

Review of Deep Learning - Based Intrusion Detection Systems for IoT Environments

Muhammad Mamman Kontagora¹ and Bartholomew Idoko²

¹Center for Cyber Space Studies, Nasarawa State University, Keffi, Nigeria.

²Department of Computer Science, Federal Polytechnic Ohodo, Enugu, Nigeria.
bartholomew.idoko@fedpod.edu.ng¹, mohakontagora14@gmail.com²

Abstract

This review examines the use of deep learning techniques in Intrusion Detection Systems (IDS) for IoT environments. The rapid expansion of IoT devices has led to increased vulnerability to cyber-attacks, making effective IDS crucial. The paper provides an overview of deep learning models such as Convolutional Neural Networks (CNNs) and others, highlighting their application in detecting network intrusions. The study aims at reviewing the effectiveness of deep learning models in IoT environments, identify the technical challenges and limitations, and suggest future research directions. Key findings from the different DL techniques such as CNNs, Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Generative Adversarial Networks (GANs) shows a high level of robustness in mitigating against different kinds of cyber threats. In IoT environment, data could appeared imbalanced in most cases which could lead to biased models that perform poorly in detecting rare but critical security threats. However, creating standardized and comprehensive datasets for IoT intrusion detection can facilitate better benchmarking and comparison of different deep learning approaches. While deep learning models significantly improve detection accuracy and adaptability, they also face challenges related to computational constraints, data quality, and vulnerability to adversarial attacks. The review underscores the need for lightweight and robust models that can operate within the limited resources of IoT devices. The review concludes that ongoing advancements in deep learning, such as federated learning and edge computing, hold promise for enhancing IDS in IoT. However, further research is necessary to address existing gaps, including the development of standardized datasets and improved resilience against sophisticated cyber threats.

Keywords: Intrusion, systems, IoT security, Deep learning, Environments, Adversarial, attacks, Federated learning.

1. Introduction

IoT represents a major Information Technological (IT) advancement, linking a wide variety of devices via the internet. These electronics equipment's, which include varieties of things from common household items to highly sophisticated systems, are embedded with sensors and software that allow them to communicate and share data. This network of interconnected devices has transformed multiple industries such as hospitality, aviation, health and factories by facilitating real-time data collection and analysis (Kiran et al., 2020). However, the rapid growth of IoT networks also presents significant security challenges, mainly due to the varied and widespread nature of these connected devices (Alsoufi et al., 2021). Robust Intrusion Detection Systems (IDSs) are now essential for information protection due to the rise in cyberattack threats on key infrastructures that are monitored by networked systems (Otoum et al., 2020). The complexity, sophistication, and difficulty of detecting cyber-attacks that endanger vital infrastructures and industrial processes have increased. These cyber- attacks have the potential to affect people' and employees' health and safety in addition to causing significant financial losses (Nader et. al., 2016). New

kinds of cyber-attacks that are not present in their databases are not detectable by conventional intrusion detection systems (IDS). In order to give industrial systems, the best defense against cyber-attacks, IDS require supplementary assistance (Nader et. al., 2016). An intrusion detection system (IDS) can be used to construct the detective control mechanism of the Internet of Things (IoT) security architecture. The IDS's detection accuracy is significantly impacted by the network traffic data used to construct it using a machine-learning or deep learning algorithm (Kannadhasan et al., 2022).

IDS are essential tools used in securing the cyberspace, tasked with monitoring network traffic to detect malicious activities that might result to a threat (Nandanwar & Katarya, 2024). IDS are generally categories into signature-based and anomaly-based. Signature-based IDS use predefined patterns of known threats for detection, while anomaly-based IDS identify deviations from normal behavior, making them more effective against new, unknown attacks. The implementation of IDS in IoT environments is challenging due to the diverse nature of devices and the dynamic network traffic (Otoum et al., 2022; Awajan, 2023). However, several researchers have keyed into the application of Artificial Intelligence (AI) such as Deep Learning (DL), Machine Learning (ML), Neural Networks (NN), etc to enhance the performance of intrusion detection systems.

DL which is a type of ML, make use of NN with multiple layers to model complex data patterns. These networks process data through various layers, each extracting higher-level features, enabling DL models to perform tasks such as image recognition, natural language processing, and anomaly detection with high accuracy (Otoum, Liu, & Nayak, 2022). The ability to manage large datasets and identify intricate patterns makes deep learning particularly useful for cybersecurity applications, including IDS in IoT environments (Awajan, 2023). In IoT, the diversity and volume of data make deep learning's automatic feature extraction and learning capabilities highly advantageous (Kalnoor & Gowrishankar, 2021).

Relevance of Security & DL in Intrusion Detection System for IoT

Security is a paramount concern in IoT environments. Due to the large number of connected devices, there are many opportunities for prospective cyber-attacks, making IoT networks particularly vulnerable to intrusion (Saba et al., 2022). Compromised IoT devices can lead to severe consequences, such as illegal access to private information, interruption of essential services, and in certain situations, physical harm (Alsoufi et al., 2020). Therefore, ensuring robust security measures is essential to protect the integrity, confidentiality, and availability of IoT systems (Asharf et al., 2020).

DL techniques enhance the effectiveness of IDS in IoT by providing sophisticated methods to analyze vast and varied data. While traditional IDS methods like signature-based and anomaly-based systems have their strengths, deep learning offers superior adaptability and precision in detecting novel threats. This is crucial in IoT environments, where the variety of devices and the dynamic nature of network traffic create unique security challenges (Thamilarasu & Chawla, 2019; Van Huong & Hung, 2019).

