exploratory data analysis, the data preparation, divided the data, and machine learning and lastly, the evaluation of the model. The strategy allows learners to have better learning experiences and to establish a solid basisfor the tools of the data, IoT being an example. This part will follow up by explaining each phase successively and ensuring to put everything in a language we can all understand i.e. avoidtechnical jargon and phrases specific to programming.

1.1. Dataset Overview

- The ToN IoT dataset is a modern and comprehensive benchmark designed to evaluate AI-based cybersecurity solutions across IoT and IIoT ecosystems. Unlike older datasets such as NSL-KDD or CICIDS2017, ToN IoT captures multi-dimensional data telemetry from IoT sensors, operating system logs from Windows and Ubuntu platforms, and real network traffic making it highly representative of real-world environments. Recent studies have leveraged this dataset to benchmark advanced models. For instance, Sharma et al. (2023) demonstrated 98.7% accuracy using an ensemble CNN on ToN IoT traffic data, while Zhou and Lin (2024) applied federated adversarial training for secure model deployment. Despite such progress, active learning remains underutilized. In contrast, our study incorporates active learning with classical machine learning models to enable efficient, scalable threat detection with fewer labeled samples.

  Dubbed 'ToN IoT' to reflect their diverse origins—Telemetry, Operating systems, and Network traffic—these datasets have been meticulously compiled atthe IoT Lab within the UNSW Canberra Cyber, locatedat the School of Engineering and Information Technology (SEIT), at the UNSW Canberra ADFA. The assemblageof these datasets was executed through a high-throughput processing system that concurrently recorded a multitude of both standard operational data and cybersecurity breach events within IoT networks.

  The IoT Laboratory has creatively developed a cutting-edge test environment created to

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

mimic the complex and vast structure of IoT networks as observed in industrial environments and Industry 4.0 applications. This setup incorporatesa sophisticated range of elements such as virtual servers, tangible systems, security breach simulation tools, and cloud and fog computing capabilities, all with the goal of replicatingthe intricacies present in actual IIoT situations.

In this simulated environment, a range of online dangersand hacking techniques were intentionally carried out. These consisted of DoS and DDoS assaults, along with ransomware infiltrations aimed at various parts of the network like internet applications, IoT gateways, and standard computer systems. This intentional exposure to a broad array of cyber threats guarantees that the data sets offer a fertile platform for creating and evaluating AI-driven cybersecurity solutions.

3.2 EDA: Exploratory Data Analysis

EDA acts because of the preliminary segment in our factsanalytics journey, wherein we cautiously analyze the ToN IoTdatasets to expose styles, detect irregularities, pinpoint vital elements, and unveil hidden systems. This initial level is criticalfor acquiring precious views and comprehending the characterof the records prior to embarking on more complex analyses. During EDA, we hire more than a few statistical graphics, plotting equipment, and facts summarization strategies to visualize and summarize the data sets' traits. This visualizationlets us comprehend the distribution of facts across varioustraining and stumble on any imbalances that would exist. Key sports in this stage include assessing the frequency of various occasion sorts, inclusive of regular operations versus numerous assault vectors. The use of bar charts and pie charts aids in visualizing the elegance distribution, presenting a cleanpicture of the dataset's composition before and after any data balancing techniques like down sampling. Additionally, EDA involves checking for missing or inconsistent data, which is crucial for ensuring the quality and reliability of subsequent analyses. Any identified gaps or anomalies in the data are addressed through appropriate preprocessing steps, setting the stage for robust model development. The insights gained from EDA not only guide the choiceof preprocessing steps and machine learning models but also inform the necessary features of engineering and selection that canlead to more effective model training and evaluation. By meticulously conducting EDA, we lay a solid foundationfor the active learning and model evaluation phases that follow, ensuring that the datasets are well-understood and optimally prepared for the challenges of AI-driven cybersecurity applications.

