Alkadhim Journal for Computer Science, Vol.3, No. 2(2025)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

A Comprehensive Review of Intrusion Detection Systems in IoT Networks Using ML and DL Techniques

[1]Fatima Rahim Nasser – Iraq

[2]Asst.Prof.Dr.Saif Ali Abd Alradha Alsaidi – Iraq

College of Computer Science and Information Technology, Wasit University, Kut, Iraq

Article information

Article history:

Received: May 24, 2025

Accepted: 2025

Available online: 2025

Keywords:

IoT, Intrusion Detection System, Machine learning (ML), Deep learning (DL).

Corresponding Author:

Full Name

[1]fatimar201@uowasit.edu.iq

[2] salsaidi@uowasit.edu.iq

DOI:

https://doi.org/10.61710/kjcs.v3i2.111

Abstract

The Internet of Things (IoT) is growing at an extremely rapid rate, impacting all aspects of our lives and extending to various fields, including wearable technology, smart sensors, and home appliances. However, the rapid growth is coupled with serious security concerns that render these technologies vulnerable to hacking opportunities and erode user privacy, as well as data protection, especially as cyber-attacks become more complex. Intrusion detection is a crucial aspect for tracking and thwarting such attacks. Machine learning (ML) and deep learning (DL) algorithms have ever-increasing efficiency in automating procedures like these. This study aims to provide researchers with a comprehensive overview of contemporary Intrusion Detection System (IDS) techniques employed in the IoT environment, highlighting strengths and weaknesses. It also gives direction to future research by suggesting that more adaptive, lightweight, and efficient intrusion detection systems can be developed to address the unique constraints of IoT networks.

1. Introduction

The Internet of Things (IoT) has emerged as the next significant technological revolution in computing, impacting all aspects of human existence [1]. The increasing network of interconnected Internet-enabled devices encompasses IoT applications in connected autos, smart homes, smart retail, supply chain management, urban environments, educational institutions, industrial facilities, organizations, agricultural settings, and healthcare centres [2]. The term IoT refers to a category of computing systems that facilitate the collection, transmission, and interconnection of devices, as well as the real-time management of data and applications [3]. Nonetheless, this rapid growth and the incorporation of electronics into everyday life present numerous concerns, especially those related to security [4].

Constructing resilient IoT networks presents various challenges, including constrained resources, inadequate energy efficiency, device heterogeneity, managing substantial data volumes, ensuring high-bandwidth data transmission, scalability, and, crucially, safeguarding user data and privacy [5, 6]. The vast collection of interconnected devices constitutes an extremely large attack surface, and they are potential points of entry for malicious entities. Moreover, the absence of standards, inherent unsafe defaults, and restricted processing capabilities of most IoT devices enhance these security risks. Strong security solutions are thus paramount to the protection of the highly dynamic IoT ecosystem [7]. These security issues must be addressed so that the Internet of Things can reach its full potential without compromising user trust and security [8]. Network Intrusion Detection Systems (NIDS) are now part of the cybersecurity defence mechanisms. These technologies notify and track security administrators of unusual behaviour that can compromise the integrity of the network [9]. Machine learning and artificial intelligence-based intrusion detection systems have increasingly been employed in the Internet of Things (IoT). Such systems will learn and know normal network behaviour patterns automatically, enabling them to detect abnormal activity well. IDSs can defend against intrusions and inform IoT devices of abnormal activity before intruders will be able to invade the network. Therefore, for IDS to be efficient, it ought to meet the requirements of time complexity, high accuracy, and low complexity. Data mining is stronger in behaviour compared to conventional IDSs and enables the realization of improved accuracy for new intrusion types through knowledge discovery [10].

Our contributions to this work are the following:

• We survey previous studies of NIDS that use AI techniques.

• We compare the performance of different models with different datasets and IoT.

2. Relevant Terms

This section introduces the two primary concepts of this paper: intrusion detection systems and the Internet of Things.

2.1. Internet of Things

IoT has undergone exponential growth over the years [11]. IoT is a network of interconnected devices that can communicate and share data without human intervention, and is utilized in various applications. These gadgets can learn and adapt to user preferences by analysing past data, enhancing prediction capabilities, and improving user experience. IoT devices connect to the Internet directly or indirectly, enabling the sharing of information and facilitating user interaction. In a nutshell, IoT establishes a unified network of physical devices that combine software applications, allowing users to access and operate their gadgets from practically anywhere via Internet-connected devices [12].

This architecture is composed of three layers. The first is the perception layer, sometimes known as the physical layer. It has sensors that detect and collect information about the surroundings. It senses specific physical factors or recognizes other intelligent objects in its environment [13]. Second Network Layer: It serves as a connection between the perception and network layers. It sends the data recorded by the preceding layer to multiple devices, hubs, or servers on the Internet via any communication medium, whether it's wired or wireless [14]. The third is the application layer, which provides end users with application-specific services while maintaining the confidentiality, integrity, and authenticity [15]**.** As shown in Figure 1.