The Paper's Objective & Structure

This paper aims to review the application of deep learning techniques to improve IDS for IoT environments. A comprehensive review of current literatures was carried out to identify existing challenges, and analyses cutting-edge DL models used in IDS. The remaining part of paper is organized thus: Section 2 gives the detail background on IoT and its security challenges. Section 3 explores various types of IDS and their relevance to IoT. Section 4 focuses on the integration of DL techniques in IDS, highlighting recent

advancements and their effects. Section 5 presents a comparative analysis of different DL models used in IDS for IoT. Finally, Section 6 look at the insights into future research directions and potential improvements in this field of study.

2. Related Works

IoT connects a wide range of devices, from simple sensors to advanced computing systems, all communicating via the internet. This architecture generally consists of three layers: the perception layer (sensors and actuators), the network layer (data transmission), and the application layer (data processing and utilization) (Kiran et al., 2020). While IoT brings numerous advantages, it also introduces significant security risks. Common threats include unauthorized access, data breaches, denial of service (DoS) attacks, and botnet attacks (Nandanwar & Katarya, 2024). These vulnerabilities are exacerbated by the diverse nature of IoT devices and their limited computational resources, which often lack strong security measures (Thamilarasu & Chawla, 2019).

Traditional Intrusion Detection Systems

Traditional Intrusion Detection Systems (IDS) have been widely used to protect network environments by monitoring traffic and identifying potential threats. These systems are generally categorized into two types: signature-based and anomaly-based IDS. Signature-based IDS detect malicious activities by looking for predefined patterns or signatures of known threats. However, they often fail to identify new or unknown attacks (Van Huong & Hung, 2019). On the other hand, anomaly-based IDS create models of normal network behavior and flag deviations as potential intrusions. This method can detect novel threats but usually has higher false positive rates due to the dynamic nature of network traffic (Susilo & Sari, 2020).

Challenges of Traditional IDS in IoT Environments

Despite their effectiveness in traditional IT settings, traditional IDS face considerable challenges in IoT networks. A significant limitation is the vast diversity and resource constraints of IoT devices, which complicates the implementation and maintenance of conventional IDS (Shareena et al., 2021). The heterogeneous nature of these devices and their often limited processing capabilities mean that traditional IDS solutions may not be feasible or effective in many IoT scenarios. Consequently, new approaches are needed to address these unique challenges and enhance the security of IoT environments

Additionally, the massive scale and distributed nature of IoT networks result in a substantial volume of data that traditional IDS may not be equipped to handle efficiently (Wani & Khaliq, 2021). Furthermore, the dynamic and often ephemeral connections between IoT devices pose challenges in maintaining up-to-date and comprehensive intrusion detection models (Otoum et al., 2022).

To address these limitations, recent research has focused on leveraging advanced ML techniques, specifically, DL to enhance the capabilities of IDS for IoT environments such as the examination of many well-known semi-supervised anomaly detection algorithms utilizing publicly accessible power system cyberattack datasets in order to determine which ones performed the best (Qi et al., 2021). Reliable intrusion detection techniques are essential for maintaining the privacy and confidentiality of data in computer networks. Effective intrusion detection is hampered by the complexity and large volume of data, since standard models have trouble processing high-dimensional data, which lowers accuracy (Olufemi, et. al.,

2024). The two methods by which the intrusion detection system operates are anomaly-based detection and signature-based detection. The data training procedure has an impact on the quality of the machine learning model that is produced in anomaly-based detection. Creating a suitable model to describe the dataset is the largest obstacle to machine learning techniques (Akbar & Ahmad, 2021). In order to construct a suitable model, this study suggests a hybrid machine learning approach that combines the feature selection method, which represents supervised learning, with the data reduction method, which represents unsupervised learning (Akbar & Ahmad, 2021). DL models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can automatically learn complex patterns and relationships from extensive datasets, which makes them ideal for detecting sophisticated cyber threats in IoT networks (Awajan, 2023). Research has revealed that DL-based IDS can achieve higher detection accuracy and lower false positive rates compared to conventional methods (Kalnoor & Gowrishankar, 2021).

Despite these advancements, several challenges remain in the deployment of DL-based IDS in IoT environments. These include deep learning models' computing requirements, the requirement for sizable labeled datasets for training, and the capacity to adjust to the constantly changing landscape of cyber threats (Tsimenidis et al., 2022). Future research must continue to address these challenges to develop more effective and scalable intrusion detection solutions for IoT networks (Khan et al., 2021).

Previous work on IDS using deep learning in IoT

Numerous studies have investigated the use of DL techniques to improve IDS for IoT environments. Tsimenidis, Lagkas, and Rantos (2022) explored the application of convolutional neural networks (CNNs) for identifying anomalies in IoT traffic. They found that CNNs, which are good at recognizing spatial hierarchies in data, effectively detected patterns indicative of security threats in IoT networks. Similarly, Khan et al. (2021) developed a DL-based IDS for MQTT-enabled IoT, showing that it achieved higher detection accuracy compared to traditional methods.

Fu et al. (2021) proposed robust DL frameworks for IDS, emphasizing their adaptability and resilience to various attack vectors. In another study, Verma et al. (2021) presented a machine learning ensemble approach that combined several models to boost the robustness and accuracy of IDS in IoT networks. Banaamah and Ahmad (2022) also demonstrated the effectiveness of deep learning algorithms in distinguishing between normal and malicious activities within IoT environments, highlighting the potential of these techniques to enhance IoT security.

Elnakib et al. (2023) developed an enhanced DL model for IoT intrusion detection, showcasing its superior performance in handling complex and dynamic data streams typical of IoT networks. Research by Ravi, Chaganti, and Alazab (2022) focused on feature fusion techniques in deep learning, which integrate multiple feature sets to improve detection accuracy.