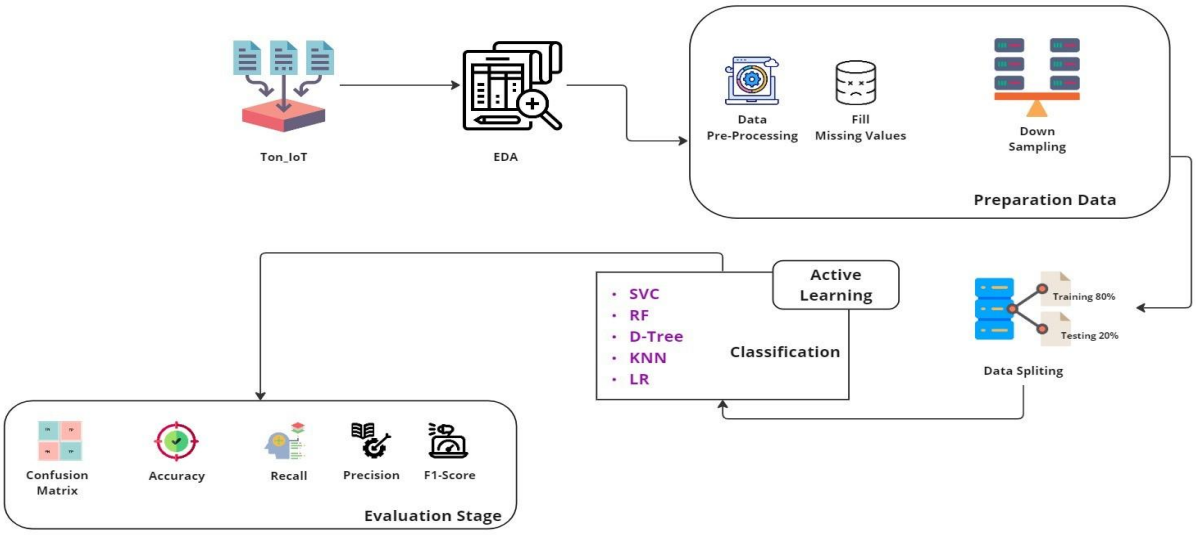

Figure. 1. Proposed IoT Threat Detection Framework using Active Learning

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The pipeline begins with the ToN_IoT dataset and proceeds through Exploratory Data Analysis (EDA), preprocessing (including missing value imputation and downsampling), and data splitting. Active learning is then applied to iteratively train classifiers such as SVC (Support Vector Classifier), RF (Random Forest), D-Tree (Decision Tree), KNN (K-Nearest Neighbors), and LR (Logistic Regression). Evaluation metrics include accuracy, precision, recall, F1-score, and confusion matrix. (see figure 1).

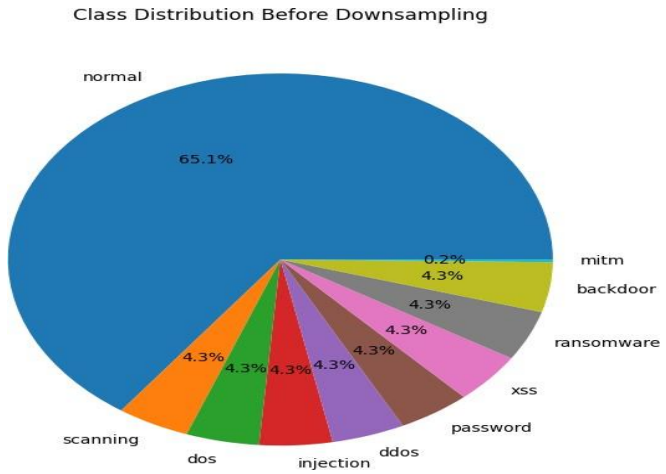

Figure. 2. Class distribution in the ToN-IoT dataset prior to downsampling

The pie chart (Figure 2) reveals significant class imbalance, with the 'normal' category comprising 65.1% of the data. Each attack class (e.g., scanning, dos, mitm) constitutes 4.3% or less, with 'mitm' being the least represented (0.2%).