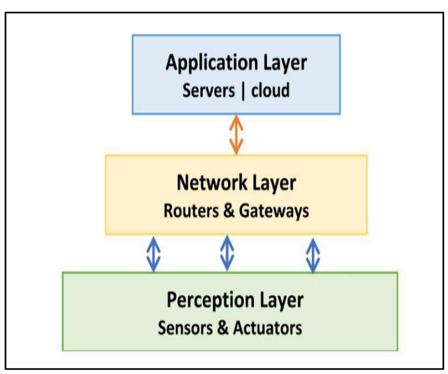

Figure (1): Layer architecture of IoT [15].

The Confidentiality, Integrity, and Availability (CIA) triangle is a fundamental concept in cybersecurity, although little research has directly linked it to IoT. In addition to the CIA trinity, recent research highlights the importance of elements such as identification and verification, privacy, and trust. The Open Web Application Security Project (OWASP) identifies IoT Attack Surface Areas that manufacturers, developers, researchers, and organizations deploying IoT technologies must be aware of. Security issues arise at several stages of the IoT architecture, each exposing distinct weaknesses and potential attacks: The perception layer, which is responsible for data collecting, faces issues such as data fraud and device destruction. Attacks include node acquisition, malicious code injection, fake data injection, replay or freshness concerns, cryptanalysis, eavesdropping, interference, and sleep deprivation. The network layer is responsible for data transmission, and its security issues centre on the availability of network resources. Common threats include denial-of-service (DoS) attacks, spoofing, sinkholes, wormholes, man-in-the-middle (MITM) attacks, routing information manipulation, Sybil attacks, and unauthorized access. The application layer provides user-requested services and is primarily vulnerable to software-related attacks, such as phishing, malicious viruses and worms, and dangerous scripts. Overall, a thorough knowledge of these problems is required [16,17].

2.2 Intrusion Detection System (IDS)

Intrusion is defined as any illegal activity that causes damage to an information system. Any attack threatening confidentiality, integrity, or availability will be considered an incursion. For example, behaviours that render computer services unusable to legitimate users are termed intrusions. IDS is a software or hardware device that detects harmful activity on computer systems and maintains system security. An IDS aims to detect many types of malicious network traffic and computer activities that a typical firewall cannot detect. This is crucial for ensuring robust protection against actions that compromise the availability, integrity, or confidentiality of computer systems [18]. Individual IDSs consist of both network-based and host-based IDS [19]. A NIDS monitors network traffic for network device security and analyses the protocols (network, application, transport, etc.) utilized to detect suspicious behaviours. HIDS monitors a host's properties and activities to detect potential threats. A host-based intrusion detection system monitors data, including traffic information, system logs, file access, and file modifications [20]. IDS systems are classified into two main categories: signature-based intrusion detection systems (SIDS) and anomaly-based intrusion detection systems (AIDS).

A. Signature-based Intrusion Detection System (SIDS): a typical method for detecting cyberattacks that uses pattern matching to identify known threats from a database of predefined attack signatures [19,20]. These systems perform well in identifying previously published assaults, but they struggle with zero-day attacks and advanced threats such as polymorphic malware. However, the rising complexity of modern attacks shows the limitations of SIDS. It emphasizes the need for alternative approaches, such as AI-based Detection Systems, to boost the efficiency of identifying emerging and advanced threats [21].

B. Anomaly-Based Intrusion Detection System (AIDS): This approach has garnered significant interest due to its ability to overcome the limitations of SIDS. AIDS uses machine learning, statistical analysis, and knowledge-based techniques to build a model of typical system functioning. Any significant variation from this expected behaviour is recorded as an anomaly, which could indicate an intrusion. Unlike SIDS, AIDS can detect zero-day assaults since it does not rely on pre-existing signature databases. AIDS development is divided into two phases: training, which builds a model of normal behaviour, and testing, which evaluates the system on new data [22].

AIDS provides various benefits, including the ability to identify previously unknown intrusions and internal harmful activity. For example, an alarm is raised if an intruder performs unusual actions within a stolen account. Furthermore, the system's reliance on specific behavioural profiles makes it difficult for attackers to avoid discovery. However, one significant weakness of AIDS is its sensitivity to large false positive rates, as new, normal activities may be misclassified as anomalies. AIDS methods are categorized into various groups, including statistics-based, pattern-based, rule-based, state-based, and heuristic-based approaches, which make them adaptable but challenging to standardize [23].

3. AI Methods for NIDS

This section provides an overview of the AI-based NIDS technique, along with specifics on the most commonly used machine learning (ML) and deep learning (DL) algorithms for designing an efficient NIDS. Machine and deep learning are widely classed as supervised and unsupervised algorithms. Unsupervised algorithms use unlabelled data to extract useful features and information, whereas supervised algorithms derive usable information from labelled data [24].

3.1. A general AI-based IDS methodology

A NIDS is generated using ML and DL approaches and typically consists of three key processes, as shown in Figure 2: (i) data pre-processing, (ii) training, and (iii) testing. All the recommended solutions begin with pre-processing the dataset to convert it into a format the algorithm can use. This stage usually includes encoding and normalization. The dataset may occasionally require cleaning, such as deleting missing data and duplicate entries, which is also conducted during this step. The pre-processed data is randomly separated into two sets: the training and testing datasets. Typically, the training dataset accounts for nearly 80% of the original dataset size, with the remaining 20% being the testing dataset. The training dataset is then used to train the machine learning (ML) or deep learning (DL) algorithm. The time required for the method to learn is determined by the size of the dataset and the complexity of the proposed model. Typically, the training period for the DL model necessitates deep and complicated structures. Once the model has been trained, predictions are made. In NIDS models, network traffic instances are expected to be either benign (standard) or belong to an attack class [25]. The following section presents a detailed review of commonly used machine learning (ML) and deep learning (DL) methods for NID systems.