Moreover, studies have also examined the integration of optimization techniques with DL for IDS. For example, Fatani et al. (2021) utilized enhanced transient search optimization to fine-tune DL models for better performance. Simon et al. (2022) proposed a hybrid approach combining DL with conventional methods to leverage the strengths of both.

Overall, the body of research indicates that DL significantly enhances the capability of IDS in IoT environments, offering higher detection accuracy, adaptability, and resilience against evolving threats.

Continued advancements in this field are crucial for developing robust security solutions that can keep pace with the rapid evolution of IoT technologies.

Deep learning has revolutionized various fields in computing, especially in recognizing complex patterns. Among the most impactful techniques are Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Generative Adversarial Networks (GANs).

CNN are designed for data structures that resemble grids, like pictures. In order to extract features from input data, they employ convolutional layers through local receptive fields, making them highly effective for spatial data analysis (Sharma et al., 2023).

RNN are tailored for sequential data. They retain information from earlier inputs, allowing them to model temporal dynamics. This capability makes RNNs ideal for analyzing time-series data, such as network traffic over time (Musleh et al., 2023).

LSTM networks, a subtype of RNNs, can learn long-term dependencies and overcome the vanishing gradient problem seen in standard RNNs. This makes them useful for tasks requiring long-term context, such as identifying patterns in network logs (Smys et al., 2020).

GAN consist of two competing neural networks; a discriminator that assesses data and a generator that produces it. This setup allows GANs to generate high-quality synthetic data, which can be used to substitute training datasets for IDS (Aldweesh, Derhab, & Emam, 2020).

Application of DL Methods in IDS

Using DL techniques in IDS for IoT environments has yielded promising results, enhancing detection accuracy and reducing false positives.

CNNs have been successfully applied to IDS to analyze network traffic data by treating it as images, identifying patterns of benign and compromised instances. Sharma et al. (2023) demonstrated that CNNs could achieve high detection rates for various attack types in IoT networks.

RNNs and LSTMs are particularly suitable for IoT environments with sequential data. They capture temporal patterns and dependencies in network traffic, crucial for detecting sophisticated attacks. For instance, Musleh et al. (2023) showed significant improvements in anomaly detection using LSTM networks compared to traditional methods.

GANs have addressed the issue of imbalanced datasets in IDS. GANs can generate synthetic attack data to balance the training datasets. This approach was explored by Aldweesh, Derhab, and Emam (2020), who found that using GAN-generated data improved the performance of their IDS models.

Further advancements involve combining these techniques to leverage their strengths. For example, hybrid models that integrate CNNs and RNNs can simultaneously capture spatial and temporal features of network data. This integration provides a more comprehensive understanding of the data, leading to better detection performance (Sharma et al., 2023).

Research by Ibitoye, Shafiq, and Matrawy (2019) explored the use of CNNs for feature extraction and LSTMs for sequence learning, which resulted in a robust IDS capable of handling the dynamic nature of IoT environments. This hybrid approach ensures that both the immediate context and long-term dependencies of network traffic are considered, improving the detection accuracy.

Moreover, studies like those by Sicato et al. (2020) have shown that deep learning-based IDS can adapt to new types of attacks with minimal human intervention. Their systems were able to learn from new data continuously, enhancing their ability to detect previously unseen threats. This adaptability is crucial for IoT environments, which are constantly evolving with new devices and technologies.

Islam et al. (2021) emphasized the importance of feature selection in enhancing IDS performance. By using deep learning techniques to automatically select and extract the most relevant features from raw data, their IDS achieved higher accuracy with lower computational costs. This approach is particularly beneficial for resource-constrained IoT devices.

Another important aspect is the robustness of IDS against adversarial attacks. Liu and Lang (2019) highlighted the vulnerability of deep learning models to such attacks, where malicious entities subtly alter input data to evade detection. To counter this, Ragab and Sabir (2022) proposed integrating adversarial training into the IDS development process, where the models are trained with both normal and adversarial examples to improve their resilience.

In practice, implementing these advanced deep learning techniques requires careful consideration of the IoT environment's specific characteristics and constraints. Ferrag et al. (2020) pointed out that real-time detection capabilities are essential for effective IDS in IoT. Therefore, models need to be optimized for both accuracy and speed, ensuring timely responses to threats.

Additionally, Jothi and Pushpalatha (2023) discussed the need for scalability in IDS. As IoT networks can grow rapidly, IDS must be able to scale with the network to maintain their effectiveness. Their work on distributed deep learning models for IDS shows promise in addressing this scalability challenge.

Finally, Qiu et al. (2020) explored the use of semi-supervised learning techniques to reduce the dependency on labeled data. In many IoT scenarios, obtaining labeled data for all potential threats is impractical. Semi-supervised models can leverage a small amount of labeled data along with a larger set of unlabeled data to improve their detection capabilities.

Case studies or Examples

Several case studies highlight the practical application and effectiveness of deep learning models in IoT intrusion detection. For instance, Liu and Lang (2019) conducted a study using CNNs for anomaly detection in smart home IoT networks. Their model achieved high accuracy in identifying malicious activities while maintaining low false positive rates, demonstrating the potential of CNNs in real-world applications.

Ragab and Sabir (2022) implemented an LSTM-based IDS for industrial IoT networks, focusing on detecting attacks in time-series data. Their system successfully identified a range of attacks, including DoS and data exfiltration, showcasing the effectiveness of LSTMs in monitoring industrial environments.

Ferrag et al. (2020) presented a hybrid IDS combining CNNs and RNNs for a smart grid environment. By integrating spatial and temporal analysis, their model improved detection rates and reduced false alarms. This hybrid approach proved effective in managing the complex data patterns of smart grids.

