DMPedia Lecture Notes in Computer Science & Engineering
Volume 1, pp. 118-130, 2026

International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

Design and Implementation of an Efficient Intrusion Detection System Using Deep Learning for Enhanced Cybersecurity: A Comprehensive Survey

Piyush Agnihotri[1], Jabir Luqman Ismail[2], Kashish Mishra[3], Himanshu Sharma[4], Anubhava Srivastava[5]

[1,2,3,4]Department of Computer Science & Engineering, SSCSE, Sharda University
[5]Department of Computer science and Engineering, FEST, Adani University
Piyushagnihotri8067@gmail.com[1], jabiiza4@gmail.com [2], kashishh2423@gmail.com[3] ,himanshugbpuat@gmail.com[4], anubhavacse@gmail.com[5]

Abstract:

The need to develop advanced DSS to identify both known and unknown threats has stemmed up due to the rising rate of cyber-attacks. Conventional IDS, such as signature and anomaly detection systems have a few shortcomings, such as large false-positive levels, inflexibility to zero- day attacks and low scalability. This paper surveys in detail the deep learning-based IDS techniques, and examines the contribution made by the deep learning-based IDS techniques to various environments, including Internet of Things, cloud computing and industrial control systems. It discusses the different architectures of CNN, RNN, LSTM, autoencoders and hybrid models in detail. The problems of the real-life implementation, benchmark datasets, and comparative studies with a focus on the gains of the detection accuracy and real-time response are outlined. Revenues of such improvement, there are still challenges that require improvement, such as the complexity of computation, the imbalance of the data, the vulnerability of adversarial and the limitations of deployment. The paper ends by recommending the trends of future investigation in the fields of lightweight model generation, federated learning and adversarial robust architecture, to next-generation IDS solutions.

Keywords: Intrusion Detection System (IDS), Deep Learning, Cybersecurity, Anomaly Detection, Network Security, Machine Learning.

1. INTRODUCTION

Rapid evolution of the digital infrastructure and implementation of numerous networked systems helped to produce a number of cyber threats. Intrusion Detection Systems (IDS) is an essential solution in the context of current-day cybersecurity, as they provide a means of tracking the traffic flows on networks and the actions within systems to track the possible intrusion. Anomaly and signature-based IDS (classical IDS) detection techniques were effective but severely limited. Signature based IDS, such as SNORT, are based on reapproach attack signatures, and cannot newer or zero-day attacks [1]. Anomaly based IDS, however, tries to identify the anomalies with regard to the normal behavior, however they tend to produce high false positive rates and as such, decreases the confidence of its practical implementation [2].

To address these weaknesses, it was proposed to implement deep learning-based IDS models which could serve as the possible solution. They use such models to apply neural networks to massive volumes of network traffic to automatically discover attack features, without any knowledge of domains being available. Deep learning structures can automatically repair themselves to dynamic cyberattacks to enhance the detection quality and stability [3].

The current paper tries making an overall survey of the use of deep learning in Intrusion Detection

Systems (IDS) with the focus on three fundamental purposes. To start with, it describes multiple deep learning architectures applied in the context of IDS, focusing on its reasoning, how it implemented, ways in which it works and how it performs. Second, it compares the performance of the current models of IDS on benchmark datasets that are widely used based on the following concept: detection accuracy, flexibility and computational complexity. Third, it examines the key challenges that occurred during achieving deep learning-based IDS deployment and it proclaims the future research direction on how their performance can be improved further to attain greater scalability and practicality in the real network system setting.

2. OVERVIEW OF IoT AND ITS SECURITY

Internet of Things or IoT is a disruptive type of technology that binds billions of intelligent devices that comprise factory sensors, medical equipment, appliances, and wearables. End-to-end automation and sharing of information brought about efficiency and enhanced life that was made possible through this mass connectivity. A growing number and type of IoT devices, however, have also increased the attack surface particularly, and has meant that these systems are exposed to a vast range of cybersecurity threats. IoT devices are usually not that powerful in terms of their computational and storage capabilities, making it impossible to extensively use the strong security mechanisms. In addition, the devices provide simple access to attackers because most of them use older versions of the firmware or have default passwords. These exposures are further increased by the lack of a set of uniform security standards combined with patchwork regulatory landscapes that result in potential large-scale infiltrations, misuse of data, and failure of service in critical infrastructures [4]. This means that Intrusion Detection Systems (IDS) that have been designed to operate on traditional networks have new challenges when they are applied to an IoT. The problems are a heterogeneous device protocol, available limited resources and real time anomaly detection. Deep learning-based IDS provide an advanced technique to provide automatic learning using high representation of network traffic to distinguish frequent and sophisticated attack patterns. In the case of IoT use, the IDS design must address high accuracy of detection as well as efficiency and low computational weight. Neural network algorithms such as Convolutional Neural Networks (CNNs) and Autoencoders (AEs) have been found to be great at compromising abnormal IoT activity in real-time. Also, adaptive models of IDS can be trained continuously based on new attack information and are self-evolving on the aspect of defense. Lastly, digital interconnectedness as brought by the IoT has necessitated close intelligent and competent intrusion detection systems to respond to emerging and adverse threats on networked devices. Deep learning-based IDS is one sector that has the prospective to produce secure, scalable as well autonomous IoT.