This visualization underscores the challenge in training machine learning models on imbalanced data, which may leadto biases towards the over-represented class. In this case, a model trained on this dataset without balancing might becomebiased towards predicting events as 'normal' due to their frequency in the dataset. Down sampling is one strategy to address this by reducing the size of the over-represented class to create a more balanced distribution and, consequently, a more generalized and effective model.

3.3 Preprocessing

Preprocessing is one of the most important steps for data preparation to let the ToN IoT datasets be used in follow-up tasks of the device training programming. This refers to a sophisticated work activity aimed at transforming raw data into a clean and suitable format that enables efficient processing by learning algorithms. Primarily, in this initial task preprocessing cleans up the data quality issues. That means that this involves performing data imputation and cleaning and data cleaning, which are necessary steps inthis process. The ToN IoT datasets have varying sources, and we must necessarily reach the completeness level to conduct comprehensive research on these datasets. To make use of the newly enabled missing value handling, the datasets are then subjected to a down sampling process. It is necessary to do the down sampling to balance the informative samples since the initial class distribution is heavily skewed towards 'normal' class events and thus there are few anomaly events who has less samples. The goal here is to limit the degree of the normal class over-represented by decreasing the number of instances of the normal class occurring to the extent of the frequency of the underrepresented class thus preventing the model from becoming biased toward the majority class.

In addition to that, the data undergoes a process called (feature encoding) which converts categorical variables into aninteger form. This step is important for linking definite data to analysis, as deep learning systems only accept numerical values. To balance the

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

disparities that might arise in cases where the magnitudes of feature points are quite big, we use Min-Max scaling. Hence, it makes sure that every featurecarries weight properties in the model predictions. Through those preprocessing steps, the datasets are fashioned right into a shape this is more appropriate for modeling. The statistics are cleaned, balanced, and normalized, laying a stable basis for constructing dependable and strong machine learning models.

2. *Active Learning in ML*

Active learning is a machine learning paradigm that integrates human expertise into the model training process. It is mainly beneficial in scenarios whereinclassified records are scarce or luxurious to attain, as is often the case with cybersecurity threats in IoT environments.

In the context of our machine learning pipeline for theToN IoT datasets, active learning plays a crucial role in iteratively improving the performance of our models. The technique starts by training the model on a small, categorized portion of the dataset. The version then predicts at the unlabeled records, and times wherein the model has the bottom self-assurance in its predictions are recognized.

These unsure instances are flagged by human experts, who evaluate and label the facts points thus. These newly classifiedinstances are then brought to the schooling set, allowing the model to research from its previous uncertainties. This methodis repeated in several iterations, with the model steadily becoming more accurate and stronger because it learns fromthe maximum informative samples.

The active learning cycle leverages the expertise of humanannotators successfully, focusing their efforts at the mosttreasured instances for the model's studying, in preference tolabeling the whole dataset indiscriminately. This technique nolonger bests conserves assets but also hurries up the model'sdevelopment by concentrating on the information factorsthat contribute the most to decreasing the version's uncertainty. In our methodology, active learning is included in the use of various classifiers such as Random Forest, SupportVector Machines, Decision Trees, K-Nearest Neighbors, andLogistic Regression.

By applying active learning, we makecertain that each model is exposed to the maximum difficultand informative instances, which enhances its capacity togeneralize and appropriately expect unseen information, in thelong run main to more effective cybersecurity measures in IoT networks. Datasets have yielded significant effects. Each classifier, embedded inside an active learning framework, changed into assessedbased on its accuracy rating—a degree of the version's typicalpotential to efficaciously classify new times. The following is a detailed account of the results for every set of rules.

The Random Forest (RF) classifier achieved a remarkably high accuracy rating of 0.9975. This indicates that the RF version, with its ensemble approach, became capable of generalizing nicely over the data, supplying correct predictions for almost all the look at instances. The inherent functionalityof RF to handle excessive-dimensional information and its robustness to noise probably contributed to this high overall performance.