Jothi and Pushpalatha (2023) explored a GAN-enhanced IDS for healthcare IoT networks. The GAN-generated synthetic data helped address the imbalance between normal and attack data, enhancing the model's ability to detect rare and sophisticated attacks. This case study highlighted the value of GANs in improving IDS performance in data-sensitive environments like healthcare.

In another example, Qiu et al. (2020) developed an IDS for IoT networks using semi-supervised learning. By combining a small amount of labeled data with a large set of unlabeled data, their model effectively detected intrusions with reduced reliance on extensive labeled datasets. This approach is particularly useful in IoT environments where labeled data is scarce.

Abdel-Basset et al. (2021) implemented a DL-based IDS in a smart city context. Their system utilized feature selection techniques to enhance detection accuracy while minimizing computational overhead. The study demonstrated the feasibility of deploying deep learning models in large-scale, real-time IoT environments.

Parimala and Kayalvizhi (2021) focused on securing fog-to-things environments using an ensemble learning-based IDS. By integrating multiple deep learning models, their system achieved robust performance against a variety of attack vectors, illustrating the benefits of ensemble approaches in complex IoT networks.

Illy et al. (2019) applied a CNN-based IDS to monitor network traffic in a smart agriculture setting. Their model effectively identified anomalies in data collected from various sensors, ensuring the security and integrity of the agricultural IoT infrastructure.

Shah et al. (2023) developed a deep learning-based IDS to protect against malicious smart contracts in IoT blockchain networks. Their model successfully detected fraudulent activities, highlighting the potential of deep learning in securing blockchain-based IoT applications.

Lastly, Almiani et al. (2020) implemented a deep recurrent neural network (RNN) for IDS in smart city infrastructures. Their system demonstrated high accuracy in detecting various attack types, showcasing the potential of RNNs in managing the dynamic and complex data of urban IoT systems.

These case studies collectively underscore the versatility and effectiveness of deep learning techniques in enhancing IDS for various IoT environments. They demonstrate that with the right model selection and optimization, DL can significantly improve the security and resilience of IoT networks.

3. Methodology

In the realm of evaluating IDS for IoT environments, a set of common metrics stands out as the go-to for assessing performance. These include accuracy, precision, recall, the F1-score, and the Receiver Operating Characteristic (ROC) curve. Accuracy, as a metric, gauges the ratio of correctly identified instances, encompassing both true positives and true negatives, over the total instances. Precision, on the other hand, zeroes in on the ratio of true positive results among all positive detections produced by the model. When it

comes to recall, also known as sensitivity, it quantifies the portion of actual positives correctly identified by the model. Now, the F1-score enters the scene as the harmonic mean of precision and recall, serving as a balance between the two. Lastly, the ROC curve sketches out the true positive rate against the false positive rate, with the area under the curve (AUC) shedding light on the model's knack for distinguishing between classes (Shah et. al., 2023).

The analyses of the evaluation matrices becomes important when considering deep learning and machine learning from the perspective of IDS in IoT. The measures provide pathway in assessing the result of the tested IDS, the best performing algorithms, and the applicability of such algorithms. The following is a brief review of the commonly used performance measures:

Accuracy

Accuracy is the purest of the measures, the simplest method that shows the ratio of the correctly identified both normal and anomalous instances to the total number of instances. It is given by:

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

The parameters are defined thus:

TP is the True Positives,
 TN is the True Negatives,
 FP is the False Positives,
 FN is the False Negatives.

Strengths: It presents the unified measure of group performance or comparative measure between two or more groups.

Limitations: It may be proactively inclined in imbalanced datasets containing an evidently greater number of normal instances as compared to the anomalous ones (García-Teodoro et al., 2009).

Precision and Recall

Precision measures the proportion of correctly identified anomalies to the total number of instances classified as anomalies:

$$Precision = \frac{TP}{TP + FP}$$

Recall (or Sensitivity) measures the proportion of actual anomalies that are correctly identified:

$$Recall = \frac{TP}{TP + FN}$$

These metrics are comparatively very useful in those scenarios where the number of false positive and false negatives must be compromised.

Strengths: Precision enables the identification of the degree to which identified anomalies are relevant while, recall targets identifying all actual anomalies.

Limitations: It is still important to consider both to get the whole picture because problematic use of one may influence the other (Sokolova & Lapalme, 2009).

F1-Score

The F1-Score is the harmonic mean of Precision and Recall and is used to balance them:

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Strengths: Encapsulates Precision and Recall in one number thus making it easier to compare different models.

Limitations: It may not accurately expose the trade-off area of Precision and Recall in the cases of highly skewed datasets (Powers, 2011).

Area under Receiver Operating Characteristic Curve (AUC-ROC)

Plotting the true positive rate against the false positive rate at different probability thresholds yields the AUC-ROC, a graphical depiction of a binary classifier system's diagnostic capacity. At different threshold values, the True Positive Rate (TPR) against the False Positive Rate (FPR) could be plotted thus:

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

This index AUC has a scale or range of 0 to 1 where AUC is closer to 1 is equal to optimal model performance.

Strengths: Offers an overall measure of the model's ability of classifying patterns as belonging to one class or the other.

Limitations: It does not use real market values (Bradley, 1997).

Confusion Matrix

This offers a thorough analysis of the predicted and actual classifications, allowing for the calculation of the metrics:

Table 1. Confusion Matrix (Source: Shah et al., 2023).

	Predicted Normal	Predicted Anomalous
Actual Normal	TN	FP
Actual Anomalous	FN	TP

Strengths: This provides a clear and detailed description of the performance of the classification models.