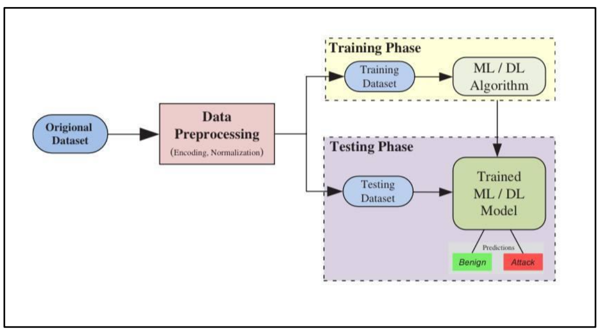

Figure (2): Generalized ML\DL-based NIDS [25]

3.2.ML algorithms

Machine Learning (ML) is a subfield of AI that focuses on creating methods and algorithms that enable computers to learn from data and make judgments or predictions without explicit programming [26]. It is used for large-scale data processing and is ideal for complex datasets with many variables and characteristics. The ML process begins with receiving training data and making observations on data through direct experience or by instruction, which results in output values. Algorithm selection should be appropriate for observing data trends, improving analytic and predictive power, and making better selections in future training data. Machine learning approaches are primarily classified into three categories: supervised, unsupervised, and reinforcement learning [27].

The following subsection provides a brief review of some of the most commonly used machine learning (ML) techniques for network intrusion detection.

3.2.1 Decision Tree (DT): Decision trees are popular for IDS because they are intuitive and easy to read. They classify data by dividing it into subgroups according to the value of the input attributes. Each node represents a feature, and each branch represents a decision rule, with leaf nodes indicating the class name [28].

3.2.2 K-Nearest Neighbour (KNN): is a basic supervised machine learning approach that uses "feature similarity" to classify data samples. By computing distances between points, KNN identifies the class of a new data point based on the majority vote of its k-nearest neighbours, with the parameter k determining model performance. The model risks overfitting when k is too small, whereas a huge k can result in misclassification. It is a popular and uncomplicated technique for machine learning classification tasks because of its simplicity, ease of implementation, and ability to learn complex functions [29].

3.2.3 Support vector machine (SVM): is a supervised machine learning technique based on the concept of a maximum margin separation hyperplane in n-dimensional feature space. It solves linear and nonlinear problems. Kernels are used to solve nonlinear issues. A dimensional input vector is initially mapped and allowed into a high-dimensional feature space using the kernel function. The support vectors are then used to compute an optimal maximum marginal hyperplane, which serves as a decision boundary. The SVM method can enhance the efficiency and accuracy of NIDS by accurately predicting normal and malicious classes [30].

3.2.4 K-means clustering: It divides data points into clusters based on similarity. In IDS, regular traffic forms distinct clusters, whereas abnormalities appear as outliers or establish their clusters. This strategy effectively detects fresh dangers, although the number of clusters must be carefully tuned. To enhance performance, the authors proposed integrating data transformation (DT) with k-means clustering for anomaly detection in Internet of Things (IoT) networks [31].

3.2.5 Ensemble methods: The main idea behind ensemble methods is to profit from the many classifiers by learning in an ensemble manner. Each classifier has various advantages and disadvantages. Some individuals may excel in identifying specific types of attacks while performing poorly on others. The ensemble approach combines weak classifiers by training several classifiers and then generating a stronger classifier using a vote algorithm [32].

3.3. Deep learning algorithms

DL is a subtype of ML that uses multiple hidden layers to obtain the features of a deep network [33]. This section describes the DL methodologies used to propose DL-based NIDS solutions in their published works.

3.3.1. Recurrent Neural Networks (RNNs): neural network structures that process sequential data, i.e., time series or text data. Its processes loop data around the network so it can retain context information from past inputs and apply it to the current input [34]. A form of neural network with sequential modelling capability is used extensively in intrusion detection. RNNs, in contrast to CNNs, support sequential input and temporal dependency learning, remembering past knowledge. RNNs can then be utilized to improve the intrusion detection performance of intrusion detection models, particularly for intrusion behaviors with temporal characteristics [35].

3.3.2. Autoencoder (AE): is one form of unsupervised machine learning algorithm for learning data representations or compressed features. It has two basic elements: an encoder and a decoder. The data is compressed into a low-dimensional representation that the decoder reconstructs into a data reconstruction. The AE is mainly applied for data dimensionality reduction and for extracting features. Therefore, AE and machine learning are combined in IDS to create novel deep-learning architectures. Many feature extraction and dimensionality reduction of data are done by AE, whereas classification is done by machine learning [36].

3.3.3. Deep Neural Network (DNN): is a very influential neural network structure, built as a feed-forward neural network (FNN) to prevent recursive connections. Its most mentioned characteristic is to accommodate numerous hidden layers with a huge impact on learning. Every hidden layer contains several neurons that input and process the output of the preceding layer. These neurons can obtain the intricate and subtle patterns in data by performing a nonlinear transformation of the activation function. The stacked hidden layers of a DNN enable complex nonlinear patterns and highly abstracted informative features to be learned from the input [37].