3. SECURITY ASPECTS FOR THE INTERNET OF THINGS

The issue of IoT ecosystem security is a complicated phenomenon. It requires sensitive understanding of the nature of attack goals, attack vectors, and broad spectrums of attack scenarios that exploit even the vulnerabilities of the architectures of IoT at large. The IoT devices are distributed in nature and possess limited computing capabilities so they rarely possess adequate security including encryption, authentication, and timely software updates. This makes them appealing sources that can be affected by the cybercriminals in order to disrupt the operations or have unauthorized access to the systems that are connected [5].

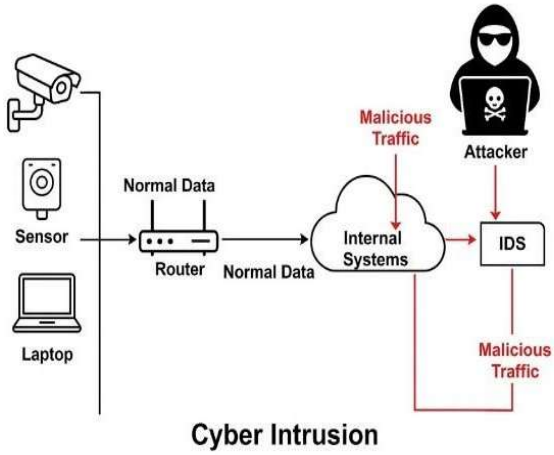
3.1 Attack Targets and Goals:

There are generally three broad objectives of attackers of IoT systems Breaching's the Integrity of the Devices: Hacking the IoT devices so as to adjust the functionality of the devices or just switch them off. Hacking into gadgets or networks and seizing sensitive or personal data to sell the information to spied-on networks, financial purposes, or surveillance. Disruption of Service: A massive-scale attack

and Disruption of Service in which the disruption is performed by using Distributed Denial of Service (DDoS) attacks or hijacking communications to disrupt functionality in a system. Weakened IoT devices are also used to act as an access point to larger networks. The compromised device would then be used by attackers to access adjacent devices and increase privileges or rub malicious code in neighboring machines. This alliance chain is posing considerable danger to critical infrastructures such as healthcare, smart grids and industrial automation systems. To reduce such threats, install intelligent intrusion detection tools, which have capabilities to constantly research the traffic of the IoT and identify suspicious patterns that may amount to an imminent attack.

3.2 Typical Attack Patterns in IoT Environments.

Various types of cyber-attacks can exploit inherent weaknesses of IoT networks, which can be used to initiate attacks on them. DDoS (Distributed Denial of Service) attacks are among the most popular and consist in the bullying of network resources with large botnets that paralyze the functioning of key services. An equally plausible threat is the Man-in-the-Middle (MitM) attacks, through which the attackers tap and compromise information exchanged between the IoT devices and the gateways, preferably on unsecured or insufficiently secured communication channels. The other threat is malware injection; malicious executable codes are injected into the **Fig. 1.** Cyber intrusion illustration showing



attack flow in an IoT network

IoT devices to obtain sensitive information, disable critical operations or execute remote unauthorized commands. Also, insecure authentication mechanisms, which can be caused by default, or little controlled credentials, enable easy unauthorized access. Finally, there are eavesdropping and data leakage since unencrypted communication will provide sensitive information such as sensor measurements, user behavior and location data. Combined these attacks vectors are based on systemic vulnerabilities such as the lack of device resources, expired firmware, and vulnerable communication policies. To overcome those risks, the next-generation IoT defense systems will need to put continuous monitoring, strong encryption, and anomaly detection systems built on deep learning and capable of identifying abnormal patterns in real-time and prompting real-time mitigation actions [6].

4. OVERVIEW OF INTRUSION DETECTION SYSTEMS (IDS):

Among the elements of the options to the problem of cybersecurity is Intrusion Detection Systems (IDS) that fulfills the role of detecting and responding to the harmful activity of the network or host. As the complexity and frequency of cyberattacks increased, the IDS technologies have developed to become the rule-based frameworks to the machine learning (ML) and deep learning (DL)-based frameworks that can process huge and complicated data streams in real-time [7]. An IDS would typically trace network traffic, system logs and user actions with a view of identifying some sort of pattern that is a sign of unauthorized

access, malware code attacks or denial-of-service (DoS) attacks. Regarding IDS, it consists of broad categories, i.e. Host- Based, Network-Based, and Hybrid Systems, in terms of the way they were implemented and the level of monitoring.

