Scientific Research Publishing

Advances in Internet of Things, 2025, 15(2), 17-32
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Use of Machine Learning and Deep Learning in Intrusion Detection for IoT

Muhannad Almohaimeed[1*], Rasha Alyoubi[1], Afnan Aljohani[1], Mashael Alhaidari[1], Faisal Albalwy[2], Fahad Ghabban[1], Ibrahim Alfadli[1], Omair Ameerbakhsh[1]

[1]Department of Information Systems, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
[2]Department of Cybersecurity, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
Email: *mmohimeed@taibahu.edu.sa

How to cite this paper: Almohaimeed, M., Alyoubi, R., Aljohani, A., Alhaidari, M., Albalwy, F., Ghabban, F., Alfadli, I. and Ameerbakhsh, O. (2025) Use of Machine Learning and Deep Learning in Intrusion Detection for IoT. *Advances in Internet of Things*, **15**, 17-32.
https://doi.org/10.4236/ait.2025.152002

Received: February 24, 2025
Accepted: March 29, 2025
Published: April 1, 2025

Abstract

The ever-increasing use of IoT devices has presented new security threats and, thus, requires IDS to protect interconnected IoT networks. This paper identifies the use of ML and DL as a new effective way of improving protection against cyber threats in IoT networks. This review aims to review the most up-to-date research on ML and DL techniques for IoT-based IDS concerning responding to new threats like zero-day attacks and Distributed Denial of Service (DDoS). Thus, the review uses twenty cognate peer-reviewed studies published between 2023 and 2024 to emphasize the methodological variability, datasets, as well as the forms of performance metrics present in the field. The outcomes show that four modern frameworks, including hybrid models, federated learning, LSTMs, and convolutional architectures, perform much better than conventional methods in terms of accuracy, detection rates, and false-positive rates. For example, models such as feature selection employing new paradigms like the inclusion of new features in the suite, cost-sensitive learning, as well as multitask paradigms show better scalability and flexibility to handle imbalanced datasets as well as cyber-attacks of other unseen types. Also, the incorporation of IDS with energy-efficient protocols and fog computing more real-time capability of such systems within IoT-constrained resources network. However, a number of limitations including computational complexity, privacy issues, and lack of a proper baseline for model comparison remain major ongoing issues. Overall, this review consolidates important ideas about the advantages and weaknesses of current methods together with directions for further investigation such as the practices of federated deep learning, adaptive algorithms, and real-time anomaly detection frameworks. In conclusion, this paper establishes the importance of ML and DL in enhancing the robustness of IoT systems to the increasing ecosystem of cybersecurity threats.

Keywords

Machine Learning, Deep Learning, Intrusion Detection, IoT Security, Cybersecurity, IDS

1. Introduction

The Internet of Things has become a rapidly growing phenomenon in the last few years where billions of devices across domains including health, transport, industries, smart cities, and numerous others. This exponential growth has brought change into daily life and made data exchange and automation much easier, but it also became a major security risk. By their very nature, IoT systems are complex and expose interconnected devices to any number of cyber threats, such as DDoS attacks on webcams, data breaches through connected home appliances, and even the newly discovered "zero-day vulnerability". This has been seen as an essential reason why Intrusion Detection Systems (IDS) have been adopted as core requisite for IoT Networks to protect against these threats [1]. This is because IDSs can pay constant attention to the traffic flowing in the networks, and hence keep alerting users to possible malicious actions, to the devices and or the whole network ecosystem. Still, such solutions fail to function efficiently when used in IoT networks because of its highly dynamic and impoverished nature. This torments them with the high number of IoT devices and the great variety of the produced data, as well as the dynamically changing threat landscape. To overcome these limitations the use of Machine Learning (ML) and Deep Learning (DL) techniques holds the key solutions. The ML and DL can model complex data patterns, update themselves for detecting newer forms of attack and can improve detection rates. Some of the methodologies used include convolutional neural networks, long short-term memory networks, and ensemble learning models, which possess the competency to classify the anomaly and cyber threats in IoT networks [2]. **Figure 1** shows the architecture of an Intrusion Detection System (IDS), highlighting its components and functionality.

Nevertheless, there are crucial security issues that IoT-based IDSs are still challenged by. Standard static ML and DL techniques are limited in detecting low-frequency intrusions, work inefficiently with imbalanced datasets, and do not recognize previously unknown or zero-day threats. However, applying these techniques in the low-power IoT settings requires additional optimization calculations, which entails other problems like computational complexity and scalability. These limitations explain why there is a need for better IDS techniques, enhanced IDS approaches, and better fitting IoT network IDS systems. The objectives of the study are:

- To address the above challenges, this review seeks to assess the use of ML and DL in IoT-based IDSs. The key objectives include:
- Evaluating the enhancement aspect of using ML and DL in the identification

of cyberattacks in IoT networks.

• Determining which classical ML and DL techniques can be used to counter new forms of threats, including zero-day attack.

• Reviewing the security performance measure of these techniques by means of metrics like accuracy, precision, recall, False Positive Rate and others.

• An analysis of the weaknesses and drawbacks of using ML and DL IDS in recognizing anomalies in IoT networks.