Limitations: It needs further analysis and inspection and it's not measured with one specific indicator (Sokolova & Lapalme, 2009).

Importance of DL Metric

Each of these metrics bears significant weight in evaluating IDS performance. Accuracy, while providing a broad measure of correctness, can sometimes paint a skewed picture if the data is imbalanced. Precision steps in, particularly in scenarios where the cost of false positives is hefty, ensuring that the IDS keeps false alarms at bay. Recall, meanwhile, takes the spotlight in situations where overlooking a threat is simply not an option, underscoring the need for the detection of all actual attacks. The F1-score comes as a unified metric that strikes a balance between precision and recall, proving especially handy when class distribution is uneven. Lastly, the ROC curve and AUC delve into the realm of trade-offs between sensitivity and specificity across various threshold settings, aiding in the selection of the optimal model threshold.

In the landscape of existing studies, these metrics reign supreme, serving as the backbone for evaluating and comparing the performance of deep learning models tailored for IDS in IoT setups. For instance, Sharma et al. (2023) leaned on accuracy, precision, recall, and the F1-score to assess their anomaly-based network intrusion detection system, showcasing its prowess in pinpointing various attack types with notable precision and recall. Similarly, Musleh et al. (2023) harnessed similar metrics to scrutinize their feature extraction-based IDS, spotlighting the model's equilibrium in terms of precision and recall, as evidenced by a lofty F1-score.

Smys, Basar, and Wang (2020) used accuracy and the ROC curve to evaluate their hybrid IDS, providing a comprehensive analysis of the model's overall performance and its ability to discriminate between normal and malicious traffic. Aldweesh, Derhab, and Emam (2020) emphasized the importance of the F1-score in their survey of anomaly-based IDS, noting its usefulness in balancing precision and recall for models dealing with imbalanced datasets.

In their analysis of adversarial attacks, Ibitoye, Shafiq, and Matrawy (2019) used precision and recall to highlight the robustness of their IDS under attack conditions. Sicato et al. (2020) and Islam et al. (2021) both utilized a combination of these metrics to demonstrate the effectiveness of their deep learning models in real-time intrusion detection scenarios, emphasizing the need for high recall to ensure comprehensive threat detection.

Liu and Lang (2019) and Ragab and Sabir (2022) focused on the F1-score and ROC curve in their evaluations, illustrating the models' ability to maintain high detection rates while minimizing false positives. Ferrag et al. (2020) used these metrics to compare different deep learning approaches, providing insights into their relative strengths and weaknesses in IDS applications.

Different deep learning models have been applied to Intrusion IDS in IoT environments, each offering distinct advantages and limitations. CNN for instance, are well-suited for spatial data analysis. Sharma et al. (2023) demonstrated that CNNs could efficiently identify network traffic patterns associated with various attack types. However, CNNs might struggle with sequential data, where temporal relationships are crucial.

RNN and their advanced variants like Long Short-Term Memory (LSTM) networks address this issue by retaining information across time steps. Musleh et al. (2023) showed that LSTMs could capture long-term

dependencies in network traffic, enhancing the detection of sophisticated attacks. Nonetheless, RNNs and LSTMs can be computationally intensive and may require significant resources, which could be a limitation in resource-constrained IoT environments.

GAN offer a unique approach by generating synthetic data to balance training datasets, improving IDS performance in detecting rare attacks. Aldweesh, Derhab, and Emam (2020) found that using GANs for data augmentation significantly boosted the accuracy of IDS models. However, GANs can be complex to train and require careful tuning to avoid issues like mode collapse.

4. Results and Discussion

Hybrid models that combine CNNs and RNNs have been explored to leverage the strengths of both. For example, Ibitoye, Shafiq, and Matrawy (2019) used CNNs for feature extraction and LSTMs for sequence learning, creating a robust IDS capable of handling both spatial and temporal data. This approach ensures comprehensive analysis but may increase computational complexity.

As shown in Table 2, there are several models commonly studied, and this table group's common machine learning techniques for Internet-instrumented devices, with measurement statistics from past studies.

Table 2. Performance Comparison of Anomaly Detection Techniques (Source: Bush et al., 2023)

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
CNN	0.94	0.90	0.88	0.89	0.92
GAN	0.91	0.87	0.91	0.93	0.90
RNN	0.96	0.94	0.91	0.92	0.95
LSTM	0.87	0.85	0.81	0.82	0.89

Implementing DL-based IDS in IoT environments presents several technical challenges. One major issue is the heterogeneity of IoT devices and protocols, which complicates the design of a unified IDS framework (Jothi & Pushpalatha, 2023). Additionally, IoT networks often involve a high volume of data traffic with diverse characteristics, requiring sophisticated models capable of real-time processing and analysis (Qiu et al., 2020). Ensuring the robustness of these systems against adversarial attacks, where attackers manipulate input data to deceive the model, is another significant concern (Abdel-Basset et al., 2021).

Data quality and availability are critical for training effective deep learning models for IDS. In IoT environments, data can be noisy, incomplete, or imbalanced, with a disproportionate amount of normal traffic compared to intrusion events (Parimala & Kayalvizhi, 2021). This imbalance can lead to biased models that perform poorly in detecting rare but critical security threats. Furthermore, obtaining labeled data for training is challenging due to the vast number of IoT devices and the dynamic nature of network traffic (Illy et al., 2019). This scarcity of labeled data necessitates the use of semi-supervised or unsupervised learning techniques, which can be less effective than supervised learning (Shah et al., 2023).