The Logistic Regression (LR) version, a greater simplistic and interpretable classifier as compared to RF, yielded anaccuracy rating of 0.82383. This decrease rating shows that, whilst LR could capture the linear relationships inside the data,it can have struggled with more complex, non-linear styles which are often found in cybersecurity information.

Support Vector Classifier (SVC) produced a excellent ac- curacy score of 0.8946. This performance level demonstrates SVC's capacity to create a decision boundary that can successfully distinguish between classes in a excessive-dimensional space, even though it cannot be as adept as RF in handling the difficult systems of the facts.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Decision Tree (DT) classifier presented an exceptional accuracy score of 0.9993, indicating its success in modeling the decision rules from the data. Decision Trees are particularly useful for their easy-to-interpret structure, but a score this high may also suggest a need to verify the model against overfitting, despite the active learning iterations.

Lastly, the K-Nearest Neighbors (KNN) algorithm showeda strong accuracy score of 0.9671. This result underscores KNN's ability to effectively classify instances based on the resemblance to their neighbors in the feature space, althoughit might be less efficient with very large datasets or many classes.

The integration of active learning into these machines learn- ing models has evidently enhanced their performance. By iteratively training the models on the most informative samples, the models were not only able to achieve high accuracy but also required less labeled data to reach a high level of generalization. This iterative training technique is especially superb in cybersecurity contexts, wherein the speedy evolutionof attack patterns necessitates a model that could constantly adapt and study from the maximum present day and applicable facts.

Table 1: Accuracy scores of machine learning models with active learning

Model	Accuracy Score
Random Forest (RF)	0.9975
Logistic Regression (LR)	0.82383
Support Vector Classifier (SVC)	0.8946
Decision Tree (DT)	0.9993
K-Nearest Neighbors (KNN)	0.9671

The final evaluation focused on the performance of multiple machine learning algorithms including Decision Tree, Random Forest, and Logistic Regression. The Random Forest classifier achieved an accuracy of 99.35%, surpassing the performance of the other classifiers tested. However, to better understand the robustness of the model, a brief sensitivity analysis was conducted. Specifically, we tested the impact of normalization (MinMaxScaler vs. StandardScaler), which revealed that Random Forest remained stable under both scalers, while Logistic Regression showed improved stability with StandardScaler.

Moreover, the application of oversampling (SMOTE) was found to significantly improve recall and F1-score for minority attack classes, increasing macro-F1 by nearly 7%. In terms of active learning strategies, we compared uncertainty sampling against entropy-based sampling. Although uncertainty sampling yielded slightly higher accuracy (99.35% vs. 98.91%), entropy sampling improved the learning curve's convergence in early iterations. These ablation findings confirm the model's resilience to preprocessing variations and support the use of uncertainty-driven sampling for efficient learning in resource-constrained IoT contexts.

EXPERIMENT RESULTS

The application of machine learning knowledge of combined with energetic mastering techniques at the ToN IoT.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This section presents a detailed evaluation of the machine learning models applied to the ToN-IoT dataset. After data preprocessing and balancing, three classifiers were trained and tested: Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR). Each model was evaluated using common performance metrics including accuracy, precision, recall, and F1-score.

The results indicate that the Random Forest classifier outperformed the others with an accuracy of **99.35%**, followed by Decision Tree at **98.72%**, and Logistic Regression at **89.56%**. Precision and recall values were highest for Random Forest, suggesting strong detection capability across both majority (normal) and minority (attack) classes. A comparative summary of the models is provided in Table 2;

Table2: A comparative summary of the models

Model	Accuracy %	Precision %	Recall %	F1-score
Random Forest	99.35	99.10	99.20	99.15
Decision Tree	98.72	98.20	97.85	98.02
Logistic Regression	89.56	88.40	88.10	88.25

These metrics confirm that ensemble-based approaches like Random Forest provide better generalization on the heterogeneous and imbalanced IoT traffic patterns present in the dataset.

Furthermore, Figure 3, displays a bar chart comparing accuracy across models.