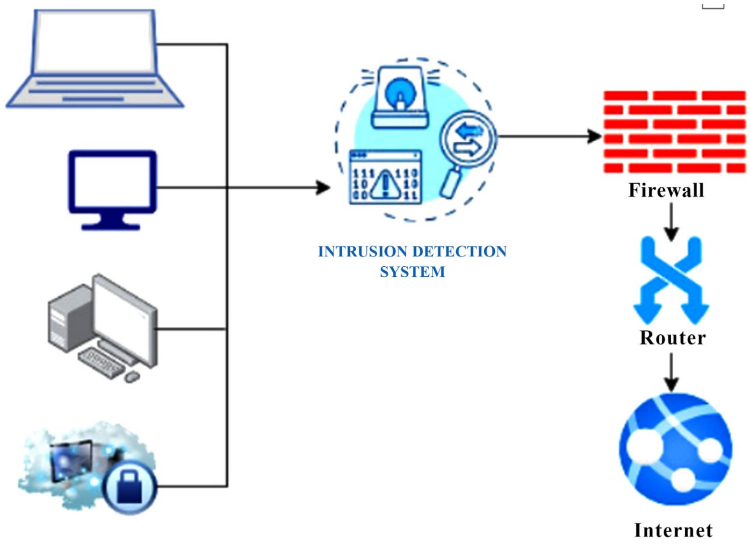

Figure 1. Intrusion detection system.

This review is limited to reviewing survey articles that present results between 2023 and 2024 using ML and DL methodologies in IoT-based IDSs. The eligibility criteria focus on reporting exact performance figures like accuracy, detection rates, false positives among other related indices; and articles which are review articles as well as studies that are out of scope of IoT are excluded from comparison. Therefore, this review aims at reviewing the existing studies to give the reader a clear picture of the state of research done on this subject, highlighting the areas that have not been covered enough by earlier approaches, and explore the possible areas of future research. Thus, this review will help to suggest better, and more effective IDS to improve security IoT networks in the world, where such connections are becoming increasingly widespread.

2. Methods

2.1. Eligibility Criteria

To ensure a focused and reliable analysis, specific inclusion and exclusion criteria were established for this review.

2.1.1. Inclusion Criteria

• **Relevance to IoT-Based IDS:** Works that propose the use of ML/DL as the basis of IDSs for IoT.

• **Security Metrics:** Analytical research that contains concrete performance characteristics assessment, including accuracy, precision, recall, F1Score, false positive rates, and detection rates.

• **Recency**: Journal recommended for papers published between the year 2023 - 2024, in order to capture the latest inventions and discoveries on the subject.

• **Publication Type**: This approach was adopted to bring scientific quality by inclining more on articles in peer reviewed journals and conference proceedings.

• **Language and Accessibility:** These comprise of studies in full text and in the English language.

2.1.2. Exclusion Criteria

• **Non-IoT Context**: Research works that encompass traditional intrusion detection systems in general without special consideration to IoT.

• **Review Articles:** To avoid replicative studies which have been a common issue in systematic reviews, meta-analysis or review papers were not included.

• **No Performance Metrics**: Articles that included only non-quantitative measurement variables or that did not have some sort of empirical support were not considered.

• **Non-Peer-Reviewed Sources:** Review articles, case reports, letters to the editor, commentaries, and other nonoriginal publications were excluded.

• **Older Studies:** Some are published before the year 2023 since findings and trends might not encompass the current advanced trends in ML/DL and IoT.

Such strict eligibility criteria provided for the inclusion of the most relevant and high-quality research that can shed the light on the efficiency of ML and DL in IoT-based IDS.

2.2. Search Strategy

The first approach of the search strategy was to ensure efficiency in the search and capture of the articles. Multiple academic databases were utilized to retrieve high-quality studies:

Databases Searched

• **IEEE Xplore:** One of the premier sources of information in technology-related studies.

• **ACM Digital Library**: Offers a broad spectrum of computing and information technology and related disciplines.

• **ScienceDirect:** Provides scholarly journals in all fields of science, including computer engineering and information assurance.

• **Google Scholar:** To optimize the search and guarantee that the latest and varied articles were included, supplement searches were made.

• **Search Terms/Keywords:** Keywords were defined to include potential different forms of artificial intelligence, which include ML, DL, and IDS based on IoT. Various terms were employed with Boolean operators and keyword networks for efficient search. Examples include:

○ (("machine learning" OR "ml") AND ("deep learning" OR "dl")) AND (("intrusion detection" OR "ids") AND ("IoT" OR "Internet of Things"))

○ (("cybersecurity" + "network security") (("anomaly detection" + "threat detection") AND ("IoT networks"))

○ ((Neural Networks OR Federated Learning) AND (IoT Devices) AND (Security Metrics))

• **Timeframe of Search**: To pursue the recent development in the field, the search was performed to identify the articles published between January 2023 and December 2024.

2.3. Study Selection Process

The study selection process was conducted in multiple stages to ensure only the most relevant and high-quality studies were included:

1. Title and Abstract Screening

○ The titles and abstracts of articles for potential inclusion in the study were initially filtered using the results of the database searches.