IoT devices typically have limited computational resources, including processing power, memory, and battery life. These constraints pose severe issues for deploying DL models, which are often computationally intensive (Alsoufi et al., 2020). The need for real-time intrusion detection further exacerbates this issue, as models must process data quickly and efficiently. Implementing lightweight models or using edge computing to distribute the computational load can help mitigate these constraints, but achieving the right balance between model complexity and resource usage remains a challenge (Asharf et al., 2020).

Deep learning-based IDS also require continuous updates to adapt to new types of attacks, necessitating regular retraining and model updates. This process can be resource-intensive and may not be feasible for all IoT devices, particularly those deployed in remote or resource-constrained environments (Nandanwar & Katarya, 2024). Additionally, maintaining the security and integrity of the IDS itself is crucial, as any compromise could result to noticeable flaws within the IoT network (Thamilarasu & Chawla, 2019).

Implementing DL-based IDS in IoT environments introduces significant security and privacy concerns. The possibility of adversarial attacks, in which malevolent individuals alter input data to trick the IDS, is one significant concern. (Qiu et al., 2020). These attacks can significantly compromise the reliability of the detection system. Additionally, the collection and processing of huge volume of data raise privacy issues, as sensitive information from IoT devices can be exposed or misused if not properly secured (Abdel-Basset et al., 2021). Ensuring data confidentiality and integrity is crucial, yet challenging, given the distributed and heterogeneous nature of IoT networks (Parimala & Kayalvizhi, 2021).

Present study on DL-based IDS for IoT also faces several general limitations. One major limitation is the lack of standardized datasets for training and evaluating IDS models. Several researches utilize diverse datasets, making it difficult to compare results across different approaches (Illy et al., 2019). Moreover, the dynamic and evolving nature of IoT environments means that models trained on existing data may quickly become outdated as new types of attacks emerge (Shah et al., 2023). This necessitates continuous updates and retraining of models, which can be resource-intensive. Another limitation is the computational cost associated with deep learning models.

IoT devices typically have limited processing power and memory, which makes deploying complex deep learning models challenging (Alsoufi et al., 2020). While methods like model compression and edge computing can mitigate these issues to some extent, they are not always sufficient to overcome the inherent limitations of IoT hardware (Asharf et al., 2020). Furthermore, the integration of DL-based IDS into existing IoT infrastructure requires significant effort in terms of compatibility and interoperability. Many IoT devices and systems are not designed with advanced security features in mind, making it difficult to retrofit them with sophisticated IDS solutions (Nandanwar & Katarya, 2024).

Although recent advancements in the area of IDS for IoT are showcasing promising trends, a significant stride involves the fusion of artificial intelligence (AI) and machine learning (ML) to bolster detection accuracy and flexibility. An interesting development is the rise of federated learning, enabling models to undergo training across multiple devices sans the need for data transfer to a central server. This innovative approach not only safeguards privacy but also curtails bandwidth consumption (Jothi & Pushpalatha, 2023). Moreover, the integration of blockchain technology for fortifying IoT data transactions and enhancing IDS reliability is gaining momentum (Qiu et al., 2020). Blockchain serves as an immutable ledger ensuring the genuineness and incorruptibility of data across IoT networks.

Potential Improvements in Deep Learning Techniques

Furthermore, there's a focus on refining deep learning techniques to elevate IDS efficacy. Strategies such as model pruning, quantization, and knowledge distillation are being investigated to mitigate the computational requirements of deep learning models, rendering them more adaptable for IoT devices with limited resources (Thamilarasu & Chawla, 2019)

Despite significant advancements, several research gaps and open issues remain. One major gap is the issue with regards inaccessibility of standard datasets for benchmarking IDS performance in IoT environments (Almiani et al., 2020). This makes it difficult to compare the effectiveness of different approaches. Moreover, current models often struggle with the dynamic nature of IoT networks, where devices frequently join and leave, and traffic patterns continuously evolve (Uğurlu & Doğru, 2019). The scalability of IDS solutions is another critical issue, as IoT networks can grow rapidly, and models must be able to handle increasing volume of data and devices. Additionally, the need for real-time detection capabilities requires models that can quickly process and analyze data without significant delays.

Further studies should concentrate more on several key areas to address the current limitations and enhance IDS effectiveness for IoT environments. Firstly, developing more efficient and lightweight deep learning models that can operate within the computational constraints of IoT devices is crucial (Thamilarasu & Chawla, 2019). Techniques like edge computing and federated learning should be further explored to distribute computational tasks and improve latency. Secondly, creating standardized and comprehensive datasets for IoT intrusion detection can facilitate better benchmarking and comparison of different approaches (Almiani et al., 2020).

Another important area is enhancing the robustness of IDS against adversarial attacks. Research should focus on developing advanced adversarial training techniques and exploring new defense mechanisms to make IDS more resilient (Qiu et al., 2020). Additionally, integrating blockchain technology with IDS can provide secure and tamper-proof data logging, improving the overall security and reliability of IoT networks (Jothi & Pushpalatha, 2023).

5. Conclusion

This review has highlighted the significant advancements in IDS for IoT environments using DL techniques. Key DL techniques like CNNs, RNNs, LSTMs, and GANs have been discussed for their robustness in mitigating against different kinds of cyber threats. Comparative analyses show that while these models offer substantial improvements in accuracy and detection capabilities, they also face challenges related to computational demands and data quality. Additionally, the evaluation metrics that are frequently applied play an important role in investigating IDS performance.

The emerging techniques of DL in IDS for IoT is a promising yet evolving field. While current models provide enhanced detection accuracy and adaptability, they are not without limitations. Issues such as high computational requirements, the need for extensive and high-quality labeled datasets, and vulnerability to adversarial attacks remain significant obstacles. Despite these challenges, the continuous advancement in deep learning algorithms and techniques is expected to address many of these issues, making IDS more robust and efficient in the future (Jothi & Pushpalatha, 2023; Qiu et al., 2020).