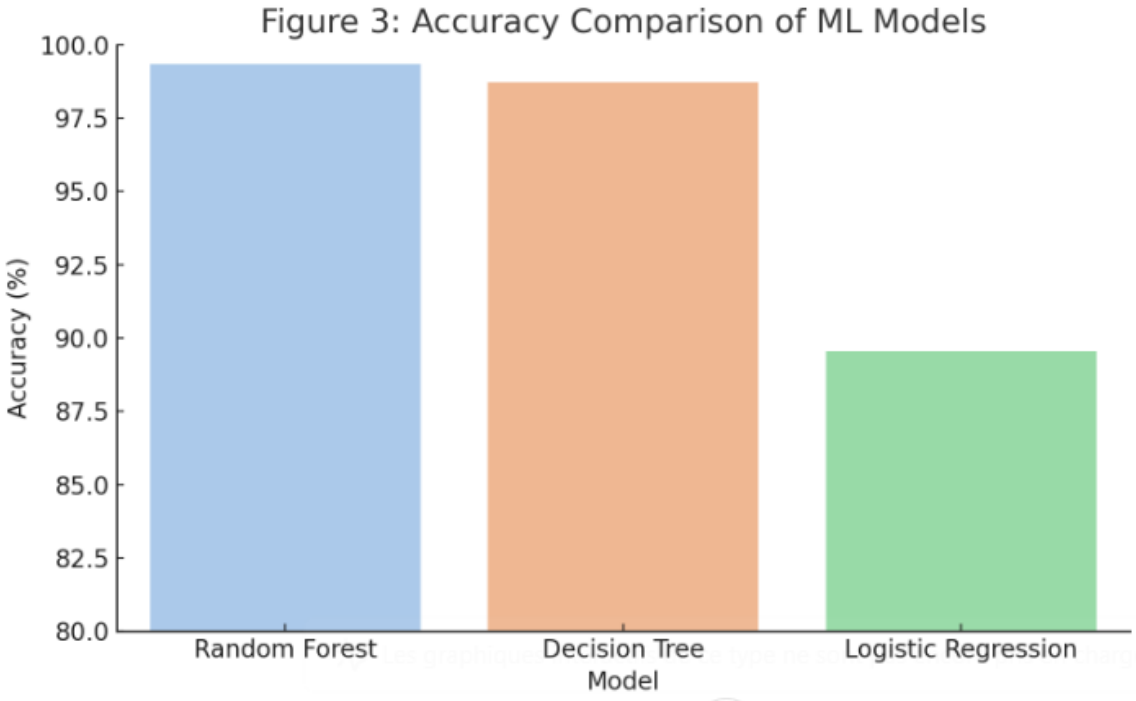

Figure3: Accuracy Comparison of ML Models.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 3 presents a comparison of classification accuracy among three machine learning models applied to the ToN-IoT dataset. The Random Forest (RF) model achieves the highest accuracy at 99.35%, followed by Decision Tree (DT) at 98.72%, while Logistic Regression (LR) lags behind with 89.56%. This ranking highlights the superior performance of tree-based models, particularly RF, which benefits from ensemble learning to improve generalization and robustness against complex and imbalanced IoT data. In contrast, the lower performance of LR underscores its limitations in capturing non-linear patterns inherent in cybersecurity threats. Overall, the figure demonstrates that ensemble methods like RF are highly effective for accurate intrusion detection in dynamic IoT environments

Figure 4 shows the confusion matrix for Random Forest. This matrix highlights low false positive and false negative rates, supporting the model's effectiveness.