○ The relevance of objects associated with IoT, ML/DL techniques, and intrusion detection was evaluated by two independent reviewers according to the source type of each study. Any divergent cases were discussed with the second or the third assessor to determine the final decision.

2. Full-Text Review

○ Full-text review was applied to the articles that passed through title and abstract screening.

○ Hence only data that satisfied all the criteria regarding inclusion, for example, performance measures and IoT relevant use case scenarios were used in the final study data set.

3. Study Inclusion

○ The identified studies were screened, and, where necessary, overlapping was eliminated, and doubtful cases were discussed among the reviewers.

Data Extraction

Since data extraction centered on the key objectives of the study, it aimed at capturing the necessary information for answering the research questions exhaustively. The extracted data included:

1. Study Details

○ Author, year, title, source, country of origin.

2. Techniques Used

○ Techniques used in the current work include not only the general methods of the ML and DL but also the concrete Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and Federated Learning.

3. Datasets

○ The CICIDS2017 dataset has been used in the three similar studies labelled as bot-IoT, ToN-IoT, and the four synthetic datasets.

4. Performance Metrics

○ Other forms of measurement include accuracy, precision, recall, F1-score, the rate of detection, the rate of false positive and AUC score.

5. Challenges and Limitations

○ Issues that have been raised include; scalability, computation, unbalanced data sets, or privacy.

The data was managed systematically with the help of Covidence, which is software used for systematic reviews to minimize errors during the extraction and synthesis of data.

3. Literature Review

This review consists of 20 state-of-the-art articles with a publication date range from 2023 to 2024 proposing ML and DL methods for IoT-based IDS. These articles include research from various locations and are derived from reputable academic journals and conference proceedings to provide a comprehensive assessment of the developments in this dynamically growing area.

The research from Elsayed *et al.* presents a hybrid IDS that employs hierarchical deep learning to defend clustered IoT environments and it uses datasets such as ToN-IoT and InSDN and has been published in the Journal of Sensor and Actuator Networks. This paper proposes a system called SATIDS, that improves feature selection using the Minimum Redundancy Maximum Relevance (MRMR) method, and the Long Short Term Memory (LSTM) networks for optimized detection rate for clustered IoT systems. The proposed framework, *i.e.* SATIDS, performs well with the ToN-IoT and InSDN datasets and shows an accuracy of 97.5%, precision of 98.4%, and F1-score of 98.05% on ToN-IoT and precision of 99%, detection rate of 99.6%, and F1-score of 99.3% on InSDN. IoT cyber threats like DDoS, ransomware, injection, and backdoor attacks were tested and it was observed that this system can classify malicious as well as normal traffic efficiently. Nevertheless, issues like computational load and restricted LSTM training to deep networks, and system scale in real-world applications, and dataset constraints like imbalanced features and the number of attack samples were mentioned as limitations [3].

The study by Telikani *et al.* introduces a hybrid Machine Learning (ML) framework called CostDeep IoT, designed to address two major challenges in IoT intrusion detection: The problem of class imbalance and the problem of detecting unknown attacks. A SAE, for feature learning tasks, and a multitask SVM, for classification tasks are used in the model. This approach incorporated cost-sensitive learning approaches to making the hinge loss function more resilient to minimal intrusion volumes. The proposed framework of the work produced better accuracy on UNSW-NB15 and BoT-Iot datasets with precision, recall and F1-scores of 96.8%, 88.8%, 92.8% respectively for UNSW-NB15 and 95.7%, 96.8%, 95.6% respectively for BoT-Iot. The model was able to identify several forms of IoT-specific cyber threats such as DDoS, reconnaissance, and theft further incor-

porating the ability to identify new types of attacks that were not encountered in its training. But, there are still a few problem areas, namely computational costs arising out of multitask learning, and real-time, large scale IoT network deployment for which optimization is still in development phase [4].

In the recent study conducted by Bhavsar *et al*. the authors have suggested designing an IDS based on an anomaly detecting method which employs a PCC and a CNN in order to protect IP applications against cyber threats. The PCC-CNN combines feature selection based on Pearson Correlation Coefficient and classification by a convolutional neural network implemented on the binary as well as on the multiclass classification approaches. The work's performance assessment through three sets of data (NSL-KDD, CICIDS-2017, and IOTID20) resulted in high accuracy for binary classification at 99% and multiclass at between 97% - 99% in addition to a low false alarm rate of 0.01. The system helped in identifying Distributed Denial of Service (DDoS), botnets and spoofing and port scans. Some limitations were observed including mismatched distribution of the datasets, high computational costs especially in multi-class classification cases which affected uniformity [5].

The work by Panthakkan *et al*. compares the six ML algorithms in intrusion detection on the IoT systems using the UNSW-NB15 dataset. These algorithms include Log linear models, k-nearest neighbors, the decision tree, random forest, boosting, and XGBoost and the results pointed to random forest as the most efficient model. Nonetheless, metrics established that Random Forest provides the best accuracy of 95.12%, a high precision of 96.26%, and F1-score of 96.17% proving that the Random Forest algorithm offers excellent performance in identifying IoT-centric attacks. Identified threats are DoS, probing attacks, and attempts at exploitation proving the versatility of the model to various categories of attacks. Some of its limitations are also acknowledged including the unavailability for coping up with multiclass classification and computational issues in real-time huge IoT networks and hence need to grow up to the complete attack possibilities [6].