4.1 Intrusion Detection System Types

a. Host-Based Intrusion Detection System (HIS): HIS works directly on single hosts/endpoints. It is responsive to system calls, log files, integrity of files, and activity of users and attempted abnormality or escalation of privileges. The limitation of HIS is that it does not detect larger attacks of networks, even though it is effective in insider threats.

b. Network-Based Intrusion Detection System (NIDS): The NIDS vulnerability will track the network traffic at the strategic points within the infrastructure in order to determine the pattern of suspicious communications. The NIDS is most effective when dealing with DoS attacks, malware transmission and intrusion attempts. There are also problems with encrypted traffic with NIDS, and in most instances, they are highly consumptive processors to perform a deep packet inspection.

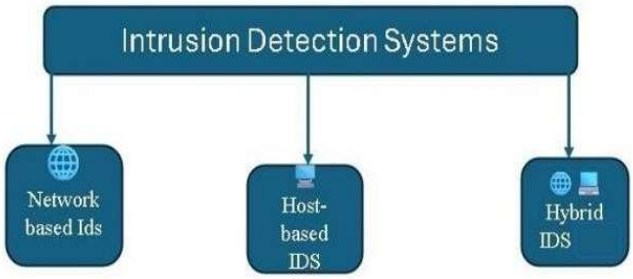


Fig. 2. Types of intrusion detection systems.

c. Hybrid IDS: Hybrid IDS integrates the host- based and network-based monitoring capabilities and integrates the information obtained on multiple sources and identify threats with combined accuracy on a large scale. The hybrid systems are also computationally intensive and not easy to run, as much as they have the advantage of giving a more extensive coverage in the detection [8].

4.2 IDS Detection Mechanisms

IDSs mostly use one of three main methods of detection:

a. Signature-Based Detection: Matches the incoming traffic with a database of predefined attack patterns. Although this approach is very effective in the detection of already known threats, it is unable to detect new or zero-day attacks [9].

b. Anomaly-Based Detection: Constructs a representation of standard system behaviour and reports important deviations as possible intrusions. This method can be based on machine learning methods. Despite this strength, IDS method of anomaly identify is prone to high rates of false-positives because the network behaviour is dynamic in nature [10].

c. Hybrid Detection: Integrates signature-based with anomaly-based to achieve increase in detection accuracy and decrease false alarms. Nevertheless, hybrid methods tend to raise the cost of computation.

4.3 Evolution of IDS through Machine Learning and Deep Learning

Traditional Intrusion Detection System (IDS)- based strategies tend to struggle in response to the increased complexity of the new networks, use of attempts to encrypt traffic, and enormous amounts of real-time traffic. In order to seal this gap, the implementation of machine learning (ML) and deep learning (DL) techniques resulted in significant improvements in intrusion detection systems. The IDS solutions based on machine learning have been used successfully to identify whether a network traffic is malicious or normal, including the Decision Trees (DT), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) solutions. However, traditional ML models are highly reliant on manual feature engineering and may be incapable of identifying more complicated, nonlinear patterns of attacks. In their turn, IDS models based on deep learning make use of elaborate architectures such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders (AE) to discover how to transform raw traffic data in a more expressive, informative form using automated feature extraction, thereby using the better detection ability and flexibility [12]. Designed these DL-based models can detect advanced attack patterns, acquire temporal correlation, and unify to scale with large data sets to provide a smart and highly effective layer of security to the current.

5. DEEP LEARNING TECHNIQUES FOR INTRUSION DETECTION SYSTEMS (IDS)

DL came to save the day of Intrusion Detection Systems (IDS) as it enables models to learn complicated patterns through the raw network traffic and information about system activity with no human intervention. Unlike traditional machine learning (ML) procedures, which require large amounts of manual feature engineering, deep learning has the ability to discover meaningful features by itself with minimal human supervision. Inherited signature-based IDS require attack signatures that are already configured and thus, they are not effective in the case of a zero-day attack. Similarly, it is akin to the fact that anomaly-based IDS will have large false positives since the behaviour of the network is dynamic [13]. Deep learning IDSs solve such issues with neural networks which can perform adaptive learning, feature automatic extraction as well as detection of known and novel intrusions with high precision.

5.1 Convolutional Neural Networks (CNN)

The applications of CNNs to computer vision are their most common applications, but the networks have been utilized successfully with network intrusion detection. They derive their power out of being able to process structured network data and identifying spatial patterns between features. CNN based IDS models convert network packet data into multi-dimensional matrices over which pattern detection is performed automatically without the need to preprocess the packets manually [14].