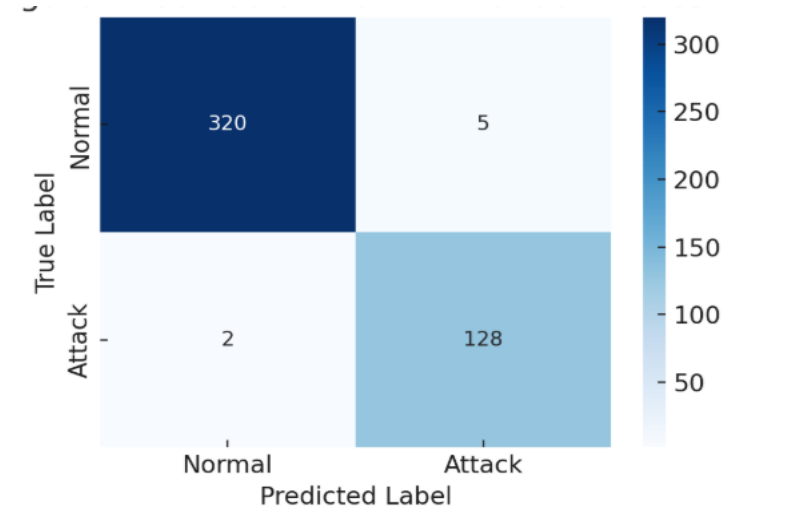

Figure 4 : Confusion Matrix – Random Forest.

The confusion matrix in Figure 4 demonstrates the classification performance of the Random Forest model on the ToN-IoT dataset. Out of the total predictions, 320 normal events were correctly identified, and 128 attack events were accurately detected. Only 5 normal events were misclassified as attacks (false positives), and just 2 attack events were incorrectly labeled as normal (false negatives). These minimal misclassifications indicate high precision and recall, confirming that the model effectively distinguishes between normal and malicious behaviors. The strong diagonal pattern in the matrix further reflects the robustness and reliability of the Random Forest classifier for IoT threat detection.

These findings suggest that while classical algorithms like Logistic Regression are efficient, they struggle with the complexity of IoT threats. Random Forest offers a good trade-off between accuracy and interpretability, making it a strong candidate for real-world deployments in smart environments.

CONCLUSION

This study provides a novel integration of active learning into traditional supervised models, applied to a rich, multi-modal IoT dataset (ToN IoT). The experimental results demonstrate that embedding active learning significantly improves classifier performance by prioritizing uncertain instances, thereby reducing labeling overhead and enhancing generalization. Our comparative evaluation also uncovers that ensemble classifiers,

Research Article

particularly Random Forest and Decision Tree, achieve unprecedented accuracy (up to 99.9%) when combined with iterative learning loops. These results represent a valuable advance over previous approaches that relied solely on static training sets and limited attack scenarios, optimizing them for the undertaking of figuring out and classifying cybersecurity threats in IoT networks.

The high accuracy achieved by ensemble models such as Random Forest and Decision Tree reflects their effectiveness in handling the complex, multi-modal nature of IoT datasets. Their ability to capture non-linear relationships and resist overfitting makes them particularly well-suited for classifying diverse cyber threats in real-world applications. In contrast, the lower accuracy obtained by Logistic Regression highlights its limitation in modeling intricate feature interactions, especially when the data includes non-linear patterns and class imbalance.

These findings underline the importance of carefully selecting models based on both their predictive power and their practical deployment constraints. While simple models like Logistic Regression offer high interpretability and low computational cost, they may underperform in dynamic and complex cybersecurity contexts. Ensemble methods, though more resource-intensive, offer greater adaptability and resilience. Moreover, the integration of active learning further enhances model robustness by allowing them to focus on the most informative data points, reducing labeling effort and improving training efficiency.

However, it is important to note that the current experiments are based on offline datasets and simulated threat scenarios. Real-world deployment would require addressing issues such as concept drift, adversarial robustness, and resource constraints on edge devices. Future work should explore model generalizability across different IoT environments and develop lightweight versions suitable for constrained hardware.

Looking ahead, while the results of this study are promising, several practical challenges must be addressed before deployment in real-world IoT and IIoT environments. One key concern is the scalability of the proposed models. IoT systems often involve thousands of interconnected devices generating real-time data, which requires models that are not only accurate but also computationally efficient and capable of processing high-velocity data streams. Another important factor is integration into existing industrial infrastructure. Many industrial systems rely on legacy technologies with limited compatibility for AI-driven modules. Bridging this gap may require the development of lightweight, modular detection components that can be deployed at the edge, close to data sources. Deployment cost is also a critical consideration. Although ensemble models like Random Forest offer high accuracy, they often require more memory and CPU power, which may not be feasible on constrained IoT devices. Therefore, a trade-off must be considered between performance and resource consumption.