The research work by Khan *et al*. puts forward IDS employing a combination of LSTM and CNN technologies to strengthen IoT protection in the disaster response process. Finally, the developed system was tested and compared with other methods of literatures on CICIDS2017 and IoTID20 datasets and achieved the accuracy of 97.36% and 99.73% respectively. Optimized in Precision, recall and F1-score metrics achieved better results than compared to traditional methods such as LDA, QDA and SVM. The model accurately captured all common types of cyber threats including DDoS, brute force, and botnet attacks through deep feature extraction, and pattern recognition. However, some issues like the increased computational load at the cloud side and handling diverse data from the IoT environment were pointed out, which needed to be fine-tuned for the real-time application of disaster scenarios [7].

The work by Radjaa *et al*. presents an FDL-IDS model oriented to improve the privacy and the efficiency in Fog-IoT networks. The system employs Long Short-

Term Memory (LSTM) networks under the framework of federated learning so that edge devices can train models while sharing the raw data, which pose the risk of privacy violation. The performance of the proposed model was also tested with the BoT-IoT dataset where it has shown detection accuracy of 99.47%, precision of 99.66% and very low false positive rate of 0.35% and false negative rate of 0.17%. It was possible to detect Distributed Denial of Service (DDoS), reconnaissance and many other botnet related attack in the decentralized approach. However, some drawbacks like increased fog nodes' computation time, gobal IID assumption which is a major assumption of most of the paradigms considered in the reviewed work as well as scalability when addressing large-scale IoT networks were identified as future research directions [8].

Ennaji *et al*. proposed a Federated Deep Learning (FDL) model for applying intrusion detection in IoT to minimize data centralization and protect the privacy of information. The model utilises a Deep Neural Network (DNN) as a model architecture, allied with the Edge-IIoTset dataset, which consists of data from IoT devices as well as multiple attacks. Analyzing the results of the assessment, the following key measures were achieved: With regards to performance measures, it was found that accuracy is equal to 90% while precision is 95.19%, and recall is 89.89%; Thus, proposed system achieved F1-score of 89.20% to detect multiple IoT-related threats in a balanced and efficient manner. These included Distributed Denial of Service (DDoS), injection, malware and man-in-the-middle. Notable difficulties mentioned are the high computational complexity of federated learning in cases with non-IID data and limited scalability potential in large volume IoT networks [9].

Walling and Lodh, suggest an AN-SFS that is an adaptive feature selection technique that can be used to enhance the IDS in IoT. To apply AN-SFS, it uses Random Forest (RF) classification since it focuses on feature interdependence and localization of certain statistics as input for dynamic attribute subset selection. The model was tested using NSL-KDD and UNSW-NB15 datasets resulting in accuracy of 99.3% and 97.5% respectively with high value of precision, recall, and F1 score for different attack types. They managed to identify different forms of threats including the DoS, R2L, U2R, and probing. Drawbacks consist of computational overload when it comes to dynamic changing of threshold value and the fact that it cannot be effectively extended to real-time large-scale IoT network application that requires further enhancement [10].

The study by Francis *et al*. applies a new approach of a two-tier convolutional deep learning model (2TCDLM) to detect intrusion in IoT networks. The system also uses a Self-Adaptive Osprey Optimization Algorithm (SA-OOA) which improves the activation function of the model. The approach involves the employment of statistical and flow feature extraction techniques with the CICIDS 2018 dataset. Details of the evaluation of the proposed model were as follows; accuracy = 99.74%, FPR = 0.019, MCC = 0.97; the proposed model performed better than the CNN, GRU, Bi-LSTM, and LSTM models. It effectively identified several types

of cyber threats such as DDoS attacks, brute force, and port scan. Nevertheless, potential issues concerning the computational burden and the practical applicability in expansive IoT networks have been pointed out, which deserve further study to optimize the real-time implementation [11].

The paper by Divakarla and Chandrasekaran, assesses the effectiveness of the supervised machine learning methods such as Decision Tree (DT) Random Forest (RF) Support vector machine (SVM), K-Nearest Neighbor (KNN), and Artificial neural network (ANN) in analysis of the anomaly based intrusion detection in IoT networks. The system used specialized data comprising of 357,952 samples and focused on a total of eight different types of attack; DoS, data probing, Malicious control, and configuration attack. Evaluation results indicated that KNN obtained the highest accuracy of 99.47% with RF following at 99.40% with additional high values of precision and recall. The study acknowledged that the anomaly detection tasks were well managed using these models but pointed at some gaps such as the scalability problem for real IoT applications and the need for improvement to accommodate large, discordant datasets [12].