For practitioners, the implementation of deep learning-based IDS offers a proactive approach to securing IoT environments. It is essential to consider the computational constraints of IoT devices and opt for optimized models that balance performance and resource usage. For researchers, there are ample opportunities to explore novel deep learning techniques and improve the robustness of IDS against emerging threats. Further studies could leverage on developing lightweight models, enhancing data privacy through federated learning, and creating standardized datasets for comprehensive evaluation (Thamilarasu & Chawla, 2019; Van Huong & Hung, 2019). In conclusion, while deep learning-based IDS for IoT environments are still in their nascent stages, their potential to transform IoT security is undeniable. Ongoing research and innovation will be key to overcoming current limitations and fully realizing the benefits of these advanced detection systems.

References

- Abdel-Basset, M., Hawash, H., Chakraborty, R. K., & Ryan, M. J. (2021). Semi-supervised spatiotemporal deep learning for intrusions detection in IoT networks. *IEEE Internet of Things Journal*, 8(15), 12251-12265.
- Akbar A. & Ahmad T. (2021). A hybrid machine learning method for increasing the performance of network intrusion detection systems. *Journal of Big Data* 8:142. Pp. 2-8
<https://doi.org/10.1186/s40537-021-00531-w>.
- Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189, 105124.
- Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, 101, 102031.
- Alsoufi, M. A., Razak, S., Siraj, M. M., Ali, A., Nasser, M., & Abdo, S. (2020, December). Anomaly intrusion detection systems in iot using deep learning techniques: a survey. In *International conference of reliable information and communication technology* (pp. 659-675). Cham: Springer International Publishing.
- Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied sciences*, 11(18), 8383.
- Altan, G. (2021). SecureDeepNet-IoT: A deep learning application for invasion detection in industrial Internet of things sensing systems. *Transactions on Emerging Telecommunications Technologies*, 32(4), e4228.
- Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, 9(7), 1177.
- Aversano, L., Bernardi, M. L., Cimitile, M., Pecori, R., & Veltri, L. (2021). Effective anomaly detection using deep learning in IoT systems. *Wireless Communications and Mobile Computing*, 2021, 1-14.
- Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, 12(2), 34.
- Banaamah, A. M., & Ahmad, I. (2022). Intrusion detection in iot using deep learning. *Sensors*, 22(21), 8417.
- Bush, I. & Abiyev, R. (2023). 'Introduction to Machine Learning and IoT' Machine Learning and the Internet of Things in Education, *Studies in Computational Intelligence* 1115, Pp. 1-7.
https://doi.org/10.1007/978-3-031-42924-8_1

- Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, 14(1), 41.
- Elnakib, O., Shaaban, E., Mahmoud, M., & Emara, K. (2023). EIDM: Deep learning model for IoT intrusion detection systems. *The Journal of Supercomputing*, 79(12), 13241-13261.
- Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A., & Lu, S. (2021). IoT intrusion detection system using deep learning and enhanced transient search optimization. *IEEE Access*, 9, 123448-123464.
- Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419.
- Fu, X., Zhou, N., Jiao, L., Li, H., & Zhang, J. (2021). The robust deep learning-based schemes for intrusion detection in internet of things environments. *Annals of Telecommunications*, 76(5), 273-285.
- Ibitoye, O., Shafiq, O., & Matrawy, A. (2019, December). Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In *2019 IEEE global communications conference (GLOBECOM)* (pp. 1-6). IEEE.
- Idrissi, I., Azizi, M., & Moussaoui, O. (2020, October). IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. In *2020 Fourth international conference on intelligent computing in data sciences (ICDS)* (pp. 1-10). IEEE.
- Illy, P., Kaddoum, G., Moreira, C. M., Kaur, K., & Garg, S. (2019, April). Securing fog-to-things environment using intrusion detection system based on ensemble learning. In *2019 IEEE wireless communications and networking conference (WCNC)* (pp. 1-7). IEEE.
- Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., ... & Cho, G. H. (2021). Towards Machine Learning Based Intrusion Detection in IoT Networks. *Computers, Materials & Continua*, 69(2).
- Jasim, A. D. (2022). A survey of intrusion detection using deep learning in internet of things. *Iraqi Journal For Computer Science and Mathematics*, 3(1), 83-93.
- Jothi, B., & Pushpalatha, M. (2023). WILS-TRS—A novel optimized deep learning based intrusion detection framework for IoT networks. *Personal and Ubiquitous Computing*, 27(3), 1285-1301.
- Kalnoor, G., & Gowrishankar, S. (2021). IoT-based smart environment using intelligent intrusion detection system. *Soft Computing*, 25(17), 11573-11588.
- Kannadhasan, S., Nagarajan, R. & Thenappan, S. (2022). Intrusion Detection Techniques based Secured Data Sharing System for Cloud Computing using MSVM. 9th International Conference on Computing for Sustainable Global Development (INDIACom). 978-93-80544-44-1/22/\$31.00_c 2022 IEEE.
- Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., ... & Buchanan, W. J. (2021). A deep learning-based intrusion detection system for MQTT enabled IoT. *Sensors*, 21(21), 7016.
- Kiran, K. S., Devisetty, R. K., Kalyan, N. P., Mukundini, K., & Karthi, R. (2020). Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, 171, 2372-2379.
- Kumar, V., Das, A. K., & Sinha, D. (2021). UIDS: a unified intrusion detection system for IoT environment. *Evolutionary intelligence*, 14(1), 47-59.
- Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, 9(20), 4396.
- Malibari, A. A., Alotaibi, S. S., Alshahrani, R., Dhahbi, S., Alabdan, R., Al-wesabi, F. N., & Hilal, A. M. (2022). A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment. *Sustainable Energy Technologies and Assessments*, 52, 102312.