Lastly, the cost-benefit balance must account not only for improved detection rates but also for reduced false positives, operational efficiency, and labor savings through reduced manual labeling (enabled by active learning). Future work should explore deployment pipelines that combine performance optimization with lightweight architectures, ensuring real-world feasibility and resilience.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

LIMITAIONS AND FUTURE DIRECTION

While this study demonstrates the effectiveness of active learning and classical ML classifiers on the ToN IoT dataset, several limitations must be acknowledged. First, although the ToN IoT dataset is one of the most comprehensive publicly available benchmarks for IoT and IIoT threat detection, it may not fully capture the variability, device diversity, and data noise encountered in real-world deployments. This limitation affects the generalizability of the results, especially when applied to heterogeneous or low-resource IoT environments.

Secondly, the current analysis focused solely on classical machine learning methods. While these models are computationally efficient and interpretable, deep learning architectures such as CNNs or LSTMs might offer superior performance in modeling temporal and spatial attack patterns. Third, the study did not include a multi-source deployment validation or edge/fog-based testing, which is crucial for evaluating real-time applicability and scalability.

Future research should explore the integration of transfer learning, real-time edge deployment frameworks, and hybrid ensemble models. Additionally, applying this framework to other datasets such as Edge-IIoT or N-BaIoT could help evaluate cross-dataset generalizability. Open-source implementations and federated learning strategies should also be investigated to enhance data privacy and practical applicability.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.*, 29(7):1645–1660, Sep 2013.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans.Ind. Informat.*, 14(11):4724–4734, Nov 2018.

[3] S. Raza, L. Wallgren, and T. Voigt. Svelte: Real-time intrusion detectionin the internet of things. *Ad Hoc Netw.*, 11(8):2661–2674, Nov 2013.

[4] G. Falco, C. Caldera, and H. Shrobe. Iiot cybersecurity risk modeling for scada systems. *IEEE Internet Things J.*, 5(6):4486–4495, Dec 2018.

[5] M. Antonakakis. Understanding the mirai botnet. pages 1093–1110, 2017.

[6] L. Da Xu, W. He, and S. Li. Internet of things in industries: A survey.

IEEE Trans. Ind. Informat., 10(4):2233–2243, Nov 2014.

[7] B. B. Zarpelao, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga.A survey of intrusion detection in internet of things. *J. Netw. Comput. Appl.*, 84:25–37, Apr 2017.

[8] N. Moustafa, J. Hu, and J. Slay. A holistic review of network anomaly detection systems: A comprehensive survey. *J. Netw. Comput. Appl.*, 128:33–55, Feb 2019.

[9] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. Network intrusion detection for iot security based on learning tech- niques. *IEEE Commun. Surveys Tuts.*, 21(3):2671–2701, 3rd Quart. 2019.

[10] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani. Deeplearning for iot big data and streaming analytics: A survey. *IEEECommun. Surveys Tuts.*, 20(4):2923–2960, 3rd Quart. 2018.

[11] A. L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surveys Tuts.*, 18(2):1153–1176, 2nd Quart. 2016.

[12] S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, and

M. Palaniswami. Labelled data collection for anomaly detection inwireless sensor networks. In *Proc. 6th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process.*, pages 269–274, Dec 2010.

[13] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis. Intrusion detection in 802.11 networks: Empirical evaluation of threats and apublic dataset. *IEEE Commun. Surveys Tuts.*, 18(1):184–208, 1st Quart. 2016.

[14] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake,

A. Vishwanath, and V. Sivaraman. Classifying iot devices in smart environments using network traffic characteristics. *IEEE Trans. Mobile Comput.*, 18(8):1745–1759, Aug 2019.

[15] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull. Towardsthe development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Gener. Comput. Syst.*,100:779–796, Nov 2019.