Sharma & Babbar, work focuses on proposing an ML framework for intrusion detection in IoT networks using NB, DT, KNN, and LR. A comparison of this Decision Tree model against other techniques by using an open-access Network Intrusion Detection dataset (NID) showed that it outperforms other models with the highest accuracy of 99.47%, followed by KNN at 99.16%; Naive Bayes and Logistic Regression had accuracies of 90.68% and 95.55% respectively. It efficiently recognized several comprehensive cyber threats peculiar to IoT, such as DDoS, data leakage, and spoofing attacks. However, the following limitations were realized during the study: Data imbalance about the IoT devices, scalability for large-scale IoT networks, and high computational overhead during feature selection and preprocessing Owing to these challenges, further enhancement is required for the actual implementation in real-life applications [13].

In the research work carried out by Wadate and Deshpande, an intrusions detection system using a feed-forward neural network (FNN) was designed for Internet of Things (IoT) networks. The system applies a newly published dataset of IoT, which represents both real and synthetic IoT traffic, to assess its binary and multiclass classification accuracy. This result is on the FNN model that was developed, and optimized using Adam with tuned hyperparameters that performed a 99.7% accuracy rate across the precision, recall, and F1-score metrics and concludes the effectiveness of the model to detect Distributed Denial of Service (DDoS), reconnaissance attacks, data theft and surveillance invasions. However, the research also lists drawbacks like high computationally intensive training and pre-processing of big data, as well as inadequate presentation of this model in resource-limited IoT devices [14].

In the work of Diallo *et al*., a three-tier IDS solution for IoT networks is developed with deep learning employing autoencoders and an MLP. The first tier utilizes an autoencoder for anomaly identification, the second tier utilizes an auto-

encoder to classify abstracted traffic as either known or unknown attacks, and the third tier implements the MLP for the classification of known attack types. The evaluation was conducted with a benchmark MQTTSet dataset; the accuracy that was established was 99 percent, 99.6 percent, and hundred percent at the respective levels. The IDS can periodically identify several different types of attacks such as DoS, MQTT Publish Flood, SlowITe, bad data, and brute force. However, some limitations in the work include the following: imbalance in the dataset as the data majority belongs to legitimate data, greater than 98%, and scalability for large IoT networks [15]. As shown in **Figure 2**, the proposed three-tier framework effectively categorizes the intrusion detection process in IoT networks.

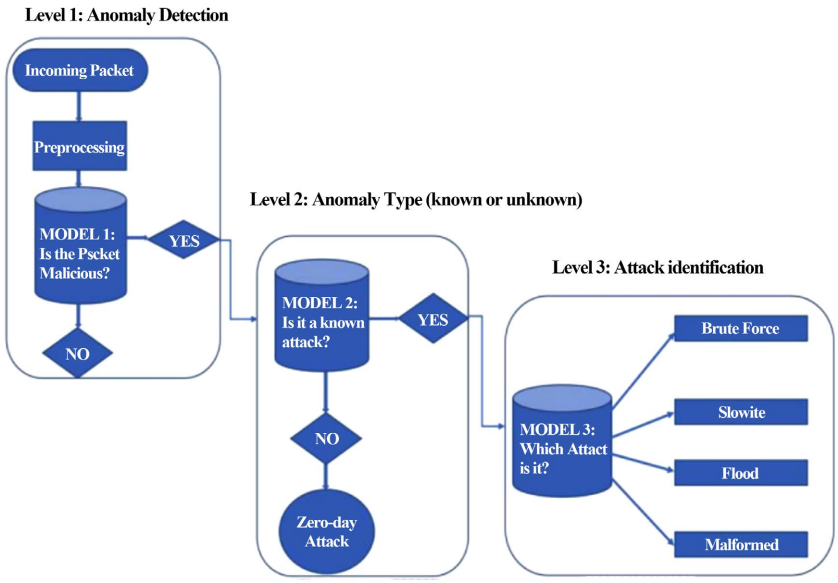

Figure 2. Overview of three-tier proposed framework.

The paper by Tong and Zhang presents a new intrusion detection system for IoT networks: IResTAE2A based on deep learning that uses improved residual TCNs with AAEs. This model employs both supervised and self-supervised learning techniques for improving feature learning and it does not involve labeled data. The system itself proved to possess a high accuracy across the datasets ranging from 99.96% in the case of CIC-IDS2018 and 99.97% in the case of CIC-IDS2017 in terms of accuracy to detect various kinds of attacks such as DoS, DDoS, infiltration, and web attacks. Nevertheless, issues like a higher computation cost which prevents real-time application, the necessity to determine an adequate threshold value, and data heterogeneity as a problem were discussed [16].

Kumar and Dubey introduced a paper that discusses a comprehensive analysis of using deep learning for network intrusion enhancement for IoT devices with CNN, LSTM, and GRU models. The models were trained and tested on the dataset called Bot-IoT for which classification of network traffic into normal and malicious traffic is considered. Among the evaluated models, LSTM revealed the highest performance with an accuracy of 99.8%, the precision of 99.7%, recall and F-

measure both 100% and CNN along with GRU performed slightly lower with an accuracy of 99.7% and 99.6% respectively. Overall, these models were found to be efficient in identifying different IoT-specific threats such as DoS, DDoS, botnet, and spoofing. Nevertheless, this work found that there are some limitations: for instance, there is usually a lot of computation time required during the training of the model, and feature extraction is a crucial aspect that must be done effectively during the pre-processing phase. Nonetheless, issues of scalability of Deep Reinforcement learning over real-time in resource-challenged IoT domain are still relevant and constitute limitations in future improvement [17].