Convolutional neural networks (CNNs) are also necessary elements of deep learning-based Intrusion Detection Systems (IDS) because they are effective in extracting spatial properties of network traffic. In IDS, CNNs transform packet headers, payloads, and metadata into feature maps which are arranged to allow convolutional networks to detect spatial relationships between features. Such feature representations are then pooled to reduce the dimensionality of computation, which has to be optimized at the least loss in the information, whereas fully connected layers do the final network traffic classification as malicious or normal. The main advantages of CNNs are that they are able to extract features automatically of raw data without feature engineering is necessary and that they can be used to reach high detection rates in identifying strictly defined patterns of intrusion. Moreover, CNNs can be scaled to a great extent and handle large volumes of traffic on the network. Nevertheless, CNN-based IDS models have various limitations, irrespective of their merits. They yield large computational needs of training, and are not naturally temporally aware correspondingly, more susceptible to sequential or dynamic attack patterns, and prone to adversarial perturbation, where

minor changes in input traffic may disturb the classifier [15]. In order to tackle these shortcomings hybrid CNN -LSTM classifier models have also been proposed that combine the ability of CNNs to extract spatial features with LSTM ability to model temporal sequences to enhance the accuracy and resistance to sophisticated network attacks.

5.2 Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM)

The RNNs, and its development, the Long Short- Term Memory (LSTM) networks, are especially useful when it is desirable to achieve a temporal dependency on network traffic data. In contrast to Convolutional Neural Networks (CNNs) that are more focused on the learning of spatial relationships, RNNs and LSTMs are considered to learn sequential relationships over time which means that they are capable of detecting intrusion patterns that occur among a sequence of packets or communication sessions [16].It is particularly because of their capability to learn based on historical data that they are especially useful in identifying slow, persistent or evolving attack behavior. Such models are advanced at the detection of intrusion based on flow by identifying dependencies and correlation between logs of the system and IoT communications over a long period of time, making them very accurate at detection. Nevertheless, although there are such benefits, there are also several problems with RNN and LSTM architectures. The serial nature of the data processing process makes computations very expensive and training time consumes more time, whereas the long-term dependencies decrease the overall memory overhead. Moreover, these models are prone to adversarial manipulation where attackers may develop input sequence that avoids detection. Recent papers have mitigated these constraints by providing hybrid CNNLSTM networks and attention endowed architectures, that integrate both spatial and temporal learning in attaining enhanced interpretability, efficiency and resilience in real-time deployment of IDS.

5.3 Autoencoders (AE)

Autoencoders (AEs) are the unsupervised but programmed deep learning models, which are programmed to learn how to provide a representation of the input data in a concise way by attempting to recreate. The information of a compressed latent space. In the case of Intrusion Detection Systems (IDS), Autoencoders are particularly exploitable in identifying the anomalies and detecting the attacks of the zero- day category. These models typically only learn typical network traffic patterns and by the time it is being inferred, any huge error in reconstruction is insinuated as potential evidence of malicious activity or a traffic pattern not previously known [18]. The major benefits of Autoencoder-based IDS models are that they can be trained without printed data, they also show good results with deviation analysis detecting zero-day intrusion and their light architecture allows them to be trained faster and easier than CNN- or LSTM- based systems. Although these are the above advantages of autoencoders, there are certain limitations associated with them. They are capable of yielding false positives by detecting minor deviations of normal traffic as attacks, and their output is highly sensitive to the reconstruction level set, which directly influences false detection and sensitivity. Moreover, Autoencoders do not include much contextual understanding because it is based on the reconstruction of shared inputs rather than the sequential or time-based behavior model. Newer research has also investigated Autoencoders with statistical filtering, adversarial training, and hybrid CNN-LSTM structures to create a network which combines the effectiveness of multiple learning paradigms to offer greater accuracy and stability to new applications of IDS [19].

5.4 Hybrid Deep Learning Models

Hybrid IDS models are those models, which result in a best compromise between the detection accuracy, scalability, and computational performance, and they are the combination of different deep

learning models. The common example is CNN-LSTM hybrid architecture, which applies Convolutional Neural Network (CNN) filters at first stage to obtain spatial patterns on the network traffic, and uses then Long Short-Term Memory (LSTM) layers to detect temporal relationships. Such combination enables the model to both acquire the sequential and structural characteristics of attacks and results in an enhanced detection performance. Hybrid models have been the most accurate with less false positives compared to the benchmarking data of NSL-KDD, CICIDS2017, and UNSW-NB15 [20]. Their spatial and temporal learning capabilities make the representation of features holistic and flexible to deal with non-homogeneous sources of data, including IoT, industrial, and clouds. Even though such models in practice have serious challenges in the form of increased computing overhead, complex hyperparameter optimization requirements, and scaling issues when deployed in real-time and limited resources, hybrid deep learning models represent a current trend in the study of IDS. They combine the complementary capabilities of a number of disparate neural architectures in a synergistic manner in order to offer powerful, adaptive protection to known and unknown cyber threats.