3.3.4. Deep Belief Network (DBN): is a generative deep model and employs multilayer Restricted Boltzmann Machines (RBMs) [38]. The primary role of DBN is to accomplish the data's intrinsic distribution and generate new samples. The distinctive advantage of DBN is the multi-layered architecture, with each layer holding an RBM. The RBM is an energy-based model that uses a probabilistic approach with visible and hidden layers for efficient simulation of the joint distribution of data by adjusting weighting parameters. DBNs are pre-trained in a layer-by-layer manner, including pre-training and fine-tuning. They are applied in many areas, including feature learning, data generation, migration learning, and unsupervised pre-training. DBN is capable of building data, minimizing it, and learning informative feature representations with excellent performance and generalization [39].

3.3.5. Convolutional Neural Network (CNN): CNN is a novel network architecture that replaces convolution computation with matrix multiplication, distinguishing it from previous artificial neural networks. CNNs gain a certain property that enhances data processing efficiency through the convolution process [40]. CNNs are constructed to leverage the two-dimensional nature of the input data to its fullest potential. CNNs have been applied to surpass other deep learning architectures in speech and image recognition. CNNs have three major layers. The convolutional layer performs the most important job of feature extraction, identifying significant elements of input data through convolutional algorithms. The pooling layer does the job of choosing the features, which simplifies parameters by reducing the number of features. These accumulated features are mapped to single classes via a fully connected layer in the last classification. The result is a hierarchy that enables the CNN to perform outstanding feature extraction and classification operations [41].

4. Intrusion Detection System in the Internet of Things

In this section, a collection of previous studies on intrusion detection in Internet of Things networks using machine learning and deep learning techniques will be presented. To facilitate the comparison of several studies, highlight the most prominent methods used and their results, and identify the strengths and limitations of each study, a table (4.1) has been prepared to summarize these studies.

In 2021, Kasongo, S. M., et al. [42] developed an advanced IDS for Industrial Internet of Things (IIoT) networks using the Genetic Algorithm (GA) for feature selection using the Random forest RF model within the fitness function and used several classifier including Decision trees, Extra tree, XGBoost, and logistic Regression were evaluated on the UNSW-NB15 dataset, which represents complex network traffic patterns. The results demonstrated a classification accuracy of 87.61% in binary classification with an AUC score of 0.98

In 2022, Disha & Waheed. [43] Analysed the performance of IDS using modern machine learning techniques such as Decision Trees, Gradient Boosting Trees, and neural networks regarding feature selection by using the Gini Impurity Weighted Random Forest technique for reducing data dimensions. The study employed more recent datasets, such as UNSW-NB 15 and Ton_IoT, which performed better. Accuracy of the DT model was 93.01% and F1 score was 93.72% on the UNSW-NB15 dataset after feature selection. The Gradient Boosting Tree model achieved an accuracy of 99.98% on the Ton_IoT dataset. Feature selection also enhanced the F1 score and reduced the number of false positives, thereby making IDS more efficient in the detection of new threats.

In 2023, Altunay, H. C., et al. [44] proposed a combination model integrating Convolutional Neural Networks and Long Short-Term Memory networks for IIoT intrusion detection in 2023. The model was evaluated on the UNSW-NB15 and X-IIoTID datasets for binary and multi-classification tests. The combination model outperformed other approaches, with 93.21% and 92.9% accuracy on the UNSW-NB15 dataset for binary and multi-class classification, respectively. In addition, it was 99.84% and 99.80% accurate, with an F1 score of 99.60% for binary classification and 90.54% for multi-class classification for the X-IIoTID dataset. This result demonstrates significant improvement in intrusion detection systems and indicates that deep learning approaches need to be implemented in order to deal with complex and voluminous datasets in Industrial Internet of Things configurations.

In 2023, Bakhsh et al. [45] improved the security of IoT networks by utilizing an intrusion detection system (IDS) supported by deep learning techniques, including Random Forest Neural Networks (RF and NN), Long Short-Term Memory (LSTM), and Feed Forward Neural Networks (FFNN).. The study used the CIC-IoT22 dataset to train models that accurately detect cybersecurity attacks, such as Denial-of-Service (DoS) attacks and flooding attacks. the FFNN achieved highest accuracy of 99.93%, precision of 99.93%, recall of 99.93%, and F1-score of 99.93%. and achieved the accuracy of 99.85% using LSTM, indicating the potential of the proposed method to improve intrusion detection in IoT networks.

In 2023, Awotunde et al. [46] prepared an extensive review for improving the performance of the Intrusion Detection System (IDS) for IIoT networks. The study was conducted using the Ton_IoT dataset, which is real-time IIoT appliance telemetry data, like refrigerators, thermostats, and motion detectors. It used the Chi-Square feature selection strategy to minimize data complexity as well as improve model efficiency. Multiple ensemble methods were used, including XGBoost, Random Forest, and AdaBoost, whose output placed XGBoost at maximum capability with an accuracy of 100%, Recall 99.79%, precision 99.95% and Recall 99.75%. Data-balancing approaches and deep learning methods were suggested by the research as future directions for performance improvement, hence making it an ideal reference point for developing optimal IDS solutions for IIoT networks.