The research of Hinojosa and Majd presents the 1D-CNN and BiLSTM-CNN models for network intrusion detection in IoT contexts using the CICIoT2023 dataset. These models categorize traffic as normal or one of seven attack types ranging from Distributed Denial of Service (DDoS) to Denial of Service (DoS), Mirai, Impersonation, Discovery, Forceful, and Web. The 1D-CNN model with an F1-score of 93.8% was slightly improved by the BiLSTM-CNN with an F1-score of 93.82% but at a cost of high computational time. The models achieved a high per-class precision and recall for dominant attack types such as DDoS, DoS, and Mirai, but were slightly less effective for less frequent types. The main difficulties are associated with the high-class imbalance in the dataset and computational complexity for real-time use. To overcome these problems, data preprocessing methods including random under-sampling, class weighting, and feature scaling were considered during the current study [18].

The research work of Chauhan *et al*. compares the results of several supervised machine learning techniques such as RF, DT, as well as SVC in detecting intrusion in IoT networks. Applying the case of CICIDS2017, the work considers binary and multi-class classification results. The testing accuracy for the RF model came to 99.66% along with both a weighted average precision and recall of 96%. DT model was followed as Testing accuracy = 95.71% as that of SVC = Testing accuracy = 95.62%. The study was also able to identify threats including DDoS, brute force, and botnet attacks. However, issues such as handling data imbalance and invoking computation tractability for practical implementation in limited resources IoT ecosystem also emerged [19].

Supervised machine learning approaches, such as LR, RF, DT, and MLP, are analyzed by Mouiti *et al*. to enhance the detection of intrusions in IoT networks. In this research, the models were trained with the UNSW-NB15 dataset to differentiate between normal and attack traffic. The RF model showed higher accuracy with an accuracy of 99.20%, LR gave an F1 score of 85.80 with DT scoring 75.50% and MLP scoring 78.30% after applying the hyperparameter tuning and adaptive synthetic sampling. The study identified DoS, probe attacks, and other network intrusions and greatly benefited from balanced data sets that improved the detection of both the majority class and the minority class. However, some of the challenges include; data set class imbalance, and handling of large computational expenses mainly while working with complicated models such as MLP. Though

methods like oversampling with ADASYN and hyperparameter tuning have provided better results, the issue of real-time assessment in limited-resource IoT networks remains a drawback [20].

To deal with challenges in IoT security resulting from the growth of 5G connections and network interconnectivity, Elshweikh *et al*. suggest an improved IDS utilizing machine learning. In this paper, three machine learning algorithms known as Random Forest (RF), Decision Tree (DT), and Gradient Boosting are chosen and tested based on the Bot-IoT dataset. When it comes to handling imbalanced datasets both Feature Engineering and Synthetic Minority Oversampling Techniques abbreviated as SMOTE were used. The provided model had a good accuracy rate with an F1 score, and it was innovative compared to IDS approaches for detecting DDoS and other IoT attacks. However, there are some limitations while applying the IDS for real-time scenarios and in the presence of a large number of heterogeneous IoT devices [21].

Mahdi proposes an intrusive detection system for IoT networks, using machine learning-based, and more specifically LSTM and convolutional layers to analyze the traffic. Using the UNSW-NB15 dataset, the system achieved an accuracy of 96.76% with precision and recall of more than 96% showing that the proposed system successfully detects anomalies as well as the different types of attacks such as DoS, LogIn, Fuzzy Logic, and Worms. Although it developed good results, a potential limitation is the failure of the SO algorithm during the training phase due to high computational costs; moreover, further research proposes suitable enhancements to enhance the scalability and versatility of the IDS in the various IoT scenarios [22].

4. Results and Discussion

With the aid of advanced ML and DL methodologies in IDS solutions, the current studies on IoT network protection show the superiority over the regular methods. Most of the conventional IDS are based on rules or signatures for detection; thus, they are prone to multi-form and progressive threats such as zero days or botnet attacks. According to the 20 synthesized studies, the ML and DL models yield improved accuracy, flexibility, and scalability based on the heterogeneity of the IoT. This is because other features like CNNs, LSTM, and ensemble learning models work hand in hand with feature engineering methods to examine intricate features within network traffic. For example, models with elements of bi-LSTM-CNN combination [18] or self-supervised learning such as IResTAE2A [16] have reached quite high levels of accuracy, with more than 99 percent of correctly identified known and new threats. These models also significantly decrease the number of false positives some of which are inherent to traditional IDS making it realistic for use in real settings.

Further, ML/DL-based IDS prove to be more effective than conventional systems in identifying attacks that represent a smaller class, say U2R or R2L, by techniques like SMOTE and cost-sensitive learning. Thus, for real-time dynamic

threats, the ML/DL systems are also useful in uplifting the overall security infrastructure of IoT against cyber threats like DDoS and data piracy. These capabilities summarize how Information technology has changed the shape of IoT network security through ML/DL.