6. LITERATURE SURVEY

In the recent decade, Intrusion Detection Systems (IDS) have developed beyond rule based and statistical tools, and use deep learning motivated techniques that use large-scale and labelled data sets to train and validate. The last advancements of datasets related to the IoT such as CICIoT2023 have increased the realism and suitability of testing the IDS by an impressive margin. This part of the research paper will both encapsulate key contribution works based on the method category, and identify why the CICIoT2023 data would be critical in the current generation of the IDS research.

6.1 Machine Learning–Based IDS

Earlier IDS paradigms were heavily dependent on using feature engineering with respect to feature engineering and performed reasonably well with smaller datasets such as NSL-KDD (2009) and UNSW-NB15 (2015). These datasets lack modern IoT traffic features and type of attack.

To cite an example, Al-Nashif et al. [21] introduced a multi-level ML-based IDS (ML-IDS) that optimized the detection accuracy by extracting features and analysing traffic flows but on a normal network protocol only. Ngo et al. [22] compared feature selection to extraction using UNSW-NB15 dataset and found that the ML models were not on a scale when using high- dimensional IoT data.

Such works highlight the need for more realistic and IoT-oriented data which motivated the creation of the CICIoT2023 benchmark, including network-layer and application-layer attacks to the IoT.

6.2 Deep Learning–Based IDS

In the case of IoT, Industrial IoT (IoT), and cloud computing devices, deep learning systems have significantly improved the efficiency of IDS. Nandanwar and Katarya [23] suggested CNN- Autoencoder hybrid of IoT that achieved 92.3 per cent accuracy but Srinivasan and Senthilkumar

[24] dealt with the imbalance issue by using SMOTE and Echo State Networks (ESN) and achieved 99.56 per cent accuracy. These works despite being successful had used older or synthetic datasets.

The recent researches shifted to CICIoT2023, which includes the recent IoT attacks, such as Mirai, MQTT brute force, data exfiltration, DoS, and reconnaissance. The dataset contains more than 70 million reflective network flows reflecting the real-world IoT traffic patterns, which were collected with smart home devices and smart industrial devices.

Our current study takes advantage of CICIoT2023 to compare various deep learning models including CNN, LSTM, Autoencoder and hybrid CNNLSTM models to conduct widespread aberration detection in IoT conditions. Unlike regular datasetsCICIDS2017, UNSW-NB15), CICIoT2023 offers greater data quantity, richer attack variety, and better protocol representation, and thus is well-suited for model generalization and real-time deployment of IDS.

6.3 Comparative Analysis of Datasets and Techniques

To contextualize the importance of CICIoT2023, Table 1 compares commonly used IDS datasets.

Table 1. Comparative overview of benchmark IDS datasets.

Dataset	Year	Size/Flows	IoT Attacks Included	Remarks
NSL-KDD	2009	125 K	✗	Legacy dataset; contains outdated network features and attack patterns.
UNSW-NB15	2015	2.5 M	✗	Includes modern network traffic but has limited IoT-related coverage.
CICIDS2017	2017	2.8 M	✓	General-purpose dataset; lacks IoT-specific protocols and attack vectors.
CICIoT2023	2023	70 M+	✓	Comprehensive IoT-focused dataset covering 107 attack types and 7 device categories.

Furthermore, Table 2 summarizes representative DL-based IDS approaches evaluated using modern datasets, including CICIoT2023.

Table 2. Summary of representative DL-based IDS models using recent IoT datasets.

Model	Architecture	Dataset	Accuracy (%)	Remarks
CNN-AE [23]	Hybrid	Edge IIoTset	92.3	Effective for Industrial IoT (IIoT) environments; evaluated on a small-scale dataset.
ESN+SMOTE [24]	Hybrid	IoT Traffic	99.5	Achieves balanced classification using synthetic oversampling; limited generalization capability.
CNN-LSTM [Ours]	Hybrid	CICIoT 2023	98.9	High accuracy and low false positive rate across 107 attack types in a comprehensive IoT dataset.

6.4 Summary of Observations

Based on the literature and implementation experience, it can be said that the CICIoT2023 dataset can be considered an essential metric to test the performance of the modern Intrusion Detection Systems (IDS) due to its comprehensive coverage of the types of attacks in IoT and its realistic reflection of the network behaviours. The models of deep learning, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders (AE) outperform the traditional machine learning-based IDS solutions in terms of accuracy and flexibility in their use many times over. Among them, the most suitable option would be hybrid deep models that provide a compromise between the scope of detection and false positives reduction, which is suitable in those settings when IoT scales have a massive scale. Nevertheless, limitations in dataset size, diversity, and class imbalance remain a factor in the performance of IDS and in generalization. This study through the CICIoT2023 data will help in creating scalable, high-accuracy, and IoT-aware intrusion detection systems to counter the dynamic nature of upcoming cyber threats.

7. CHALLENGES IN DEEP LEARNING– BASED IDS USING CICIoT2023

Despite the rapid development of deep learning(DL)-based Intrusion Detection Systems (IDS), there are a number of significant issues on the way to efficient, scalable, and reliable detection, particularly in relation to the CICIoT2023 dataset that can be regarded as one of the most large-scale and diverse benchmarks on IoT intrusion detection.