In 2023, Le et al. [47] proposed A fusion to enhance the performance of intrusion detection systems in IoT networks. The authors applied state-of-the-art methods, such as Mean Decrease in Impurity (MDI), to determine the most significant features. Explainable AI methods, such as LIME and Counterfactual, were employed to interpret and examine the model's decisions. The method was tested on two big datasets, CICIoT2023, with a detection accuracy of 99.5%, a precision of 98.51%, a recall of 99.63%, and an F1 value of 99.07%. IoTID20 also reported 100% results for all scales. Results confirmed significant improvements in capability explanation and accurate delimitation of classification boundaries between different categories of attacks, which reveal the benefits of implementing state-of-the-art and explainable AI techniques to enhance IoT security.

In 2023, Sayed, N., et al. [48] introduced two new models for CNN to identify nine attacks from the NF-UNSW-NB15-v2 dataset. Accuracy levels were established as 99% detection of most attack classes, indicating model performance in classifying classes. Research was compounded by imbalanced classes in the dataset, requiring resampling and cost-sensitive learning to improve model performance. This research is a valuable contribution to the literature in the area of intrusion detection systems for IoT environments, as it offers effective solutions that are resource-hungry for devices.

In 2024, Sarhan et al. [49] evaluated the performance of IDSs in IoT systems by using feature extraction techniques (PCA, LDA, Autoencoder) and six ML algorithms on three benchmark datasets (UNSW-NB15, Ton-IoT, CSE-CIC-IDS2018). Accuracy was found to be maximum with the Autoencoder and DT algorithm on the Ton-IoT and CSE-CIC-IDS2018 datasets, with values of 98.23% and 98.15%, respectively. For comparison, CNN had the best accuracy of 98.16% on UNSW-NB15. The study highlighted the contribution of feature selection and dimensionality reduction, and concluded that an ideal 20 dimensions would enhance performance, and recommended applying a standard set of features in order to generalize and apply to real-world settings.

In 2024, Almotairi et al. [50] focused on enhancing the efficiency of IDSs in IoT networks using the aid of ML techniques. The study utilized the Ton-IoT dataset and applied the K-Best algorithm to identify 15 informative features. A Stack Classifier model was built, a collection of multiple traditional algorithms like RF, SVM, NB, and K-NN. The result was that the ensemble model outperformed individual models with a staggering accuracy of 99.99%, precision of 99.98%, recall of 99.99%, and F1 score of 99.99%. This is to further clarify its effectiveness in detecting malicious behaviour and minimizing false positives in IoT networks.

In 2024, Inuwa & Das. [51] Compare the efficiency of ML models in detecting anomalies in IoT networks using the Ton-IoT and BoT-IoT datasets. Five models were utilized: NNs, SVM, DT, KNN, and Logistic Regression. The results revealed that Neural Networks performed better than other models with an accuracy of 99.99%. Therefore, they are the most appropriate to utilize in the detection of cyberattacks. This study is a helpful roadmap to enhancing cybersecurity practice in IoT environments.

In 2024, Xiao et al. [52] wanted to develop an expert intrusion detection system for IoT networks using Autoencoder technology. Traditional models were limited by two inbuilt challenges: limited computing capability on edge devices and higher accuracy demand in models with reduced sizes. To overcome these, scientists used an Extreme Learning Machine to implement an Autoencoder, dividing data into separate fields to attain the best performance. Experimental testing on the NSL-KDD dataset showed improvements in accuracy and F1-score of 3.5% and 2.9%, respectively, without sacrificing model lightness, thus making it deployable on resource-constrained edge devices.

In 2024, Li et al. [53] used the Ton-IoT dataset to compare Feature Selection (FS) and Feature Extraction (FE) techniques to improve the performance of IDS in IoT networks. Five machine learning algorithms were utilized in the experiment: Multi-Layer Perceptron, K-NN, RF, DT, and NB. FE outperformed FS, which achieved the highest accuracy of 86% when the Random Forest algorithm was applied to all 77 features and 89.1% when the k-Nearest Neighbours algorithm was used on 33 features. The study emphasizes the need to select a strategy that is most suitable for the system's requirements and available resources.

In 2024, Sayegh, H. R., et al. [54] proposed an intrusion detection system (IDS) based on a Long Short-Term Memory (LSTM) model to enhance the security level of IoT networks. SMOTE was utilized in this work to generate synthetic minority class samples, thereby overcoming the data imbalance issue. The proposed system outperformed other methods, achieving detection rates of 99.34% and 99.75% using the CICIDS2017 and NSL-KDD datasets, respectively. One of the difficulties emphasized was dealing with temporal data and precisely balancing classes in the datasets so that the system performs well.