ML/DL models have several advantages-flexibility, accuracy, and capability of handling large volumes of data but notwithstanding that they also have shortcomings. The flexibility in the performance of ML/DL techniques originates from the fact that the algorithms can recognize patterns and apply the same to unknown types of attacks. For instance, several state-of-the-art deep learning frameworks encompassing autoencoder and adversarial networks were used in feature extraction and anomaly detection tasks to prove high effectiveness [15]. Further, other classifier methods such as ensemble learning that combine classifiers such as the Random Forest (RF) and Gradient Boosting have been proven to enhance multiclass classification considerably according to recent works of [19] [21]. These strengths support the proposition that ML/DL is well-positioned to manage the increasing complexity of IoT networks.

However, the challenge that accompanies trainers and deploying ML/DL models is that there is a high computational cost. Most research such as [17] noted that CNN and LSTMs especially are computationally intensive, and thus, cannot be applied to low-power IoT devices. Moreover, the models are tested on either artificial or unbalanced data which are essentially far from real-life situations. For example, most of the datasets applied in the reviewed studies, including CICIDS2017 and UNSW-NB15, do not contain variety in terms of attack strategies or may not fully characterize the heterogeneity of the IoT networks. Due to this, the proliferation of datasets from the domain seems to present a limited variety, which could affect the stability of these models when used in applications across different IoT structures.

The application of IDS based on ML/DL techniques in practice in an IoT environment is problematic. Another potential problem is referred to as dataset variation. Most of the works depend on a few datasets that are not real-world traffic or the continuously growing variety of IoT threats like Bot-IoT or NSL-KDD datasets. This limits the models in a way to understand new forms of attacks, which are not presented as a part of the training data set and new conditions of the network. The other crucial issue is the scalability in real-time. Although numerous models reach favorable offline performance, using them in real-time IoT networks demands low latency, which is infeasible due to the computational intensity of deep models. Although methods like federated learning, discussed by Radjaa and his team in their work [8], mitigate some of the scalability challenges, novel challenges emerge, comprising node synchronization and working with non-IID data.

There are also cost concerns that stand as a hurdle to increasing the use of technology by the organization. The large-scale databases themselves are necessary for training the advanced characteristic ML/DL models; nevertheless, high computational power is mandatory and pricey. Moreover, these systems have the problem

of high energy consumption, mainly for IoT, where devices may be limited in energy sources. This provokes a discussion regarding the applicability of defining resource-demanding models such as CNNs or BiLSTMs over battery-assisted IoT networks.

5. Conclusion

The ML/DL-based IDS have brought revolutionary improvement in IoT network security as they have offered higher accuracy, flexibility, and scalability than conventional systems. However, issues like the types of datasets to incorporate, real-time applicability, and computational load are still considerable hurdles. For these problems, future research focuses on the lightweight model, federated learning, and the hybrid approach, which can be empowered by the ML/DL techniques to enhance the security of the IoT ecosystem comprehensively.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks*, **76**, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[2] Berman, D.S., Buczak, A.L., Chavis, J.S. and Corbett, C.L. (2019) A Survey of Deep Learning Methods for Cyber Security. *Information*, **10**, Article 122. https://doi.org/10.3390/info10040122

[3] Elsayed, R., Hamada, R., Hammoudeh, M., Abdalla, M. and Elsaid, S.A. (2022) A Hierarchical Deep Learning-Based Intrusion Detection Architecture for Clustered Internet of Things. *Journal of Sensor and Actuator Networks*, **12**, Article 3. https://doi.org/10.3390/jsan12010003

[4] Telikani, A., Rudbardeh, N.E., Soleymanpour, S., Shahbahrami, A., Shen, J., Gaydadjiev, G., *et al.* (2024) A Cost-Sensitive Machine Learning Model with Multi-task Learning for Intrusion Detection in IOT. *IEEE Transactions on Industrial Informatics*, **20**, 3880-3890. https://doi.org/10.1109/tii.2023.3314208

[5] Laha, B., Basu, D., Biswas, S., Gupta, P. and Sadhukhan, B. (2023) Intrusion Detection in IOT Systems Using Ensemble Machine Learning Techniques. 2023 *IEEE 4th Annual Flagship India Council International Subsections Conference* (*INDISCON*), Mysore, 5-7 August 2023, 1-7. https://doi.org/10.1109/indiscon58499.2023.10270505

[6] Panthakkan, A., Anzar, S.M. and Mansoor, W. (2023) Enhancing IOT Security: A Machine Learning Approach to Intrusion Detection System Evaluation. 2023 *IEEE International Conference and Expo on Real Time Communications at IIT* (*RTC*), Chicago, 2-5 October 2023, 19-23. https://doi.org/10.1109/rtc58825.2023.10304239

[7] Khan, I.U., Ayub, M.Y., Abdollahi, A. and Dutta, A. (2023) A Hybrid Deep Learning Model-Based Intrusion Detection System for Emergency Planning Using IOT-Network. 2023 *International Conference on Information and Communication Technologies for Disaster Management* (*ICT-DM*), Cosenza, 13-15 September 2023, 1-5. https://doi.org/10.1109/ict-dm58371.2023.10286954