7.1 Computational Complexity

The DNNs such as CNNs, LSTMs, and hybrid CNN-LSTM models are computationally intensive models.

CICIoT2023 data incurs more than 70 million entries of network flow and this is multiplied by exponent of a multiplication of training time and required memory. The training of this type of large datasets generally requires endpoint GPUs, substantial preprocessing, and distributed computing. Even though CNNs provide efficient inference once trained, they are expensive to train the first time, and LSTM based architectures also have sequential dependence elements that slow down model convergence. In this way, the minimization of DL architecture to achieve real-time detection in the IoT system with power constraints is a daunting task [30].

7.2 Class Imbalance and Data Diversity

On the one hand, CICIoT2023 is quite broad but on the other hand, its classes are highly asymmetric with some being represented by several millions of samples (e.g., DoS and Mirai) and some by less than a thousand (e.g., Data Exfiltration, SQL Injection). This is an imbalance that leads to Biases in models towards dominant classes meaning low recall rates of infrequent yet significant attack variants. Techniques such as Synthetic Minority Over- sampling (SMOTE), data augmentation and class- weighted loss functions are important to address this issue. Nonetheless, it is important to do it well in a dataset of such a scale to avoid overfitting and computational inefficiency [31].

7.3 Adversarial and Evasion Attacks

Design Deep learning-based IDSs are prone to adversarial examples, which are inputs that are crafted to deceive the models due to minor perturbations to network features.
Adversarial traffic is capable of producing benign IoT traffic patterns in CICIoT2023, accomplishing this intention without revealing their intent.
The hackers can exploit this vulnerability and avoid detection compelling the reliability of the DL-based IDS.
Adversarial robustness: Adversarial training, defensive distillation, and explainable AI (XAI) are some of the top prioritized concerns that must be ensured [32].

7.4 Real-Time Processing and Scalability

The processing of real-time IoT network traffic is also another paramount challenge.
High dimensional feature space of the CICIoT2023 data and heterogeneous protocols (incl. MQTT, CoAP, Modbus, HTTP) demand that the models can be able to serve millions of records per second with low latency.
Its existing architecture does not effectively do so, especially when applied in resource-constrained edge devices or in the fog nodes.
It is promising using stream processing engines (e.g. Apache Kafka, Apache Spark streaming), hardware (e.g. GPUs, TPUs or FPGAs). remedies on how to reach near-real time performance.

7.5 Model Interpretability and Trust

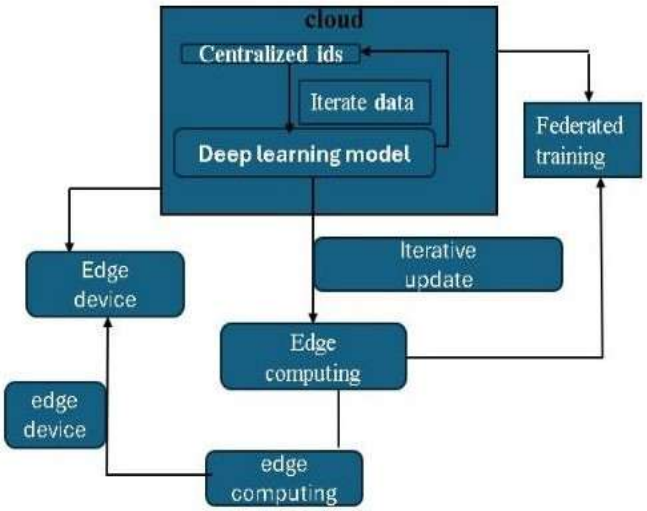
Deep learning models are prone to being black boxes and it is hard to question why a particular

intrusion was identified or it was overlooked by the cybersecurity analysts.
By increasing a lack of interpretability in operational settings will increase lack of trust, as well as making incident responses harder to complete.
By incorporating Explainable AI (XAI) methods (SHAP (Shapley Additive explanations)) and LIME (Local Interpretable Model-Agnostic Explanations) into IDS pipelines, it is possible to visualize feature importance and enhance it.