Table 1: Comparison between different approaches to intrusion detection systems for IoT networks

Authors	Dataset	Methodology	Accuracy	Strengths	Limitation
[42]	UNSW-NB15	GA, RF, LR, NB, DT, ET, XG Boost	87.61%	Used GA to select an important feature	only used one dataset and a Low accuracy

					result
[43]	UNSW-NB15 and Ton-IoT	DT, RF, AdaBoost, GBT, MLP, LSTM, GRU	99.98%	Comprehensive performance and excels with high accuracy	high computation cost
[44]	UNSW-NB15 and X-IIoTID	CNN, LSTM	99.80%	Used deep learning techniques	a long-time detection and high computation cost
[45]	CIC-IoT22	FFNN, LSTM, RF, and NN.	99.85%	The ability to learn complex patterns	Complexity And needs a long time to train
[46]	Ton-IoT	XGBoost, RF, ET	99%	Used ensemble techniques to classify	only used one dataset
[47]	CICIoT2023 and IoTID20	Gradient Boosting, DT, RF, with LIME and Counterfactual	98.3%	Enhance generalization	High computation cost
[48]	NF-UNSW-NB15-v2	CNNs	99%	Used deep learning techniques	only used one dataset and a long-time detection
[49]	Ton-IoT, UNSW-NB15 And CSE-CIC-IDS2018	DT, LR, NB, RNN, CNN, DFF	98.33%	Used diverse techniques and evaluation methods across three datasets	Long-time detection and high computation cost
[50]	Ton-IoT	NB, RF, KNN, SVM	99.99%	Selecting the most important feature	only used one dataset The model lacks generalization
[51]	Ton-IoT and Bot-IoT	SVM, NN, KNN, DT, LR	99.99%	Comprehensive performance and excels with high accuracy	High computational cost
[52]	NSL-KDD	Autoencoder, ELM	94.32%	An accurate and lightweight model	only used one dataset
[53]	Ton-IoT	Multi-Layer Perceptron, K-NN, RF, DT, and NB.	89.1%	Focuses on feature education techniques	Low accuracy result, and only used one dataset
[54]	CICIDS2017 and NSL-KDD	LSTM	99.75%	Solved the imbalance problem and used LSTM	Long detection time

The reliability of research in the area of intrusion detection systems for IoT networks is influenced by several foundational factors. Most significant among them is dataset diversity and completeness, as research that utilizes varied and multiple datasets is more reliable than work based on a single dataset. Diversity provides generalizability and reduces bias in findings. Methodological comprehensiveness is the second aspect, where studies that employ an array of integrated methods and offer extensive comparisons between different methodologies are more insightful regarding the problem and yield more robust solutions. The third factor is the transparency of results and limitations. More reliable studies are those that openly acknowledge their limitations and challenges, such as high computational costs and difficulties in generalization, unlike studies that present idealized outcomes without declaring their limitations. The fourth factor is real-world issue management in the field, e.g., data imbalance and network complexity, where studies that address such practical challenges provide more applicable and implementable solutions. Finally, methodological innovation with assured results is regarded as a critical variable. An investigation that employs new techniques while achieving assured results in repetitive experiments is more credible than one that attains high accuracy in a single successful experiment.

5. Challenges of IDS in IoT networks

The field of intrusion detection in IoT networks faces several critical challenges that must be addressed to develop robust, efficient, and scalable solutions:

1. Diversity and Imbalance of Data: The huge amounts of heterogeneous data generated by IoT networks are caused by a myriad of devices, including sensors, cameras, and smart appliances. This heterogeneity creates difficulties in building homogeneous detection models. In addition, imbalanced datasets, where attack traffic is a small proportion of the total traffic, have biases toward majority classes that hinder the performance of machine learning models.

2. Resource Limitations: The processing power, memory, and energy resources of many IoT devices are constrained. Designing a lightweight IDS that can operate effectively under these limitations while maintaining high accuracy, particularly when utilizing sophisticated AI algorithms, can be challenging.

3. False Positives and Detection Accuracy: In AIDS, inappropriately high false-positive rates are a major concern. Misclassifying harmless actions as a threat might cause wastage of resources and loss of trust in the IDS.

4. Zero-Day and Evolving Threats: The major issue is that cyber threats evolve constantly, for example, advanced persistent threats (APTs) and zero-day attacks.

5. Scalability and Real-Time Processing: The IDS needs to be scalable enough to handle an enormous volume of data with real-time threat detection, as more and more devices are getting associated with the Internet of Things.

6. Dataset and benchmarking availability: Model performance benchmarking is hindered by the unavailability of real-world and large-scale datasets for IoT-specific IDS evaluation.

6. Conclusion

This research investigated the utilization of advanced artificial intelligence (AI) techniques to enhance Intrusion Detection Systems (IDS) of Internet of Things (IoT) networks in resolving some of the most serious problems, including security threats, false alarms, and limited resources. Through the analysis of current approaches and combining current state-of-the-art approaches, the research highlighted the requirement of feature extraction, ensemble techniques, and testing of real-world datasets in designing effective intrusion detection system (IDS) solutions.

The results show that ensemble techniques and hybrid models can be utilized together to enhance the detection rate at maintaining lower computational complexity. Further, comparison against available literature suggests that using deep learning techniques in association with feature optimization is required to generate scalable and efficient security for IoT networks.

More efforts must be focused on addressing other challenges, i.e., data heterogeneity, real-time detection in resource-limited situations, and the incorporation of explainable AI techniques to enhance the interpretability and reliability of IDS solutions. The application of these sophisticated techniques can safeguard the IoT system from upcoming threats, making its sustainable development and users' confidence possible.

References

[1] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," Sensors (Switzerland), vol. 19, no. 9, doi: 10.3390/s19091977, 2019.