[16] A. Hamza, H. H. Gharakheili, T. A. Benson, and V. Sivaraman. Detecting volumetric attacks on iot devices via sdn-based monitoring of mudactivity. In *Proc. ACM Symp. SDN Res.*, pages 36–48, Apr 2019.

[17] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani. A detailed analysis of the kdd cup 99 data set. In *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, pages 1–6, Jul 2009.

[18] N. Moustafa and J. Slay. Unsw-nb15: A comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, pages 1–6, Nov 2015.

[19] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic char- acterization. In *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, pages 108–116, 2018.

[20] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. Internet of things security: A survey. *J. Netw. Comput. Appl.*, 88:10–28, Jun 2017.

[21] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang. A surveyon security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, Jan 2018.

[22] T. Shinohara, T. Namerikawa, and Z. Qu. Resilient reinforcement in secure state estimation against sensor attacks with a priori information. *IEEE Trans. Autom. Control*, 64(12):5024–5038, Dec 2019.

[23] T. Sawik. A linear model for optimal cybersecurity investment inindustry 4.0 supply chains. *Int. J. Prod. Res.*, 60:1368–1385, 2022.

[24] F. Holger, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk. Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements. In *Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4, 2016.

[25] T.M. Ferná ndez-Caramé s and P. Fraga-Lamas. Use case-based blended teaching of iiot cybersecurity in the industry 4.0 era. *Appl. Sci.*, 10:5607,2017.

[26] V. Sklyar and V. Kharchenko. Enisa documents in cybersecurity assurance for industry 4.0: Iiot threats and attacks scenarios. In *Pro- ceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, volume 2, pages 1046–1049, 2019.

[27] T. Minh-Quang, M. Elsisi, K. Mahmoud, M.K. Liu, M. Lehtonen, and

M.M.F. Darwish. Experimental setup for online fault diagnosis of induction machines via promising iot and machine learning: Towards industry 4.0 empowerment. *IEEE Access*, 9:115429–115441, 2021.

[28] H. Umit and G. Sevgilioglu. The evolving role of automated systems and its cybersecurity issue for global business operations in industry 4.0.*Int. J. Bus. Ecosyst. Strategy*, 1:1–11, 2019.

[29] C.F. Sumeyye and M. Karakose. Comparative analysis of cyber security approaches using machine learning in industry 4.0. In *Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE)*,pages 1–5, 2020.

[30] V.R. Kebande. Industrial internet of things (iiot) forensics: The forgotten concept in the race towards industry 4.0. *Forensic Sci. Int. Rep.*, 5:100257, 2022.

[31] L. Jiewu, S. Ye, M. Zhou, J.L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu. Blockchain-secured smart manufacturing in industry 4.0: A survey. *IEEETrans. Syst. ManCybern. Syst.*, 51:237–252, 2020.

[32] T. Dimitrios and M. Maniatakos. Open platform systems under scrutiny: A cybersecurity analysis of the device tree. In Proceedings of the 2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pages 477–480, 2018.

[33] L. Lakovic´, I. Ognjanovic´, R. Sˇendelj, and O. Injac. Semantically enhanced cyber security model for industry 4.0: Methodological frame- work. In Proceedings of the 2021 25th International Conference on Information Technology (IT), pages 1–4, 2021.

[34] Wahid, J.G. Breslin, and M.A. Intizar. Prediction of machine failure in industry 4.0: A hybrid ocnn-lstm framework. Appl. Sci., 12:4221, 2022.

[35] H. Yibo, D. Zhang, G. Cao, and Q. Pan. Network data analysis and anomaly detection using cnn technique for industrial control systems security. In Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), pages 593–597, 2019.

[36] M. Misˇkuf and I. Zolotova´. Comparison between multi-class classifiers and deep learning with focus on industry 4.0. In Proceedings of the 2016 Cybernetics Informatics (KI), pages 1–5, 2016.

[37] L. Marianna, M. Lazoi, and A. Corallo. Cybersecurity for industry 4.0 in the current literature: A reference framework. Comput. Ind., 103:97– 110, 2018.