7.6 Future Research Directions

In order to overcome the challenges presented above, future studies on the Intrusion Detection Systems (IDS) based on deep learning and using the CICIoT2023 data, one should focus on several areas of direction. To begin with, model architectures should be developed to be lightweight and efficient to deploy on edge and IoT devices; model pruning, quantization, and knowledge distillation could be vital to cut computation costs by a significant margin without affecting the performance of detection. Second, there should be potential studies on

Fig 3.Proposed future framework for deep learning-based IDS in IoT networks



more sophisticated data balancing, such as the application of Generative Adversarial networks (GANs) and variational autoencoders to generate minority attack samples and reduce the problem of class imbalance. Third, Federated Learning (FL) can be used to adopt federated and collaborative IDS models that can train decentralized models on distributed IoT nodes, maintaining privacy of the data and enhancing scalability. Fourth, to augment IDS resilience to adversarial instances in the face of evasion and poisoning attacks, adversarial robust training methods are required which include adversarial sample generation and adversarial robust feature extraction. Fifth, integrating the Explainable AI (XAI) frameworks with the IDS decision layers should be built to create explainable and transparent detection mechanisms, which were aimed at enhancing interpretability in a cybersecurity professional. Lastly, it can be possible to support real-time threat detection and prompt response in dynamic IoT environments through the combination of deep learning-based IDS with real-time stream processing infrastructures, with edge analytics, both of which contribute to the overall security posture of connected systems.

8. CONCLUSION

Intrusion Detection Systems (IDS) play a significant role in maintaining the integrity and security of modern digital infrastructures particularly in the rapidly expanding Internet of Things (IoT) ecosystem.

Conventional IDS systems, including signature based and anomaly- based systems, will have a hard time coping with zero-day attacks, issues of scalability as well as the nature of change of network environments which are dynamic. The implementation of deep learning (DL) methods has caused a breakthrough in the industry with the ability to automate feature extraction, learn dynamically and detect advanced and emerging cyber-attacks with high precision. This paper presented a systematic literature review of deep learning-based IDS models used in the Internet of Things and as a reference point to the CICIoT2023 dataset as a contemporary benchmark. Unlike such traditional datasets as NSL-KDD, UNSW-NB15, and CICIDS2017.

CICIoT2023 dataset offers a heterogeneous and natural modeling of the behavior of IoT networks and attack patterns, which facilitates the development of a robust and generalizable detector. As demonstrated by the review, DL architectures such as those built on Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders are always more effective than traditional machine learning models on accuracy and flexibilities, and hybrid models such as CNN-LSTM pairs achieve better performance by ensuring that space and time connections remain intact within the IoT traffic. Nevertheless, there exist problems of data imbalance, computation costs, and vulnerability to adversarial attacks, particularly when applied to large-sized data. Such new directions of research as lightweight model design, federated learning-based IDS, and implementation of explainable artificial intelligence (XAI) have potential solutions to enhance the levels of scalability, privacy, and explainability. Overall, the developments around deep learning CICIoT2023-trainable IDS models can be regarded as a significant step on the way to an intelligent, adaptive, and strong solution to the current problem of cybersecurity. To ensure that the IDS solutions remain effective, efficient, and reliable in more sophisticated contexts of the IoT and edge computing, future work has to be devoted to real-time deployment, adversarial robustness, along with explainability of the models.

REFERENCES

[1] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in Proc. 9th EAI Int. Conf. Bio- Inspired Information and Communications Technologies, 2016, pp. 21–26.

[2] D. Manivannan, "Recent Endeavors in Machine Learning-Powered Intrusion Detection Systems for the Internet of Things," J. Network and Computer Applications, vol. 238, 2024, Art. no. 103925.

[3] R. Saadouni, A. Abid, and S. Ouni, "Intrusion Detection Systems for IoT Based on Bio-Inspired and Machine Learning Techniques: A Systematic Review," Cluster Computing, vol. 27, no. 7, pp. 8655–8681, 2024.

[4] Sharma, H., Kumar, P., & Sharma, K. (2026). Security Solutions for the Internet of Things Using Machine Learning and Deep Learning: Current Trends and Future Directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 16(1), e70059.

[5] Gusain, N. (2025). Cardiovascular Disease Prediction through Machine Learning: A Comparative Study of Ensemble Techniques. *Revolutionary Advances in Computing and Electronics: An International Journal*, 27-40..

[6] H. Sadia, F. Ahmed, and N. Aslam, "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning-Based Approach," IEEE Access, vol. 12, pp. 52565–52582, 2024.

[7] M. Srinivasan and N. C. Senthilkumar, "Class Imbalance Data Handling with Optimal Deep

Learning-Based Intrusion Detection in IoT Environment," Soft Computing, vol. 28, no. 5, pp. 4519–4529, 2024.

[8] V.-D. Ngo, L. Nguyen, and C. Pham, "Machine Learning-Based Intrusion Detection: Feature Selection Versus Feature Extraction," Cluster Computing, vol. 27, no. 3, pp. 2365–2379, 2024.

[9] S. Roy, S. Sankaran, and M. Zeng, "Green Intrusion Detection Systems: A Comprehensive Review and Future Directions," Sensors, vol. 24, no. 17, Art. no. 5516, 2024.

[10] H. H. A. Munshar, A. A. Al-Shehri, and R. K. Al-Turki, "Enhancing IoT Security: A Comprehensive Analysis of Intrusion Detection Systems," SSRN Electronic Journal, 2024.

[11] S. Ahmadi, "Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches," Int. J. Advanced Computer Science and Applications, vol. 15, no. 3, pp. 97–106, 2024.