[2] N. A. Hussien, S. A. A. A. Alsaidi, I. K. Ajlan, M. F. M. Firdhous, and H. T. H. S. Al Rikabi, "Smart shopping system with RFID technology based on internet of things," International Journal of Interactive Mobile Technologies, vol. 14, no. 4, pp. 17–29, 2020, doi: 10.3991/ijim.v14i04.13511.

[3] A. Alamer, B. Soh, and D. E. Brumbaugh, "MICKEY 2.0.85: A secure and lighter MICKEY 2.0 cipher variant with improved power consumption for smaller devices in the IoT," *Symmetry (Basel)*, vol. 12, no. 1, Jan. 2020, doi: 10.3390/SYM12010032.

[4] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, Institute of Electrical and Electronics Engineers Inc., Sep. 2018, pp. 163–168. doi: 10.1109/TrustCom/BigDataSE.2018.00034.

[5] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions," 2022, *Hindawi Limited*. doi: 10.1155/2022/4016073.

[6] A. G. Ayad, N. A. Sakr, and N. A. Hikal, "A hybrid approach for efficient feature selection in anomaly intrusion detection for IoT networks," *Journal of Supercomputing*, Dec. 2024, doi: 10.1007/s11227-024-06409-x.

[7] A. Odeh and A. Abu Taleb, "Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection," *Applied Sciences (Switzerland)*, vol. 13, no. 21, Nov. 2023, doi: 10.3390/app132111985.

[8] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in *2021 26th International Conference on Automation and Computing:System Intelligence through Automation and Computing, ICAC 2021, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.23919/ICAC50006.2021.9594183.*

[9] M. A. Bouke and A. Abdullah, "An empirical assessment of ML models for 5G network intrusion detection: A data leakage-free approach," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 8, Jun. 2024, doi: 10.1016/j.prime.2024.100590.

[10] B. I. Farhan and A. D. Jasim, "Survey of Intrusion Detection Using Deep Learning in the Internet of Things," Iraqi Journal for Computer Science and Mathematics, vol. 3, no. 1, pp. 83–93, 2022, doi: 10.52866/ijcsm.2022.01.01.009.

[11] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends," Mar. 01, 2024, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/s24061968.

[12] A. Raj and S. D. Shetty, "IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey," Jan. 01, 2022, Springer. doi: 10.1007/s11277-021-08958-3.

[13] R. A. Radouan Ait Mouha, "Internet of Things (IoT)," Journal of Data Analysis and Information Processing, vol. 09, no. 02, pp. 77–101, 2021, doi: 10.4236/jdaip.2021.92006.

[14] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," May 01, 2022, Elsevier Ireland Ltd. doi: 10.1016/j.cosrev.2022.100467.

[15] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions," Jul. 01, 2020, MDPI AG. doi: 10.3390/electronics9071177.

[16] L. Santos, C. Rabadão, and R. Gonçalves, "Intrusion Detection Systems in Internet of Things A literature review."

[17] S. Tsimenidis, T. Lagkas, and K. Rantos, "Deep Learning in IoT Intrusion Detection," Journal of Network and Systems Management, vol. 30, no. 1, Jan. 2022, doi: 10.1007/s10922-021-09621-9.

[18] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[19] T. Al-Shurbaji et al., "Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review", doi: 10.1109/ACCESS.2023.1120000.

[20] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," 2021, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2021.3129336.

[21] S. El Hajla, E. Mahfoud, Y. Maleh, and S. Mounir, "Attack and anomaly detection in IoT Networks using machine learning approaches," in Proceedings - 10th International Conference on Wireless Networks and Mobile Communications, WINCOM 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/WINCOM59760.2023.10322991.