[8] Radjaa, B., Nabila, L. and Salameh, H.B. (2023) Federated Deep Learning-Based In-

trusion Detection Approach for Enhancing Privacy in Fog-IOT Networks. 2023 10*th International Conference on Internet of Things*: *Systems*, *Management and Security* (*IOTSMS*), San Antonio, 23-25 October 2023, 156-160. https://doi.org/10.1109/iotsms59855.2023.10325826

[9] Ennaji, E.M., El Hajla, S., Maleh, Y. and Mounir, S. (2024) Federated Deep Learning Models for Intrusion Detection in IOT. *Proceedings of the* 7*th International Conference on Networking*, *Intelligent Systems and Security*, Meknes, 18-19 April 2024, 1-5. https://doi.org/10.1145/3659677.3659837

[10] Walling, S. and Lodh, S. (2024) Enhancing IOT Intrusion Detection through Machine Learning with AN-SFS: A Novel Approach to High Performing Adaptive Feature Selection. *Discover Internet of Things*, **4**, Article No. 6. https://doi.org/10.1007/s43926-024-00074-5

[11] Francis, G., Sheeja, S. and John, A. (2023) IOT Intrusion Detection Using the Two-Tier-Convolutional Deep-Learning Model. 2023 *International Conference on IOT, Communication and Automation Technology* (*ICICAT*), Gorakhpur, 23 June 2023, 1-7.

[12] Divakarla, U. and Chandrasekaran, K. (2023) IOT Devices Using Supervised Machine Learning Models for Anomaly Based Intrusion Detection. 2023 *International Conference on Emerging Smart Computing and Informatics* (*ESCI*), Pune, 1-3 March 2023, 1-5. https://doi.org/10.1109/esci56872.2023.10099676

[13] Sharma, A. and Babbar, H. (2023) Enhancing IOT Security: Machine Learning-Based Network Intrusion Detection. 2023 3*rd Asian Conference on Innovation in Technology* (*ASIANCON*), Ravet, 25-27 August 2023, 1-6. https://doi.org/10.1109/asiancon58793.2023.10269850

[14] Wadate, A.J. and Deshpande, S.P. (2023) A Deep Machine Learning Approach for Intrusion Detection in IOT. 2023 *International Conference on Computing*, *Communication*, *and Intelligent Systems* (*ICCCIS*), Greater Noida, 3-4 November 2023, 58-63. https://doi.org/10.1109/icccis60361.2023.10425682

[15] Diallo, A., Affognon, L., Diallo, C. and Ezin, E.C. (2023) A Three-Level Deep Learning Intrusion Detection System for IOT Network. 2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE), Dubai, 30-31 December 2023, 1-6. https://doi.org/10.1109/icecce61019.2023.10442798

[16] Tong, J. and Zhang, Y. (2024) A Real-Time Label-Free Self-Supervised Deep Learning Intrusion Detection for Handling New Type and Few-Shot Attacks in IOT Networks. *IEEE Internet of Things Journal*, **11**, 30769-30786. https://doi.org/10.1109/jiot.2024.3414492

[17] Kumar, M. and Dubey, S.K. (2023) Network Intrusion Detection for IOT Devices Using Deep Learning. 2023 10th *IEEE Uttar Pradesh Section International Conference on Electrical*, *Electronics and Computer Engineering* (*UPCON*), Gautam Buddha Nagar, 1-3 December 2023, 1198-1203. https://doi.org/10.1109/upcon59197.2023.10434703

[18] Hinojosa, A. and Majd, N.E. (2024) Edge Computing Network Intrusion Detection System in IOT Using Deep Learning. 2024 33*rd International Conference on Computer Communications and Networks* (*ICCCN*), Kailua-Kona, 29-31 July 2024, 1-6. https://doi.org/10.1109/icccn61486.2024.10637611

[19] Chauhan, D., Shah, M. and Joshi, H. (2023) A Novel Intrusion Detection System Based on Machine Learning for Internet of Things (IOT) Devices. 2023 3*rd International Conference on Smart Data Intelligence* (*ICSMDI*), Trichy, 30-31 March 2023, 427-434. https://doi.org/10.1109/icsmdi57622.2023.00081

[20] Mouiti, M., Elhariri, A., Habibi, O. and Lazaar, M. (2023) Toward Improving Internet of Things (IOT) Networks Security Using Machine Learning Based Intrusion Detection System. 2023 *International Conference on Digital Age & Technological Advances for Sustainable Development* (*ICDATA*), Casablanca, 3-5 May 2023, 46-51. https://doi.org/10.1109/icdata58816.2023.00018

[21] Elshweikh, A.A., Maher, A.M., Hussein, M. and Elbayoumy, A.D. (2024) Intrusion Detection System for IOT Using Machine Learning. 2024 *International Telecommunications Conference* (*ITC-Egypt*), Cairo, 22-25 July 2024, 326-331. https://doi.org/10.1109/itc-egypt61547.2024.10620546

[22] Mahdi, M.A. (2024) Secure and Efficient IOT Networks: An AI and Ml-Based Intrusion Detection System. 2024 3*rd International Conference on Artificial Intelligence for Internet of Things* (*AIIoT*), Vellore, 3-4 May 2024, 1-6. https://doi.org/10.1109/aiiot58432.2024.10574789