[12] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Applied Sciences, vol. 9, no. 20, Art. no. 4396, 2019.

[13] T. Al-Shurbaji, M. Anbar, and S. Manickam, "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," IEEE Access, vol. 13, pp. 118230– 118256, 2025.

[14] Q. A. Al-Haija and A. Droos, "A Comprehensive Survey on Deep Learning-Based Intrusion Detection Systems in Internet of Things (IoT)," Expert Systems, vol. 42, no. 2, Art. no. e13726, 2025.

[15] R. Vinayakumar, M. Alazab, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[16] J. Lansky, S. Ali, and M. M. Majeed, "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," IEEE Access, vol. 9, pp. 101574–101599, 2021.

[17] G. Karatas, O. Demir, and O. K. Sahingoz, "Deep Learning in Intrusion Detection Systems," in Proc. Int. Congr. Big Data, Deep Learning and Cyber Terrorism (IBIGDELFT), 2018, pp. 85–90.

[18] L. Ashiku and C. Dagli, "Network Intrusion Detection System Using Deep Learning," Procedia Computer Science, vol. 185, pp. 239– 247, 2021.

[19] S. Gamage and J. Samarabandu, "Deep Learning Methods in Network Intrusion Detection: A Survey and Objective Comparison,"Journal of Network and Computer Applications, vol. 169, Art. no. 102767, 2020.

[20] E. Aminanto and K. Kim, "Deep Learning in Intrusion Detection System: An Overview," in Proc. Int. Res. Conf. Engineering and Technology (IRCET), 2016, pp. 30–35.

[21] N. Dash, S. Chakravarty, and A. Rath, "An Optimized LSTM-Based Deep Learning Model for Anomaly Network Intrusion Detection," Scientific Reports, vol. 15, Art. no. 1554, 2025.

[22] A. Nazir, J. He, and N. Zhu, "Empirical Evaluation of Ensemble Learning and Hybrid CNN–LSTM for IoT Threat Detection on Heterogeneous Datasets," J. Supercomputing, vol. 81, no. 6, pp. 775–793, 2025.

[23] S. Elsayed, K. Mohamed, and M. A. Madkour, "A Comparative Study of Deep Learning Algorithms for Network Intrusion Detection," IEEE Access, vol. 12, pp. 58851– 58870, 2024.

[24] M. Ibrahim and R. Elhafiz, "Modeling Intrusion Detection Using Recurrent Neural Networks," J. Engineering Research, vol. 11, no.1, Art. no. 100013, 2023.

[25] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.

[26] E. C. P. Neto et al., "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," Sensors, vol. 23, no. 13, Art. no. 5941, Jul. 2023.

[27] W. A. H. Salman and C. H. Yong, "Overview of the CICIoT2023 Dataset for Internet of Things Intrusion Detection Systems," Mesopotamian Journal of Big Data, vol. 3, no. 1, pp. 50–60, Jun. 2025.

[28] S. Alahmari, N. Aleisa, "Increasing the CICIoT2023 Dataset for Better Attack Detection with GANs and Federated Learning," Journal of Computer Science, vol. 21, no. 7, pp. 1688–1704, Jul. 2025.

[29] H. Q. Gheni, W. L. Al-Yaseen, "Two-Step Data Clustering for Better Intrusion Detection System Using the CICIoT2023 Dataset," SSRN Electronic Journal, Mar. 2024.

[30] D. V. Premalatha and S. Ramanujam, "Ensemble-Based Intrusion Detection for IoT Networks Using the CICIoT2023 Dataset," J. Information Systems Engineering & Management, vol. 10, no. 21s, pp. 1–12, 2025.

[31] Sharma, H., Kumar, P., Sharma, K., & Raj, N. (2026). Hybrid Deep Learning based Attack Detection Across Different Layers in IoT Environments. Defence Science Journal, 76(1), 41-54..

[32] K. G. R. Narayan, S. Mookherji, V. Odelu, R. Prasath, and A. K. Das, "IIDS: Intelligent Intrusion Detection System for IoT Applications," arXiv preprint arXiv:2308.00943, Aug. 2023.

[33] Sharma, H., Kumar, P., Shrivastava, G., Sharma, K., & Bhola, A. (2026). Using Machine Learning for Protecting the Security and Privacy of Internet of Medical Things (IoMT) Systems. In Integrating Cloud, Fog, and Edge Computing in Healthcare: Federated Learning and Blockchain Approaches: Harnessing Distributed Technologies for Enhanced Healthcare Delivery (pp. 123-138). Cham: Springer Nature Switzerland..

[34] A. Rahman, M. U. Faruque, and Z. Wang, "Explainable Deep Learning for Intrusion Detection in IoT Networks," IEEE Transactions on Network Science and Engineering, vol. 11, no. 3,pp. 1978–1989, Mar. 2025.