[22] Y. Otoum and A. Nayak, “AS-IDS: Anomaly and Signature Based IDS for the Internet of Things,” Journal of Network and Systems Management, vol. 29, no. 3, Jul. 2021, doi: 10.1007/s10922-021-09589-6.
[23] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 1, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
[24] T. Talaei Khoei and N. Kaabouch, “A Comparative Analysis of Supervised and Unsupervised Models for Detecting Attacks on the Intrusion Detection Systems,” Information (Switzerland), vol. 14, no. 2, Feb. 2023, doi: 10.3390/info14020103.
[25] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.
[26] M. Aljanabi, M. A. Ismail, and A. H. Ali, “Intrusion detection systems, issues, challenges, and needs,” International Journal of Computational Intelligence Systems, vol. 14, no. 1, pp. 560–571, 2021, doi: 10.2991/ijcis.d.210105.001.
[27] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, “Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey,” IEEE Access, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.
[28] O. Ogundairo, “Machine Learning Algorithms for Intrusion Detection Systems,” 2024. [Online]. Available: https://www.researchgate.net/publication/382917701
[29] G. Karatas, O. Demir, and O. K. Sahingoz, “Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset,” IEEE Access, vol. 8, pp. 32150–32162, 2020, doi: 10.1109/ACCESS.2020.2973219.
[30] E. M. Roopa Devi and R. C. Suganthe, “Enhanced transductive support vector machine classification with grey wolf optimizer cuckoo search optimization for intrusion detection system,” in Concurrency and Computation: Practice and Experience, John Wiley and Sons Ltd, Feb. 2020. doi: 10.1002/cpe.4999.
[31] B. Yan and G. Han, “Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System,” IEEE Access, vol. 6, pp. 41238–41248, Jul. 2018, doi: 10.1109/ACCESS.2018.2858277.
[32] W. Samek, G. Montavon, S. Lapuschkin, C. J. Anders, and K. R. Müller, “Explaining Deep Neural Networks and Beyond: A Review of Methods and Applications,” Proceedings of the IEEE, vol. 109, no. 3, pp. 247–278, Mar. 2021, doi: 10.1109/JPROC.2021.3060483.
[33] G. Thamilarasu and S. Chawla, “Towards deep-learning-driven intrusion detection for the internet of things,” Sensors (Switzerland), vol. 19, no. 9, May 2019, doi: 10.3390/s19091977.
[34] H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: A survey,” Oct. 01, 2019, MDPI AG. doi: 10.3390/app9204396.
[35] S. Li et al., “CRSF: An Intrusion Detection Framework for Industrial Internet of Things Based on Pretrained CNN2D-RNN and SVM,” IEEE Access, vol. 11, pp. 92041–92054, 2023, doi: 10.1109/ACCESS.2023.3307429.
[36] A. S. Qureshi, A. Khan, N. Shamim, and M. H. Durad, “Intrusion detection using deep sparse auto-encoder and self-taught learning,” Neural Comput Appl, vol. 32, no. 8, pp. 3135–3147, Apr. 2020, doi: 10.1007/s00521-019-04152-6.
[37] H. Liao et al., “A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things,” IEEE Access, vol. 12, pp. 4745–4761, 2024, doi: 10.1109/ACCESS.2023.3349287.
[38] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. A. S. Al-Rimy, “DeepIoT.IDS: Hybrid deep learning for enhancing IoT network intrusion detection,” Computers, Materials and Continua, vol. 69, no. 3, pp. 3946–3967, 2021, doi: 10.32604/cmc.2021.016074.
[39] I. H. Sarker, “Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective,” SN Comput Sci, vol. 2, no. 3, May 2021, doi: 10.1007/s42979-021-00535-6.
[40] Widad K. Mohammed, Mohammed A. Taha, Haider D. A. Jabar, and Saif Ali Abd Alradha Alsaidi, “Object Detection Techniques: A Review,” Wasit Journal of Computer and Mathematics Science, vol. 2, no. 3, pp. 59–68, Sep. 2023, doi: 10.31185/wjcms.165.
[41] L. Ashiku and C. Dagli, “Network Intrusion Detection System using Deep Learning,” in Procedia Computer Science, Elsevier B.V., 2021, pp. 239–247. doi: 10.1016/j.procs.2021.05.025.
[42] S. M. Kasongo, “An advanced intrusion detection system for IIoT Based on GA and tree based algorithms,” IEEE Access, vol. 9, pp. 113199–113212, 2021, doi: 10.1109/ACCESS.2021.3104113.

[43] R. A. Disha and S. Waheed, “Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique,” Cybersecurity, vol. 5, no. 1, Dec. 2022, doi: 10.1186/s42400-021-00103-8.

[44] H. C. Altunay and Z. Albayrak, “A hybrid CNN + LSTMbased intrusion detection system for industrial IoT networks,” Engineering Science and Technology, an International Journal, vol. 38, Feb. 2023, doi: 10.1016/j.jestch.2022.101322.

[45] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System,” Internet of Things (Netherlands), vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100936.

[46] J. B. Awotunde et al., “An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks,” Applied Sciences (Switzerland), vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042479.

[47] T. T. H. Le, R. W. Wardhani, D. S. Catur Putranto, U. Jo, and H. Kim, “Toward Enhanced Attack Detection and Explanation in Intrusion Detection System-Based IoT Environment Data,” IEEE Access, vol. 11, pp. 131661–131676, 2023, doi: 10.1109/ACCESS.2023.3336678.

[48] N. Sayed, M. Shoaib, W. Ahmed, S. N. Qasem, A. M. Albarrak, and F. Saeed, “Augmenting IoT Intrusion Detection System Performance Using Deep Neural Network,” Computers, Materials and Continua, vol. 74, no. 1, pp. 1351–1374, 2023, doi: 10.32604/cmc.2023.030831.

[49] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in IoT networks,” Digital Communications and Networks, vol. 10, no. 1, pp. 205–216, Feb. 2024, doi: 10.1016/j.dcan.2022.08.012.

[50] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, “Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models,” Systems Science and Control Engineering, vol. 12, no. 1, 2024, doi: 10.1080/21642583.2024.2321381.

[51] M. M. Inuwa and R. Das, “A comparative analysis of various machine learning methods for anomaly detection in cyberattacks on IoT networks,” Internet of Things (Netherlands), vol. 26, Jul. 2024, doi: 10.1016/j.iot.2024.101162.

[52] Y. Xiao, Y. Feng, and K. Sakurai, “An Efficient Detection Mechanism of Network Intrusions in IoT Environments Using Autoencoder and Data Partitioning,” Computers, vol. 13, no. 10, Oct. 2024, doi: 10.3390/computers13100269.

[53] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, “Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning,” J Big Data, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00892-y.

[54] H. R. Sayegh, W. Dong, and A. M. Al-madani, “Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data,” Applied Sciences (Switzerland), vol. 14, no. 2, Jan. 2024, doi: 10.3390/app14020479.