- Manhas, J., & Kotwal, S. (2021). Implementation of intrusion detection system for internet of things using machine learning techniques. *Multimedia Security: Algorithm Development, Analysis and Applications*, 217-237.
- Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. (2023). Intrusion detection system using feature extraction with machine learning algorithms in IoT. *Journal of Sensor and Actuator Networks*, 12(2), 29.
- Nader, P., Honeine, P., Beuseroy, P., (2016). Detection of Cyberattacks In a Water Distribution System Using Machine Learning Techniques. ISBN: 978-1-4673-7504-7 ©2016 IEEE.
- Nandanwar, H., & Katarya, R. (2024). Deep learning enabled intrusion detection system for Industrial IOT environment. *Expert Systems with Applications*, 249, 123808.
- Olufemi, J., Sulaiman, O., Michael Favour Edafeajiroke, M. & Kazeem, A. An Enhanced Network Intrusion Detection System using Dimensionality Reduction Techniques. *Kasu Journal of Computer Science* Vol. 1 No. 4 [December, 2024], pp. 689-701 <https://doi.org/10.47514/kjcs/2024.1.4.001>
- Otoum, S., Kantarci, B. & Mouftah, H. (2020). A Novel Ensemble Method for Advanced Intrusion Detection in Wireless Sensor Networks. *IEEE Conference on Automation Science and Engineering*. 978-1-7281-5089-5/20/\$31.00 ©2020 IEEE. Pp. 511-533
- Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: A deep learning-based intrusion detection framework for securing IoT. *Transactions on Emerging Telecommunications Technologies*, 33(3), e3803.
- Parimala, G., & Kayalvizhi, R. (2021, January). An effective intrusion detection system for securing IoT using feature selection and deep learning. In *2021 international conference on computer communication and informatics (ICCCI)* (pp. 1-4). IEEE.
- Qaddoura, R., M. Al-Zoubi, A., Faris, H., & Almomani, I. (2021). A multi-layer classification approach for intrusion detection in iot networks based on deep learning. *Sensors*, 21(9), 2987.
- Qi, R.; Rasband, C.; Zheng, J.; Longoria, R. (2021) Detecting Cyber Attacks in Smart Grids Using Semi-Supervised Anomaly Detection and Deep Representation Learning. <https://doi.org/10.3390/info12080328>
- Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., & Qiu, M. (2020). Adversarial attacks against network intrusion detection in IoT systems. *IEEE Internet of Things Journal*, 8(13), 10327-10335.
- Ragab, M., & Sabir, M. F. S. (2022). Outlier detection with optimal hybrid deep learning enabled intrusion detection system for ubiquitous and smart environment. *Sustainable Energy Technologies and Assessments*, 52, 102311.
- Ravi, V., Chaganti, R., & Alazab, M. (2022). Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks. *IEEE Internet of Things Magazine*, 5(2), 24-29.
- Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering*, 99, 107810.
- Sahar, N., Mishra, R., & Kalam, S. (2021). Deep learning approach-based network intrusion detection system for fog-assisted iot. In *Proceedings of international conference on big data, machine learning and their applications: ICBMA 2019* (pp. 39-50). Springer Singapore.
- Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., ... & Marina, V. (2023). Deep learning-based malicious smart contract and intrusion detection system for IoT environment. *Mathematics*, 11(2), 418.
- Shareena, J., Ramdas, A., & AP, H. (2021). Intrusion detection system for iot botnet attacks using deep learning. *SN Computer Science*, 2(3), 1-8.
- Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. *Computers and Electrical Engineering*, 107, 108626.

- Sicato, J. C. S., Singh, S. K., Rathore, S., & Park, J. H. (2020). A comprehensive analyses of intrusion detection system for IoT environment. *Journal of Information Processing Systems*, 16(4), 975-990.
- Simon, J., Kapileswar, N., Polasi, P. K., & Elaveini, M. A. (2022). Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm. *Computers and Electrical Engineering*, 102, 108190.
- Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, 2(04), 190-199.
- Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information*, 11(5), 279.
- Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, 19(9), 1977.
- Tsimenidis, S., Lagkas, T., & Rantos, K. (2022). Deep learning in IoT intrusion detection. *Journal of network and systems management*, 30(1), 8.
- Uğurlu, M., & Doğru, İ. A. (2019, September). A survey on deep learning based intrusion detection system. In *2019 4th International Conference on Computer Science and Engineering (UBMK)* (pp. 223-228). IEEE.
- Van Huong, P., & Hung, D. V. (2019, December). Intrusion detection in IoT systems based on deep learning using convolutional neural network. In *2019 6th NAFOSTED conference on information and computer science (NICS)* (pp. 448-453). IEEE.
- Verma, P., Dumka, A., Singh, R., Ashok, A., Gehlot, A., Malik, P. K., ... & Hedabou, M. (2021). A novel intrusion detection approach using machine learning ensemble for IoT environments. *Applied Sciences*, 11(21), 10268.
- Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access*, 7, 41525-41550.
- Wani, A., & Khaliq, R. (2021). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). *CAAI Transactions on Intelligence Technology*, 6(3), 281-290.
- Yaras, S., & Dener, M. (2024). IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. *Electronics*, 13(6), 1053.
- Zhong, M., Zhou, Y., & Chen, G. (2021). Sequential model based intrusion detection system for IoT servers using deep learning methods. *Sensors*, 21(4), 1113.