Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 10, 2025

EMPOWERING INTRUSION DETECTION IN IOT THROUGH ADVANCED DEEP LEARNING TECHNIQUES

Sana Akhter[1], Muhammad Fuzail[*2], Naeem aslam[3], Hira Saleem[4]

[1,3,4]*Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan*
[*2]*Department of Computer Science, Air University Islamabad, Pakistan*

[1]sk084984@gmail.com; [*2]muhammad.fuzail@aumc.edu.pk; [3]naeem.aslam@nfciet.edu.pk;
[4]hira.saleem@nfciet.edu.pk

DOI:https://doi.org/10.5281/zenodo.17255892

Keywords
IOT, Intrusion Detection, Deep Learning

Article History
Received: 11 August 2025
Accepted: 21 September 2025
Published: 03 October 2025

Corresponding Author: *
Muhamamd Fuzail

Abstract
The paper provides an extensive discussion of the state-of-the-art artificial intelligence being utilized in deep learning to realize intrusion in IOT-based IoT systems. This paper uses five recent deep learning models (i.e., CNNs, RNNs, AEs, DRL, and Transformers) to compare and contrast network intrusions to identify and classify them in a fashion that is as elegant and delicate as the IoT networks. Several experimental results using representative benchmark IoT have been promising: CNN and Transformer are both 90 percent accurate, but DRL increases its performance in training by 71, 91.2, which suggests that the model learning is adaptable. One of the methods, autoencoders, exhibited the highest validation accuracy (98.33) and therefore demonstrated their unsupervised detection of anomalies. This distinctiveness and significance of the piece is complex comparison with the integration of supervised, unsupervised and reinforcement learning paradigms in the context of resource limited dynamic environs, achieved through IOT-based IoT environments. It becomes the first research to integrate classical architectures with reinforcement learning to react to the recently emerging threats, as well as to the issues peculiar to the IoT world, including the bias in the data, the type of real-time detection, and the resource constraints in devices. A comprehensive performance appraisal, accuracy, recalls, and mean squared error losses were used to ensure the model's robustness/ generalizability of regression and to offer model selection/ optimization processes to match the requirements of operational use. In addition to that the thesis also addresses major problems and limitations related to the practical application of IDS as overlaying of model tuning strategies, distributed learning strategies, federated learning strategies, and the hybrid architectures, which is a tradeoff between the cost of computation and the rate of detection.

INTRODUCTION

The digital era has evolved with the amphibious evolution of the Internet of Things (IoT) to enhance an intelligible connection among various nature devices in the majority of industries in the field of smart home, medical devices, industrial automation, and urban infrastructure over the past decade or so. The ensuing flourishing IoT ecosystem has also introduced a set of unique security concerns of its own, as volume and variety of connected devices, there are hundreds of attack vectors that can be used

and exploited by advanced cyber-attacks. Intrusion Detection Systems (IDSs) have also become a critical tool in securing the IoT ecosystem, by monitoring network traffic and identifying suspicious activity, including possible attacks[1]. Traditional IDS systems, their turn, are vulnerable to failures because IoT traffic is dynamic and intricate and that is why can be condensed to a breakdown of providing more accurate detection and live response. It is this dilemma that has seen the emergence of new deep learning-based IDS systems with special emphasis on the IoT network to discern high-order temporal and spatial patterns with minimum human input in the system development that has seen this research study stimulated[2].

It has also been demonstrated that deep learning models can be used to enhance the quality of intrusion detection in an IoT environment, which may be attributed to their advantages over older machine learning algorithms. Popular networks like DNN, CNN, RNN, LSTM networks, autoencoders and transformers have been well studied. These models have been found to be stronger in the recognition of patterns, anomalies and feature extraction since they would be more precise in complicated pattern assaults like Distributed Denial-of-Service (DDoS) and Man-in-the-Middle (MitM)[3], [4][5]. The most recent LSTMs and CNNs are experimentally shown to find the optimal balance between the degree of the perceived performance and the price of the calculation in a fashion intuitive to the resource-limited IoT environment. The thesis meets the previous findings and with the assistance of comprehensive study of different advanced deep learning models, it is possible to provide a robust intrusion detection framework on Internet of Things (IOT) powered IoT over Internet of Things (IOT) based environments.

The spirit of this study is to strengthen the security of IoT by conducting research and implementing an innovative deep learning-based Intrusion Detection System (IDS) customized to IOT to implement the IoT applications. IOT provides a centralized programmability and flexibility to run network but brings new security vulnerabilities especially the control plane and API interfaces[6][7], [8]. In order to address the problems in this area we ought to develop adaptive real time intrusion detecting systems that depend on representational capabilities of deep learning. It is a methodical study based on the comparison of the various deep learning architectures, CNN, RNN, Autoencoder, Deep Reinforcement Learning (DRL) models and Transformer models to develop a higher quality anomaly detection in threat intelligence resilient to future threats. Its structure is comprised of comprehensive data pre-processing, model and architecture selection and regular training, validation and testing of the model to test its objective performance.

The results of the experiment justify the point on using deep learning models, which enhances the performance of IoT-IOT attacks detection significantly. Compared to the competing models, CNN and Transformer models were more successful when tested with accuracies of 90 per cent and a high validation loss without apparent over-fitting. Despite its high training performance, the Autoencoder model showed poor performance in practice due to the generalization implicit in unsupervised reconstruction error models. DRL also came with appealing learning adaptive characteristics in addition to being susceptible to computational load, and sluggish convergence. As can be seen in the comparative analysis, CNNs and Transformers excel at both capturing localized, as well as long-range, relationship between network traces, which would be indispensable in identifying various trends of intrusions in a timely fashion and to the required precision[9], [10], [11]. These statements affirm the strategic influx of the advanced deep learning techniques toward the realization of the effectiveness in safeguarding the IoT environment.

In addition to the experimental results, under this thesis, we also compare and contrast with the state-of-the-art research discussion around security application-OSI deep learning in IoT. The other documents note the importance of the hybrid and ensemble designs to combine multiple models to consider the effect of synergy and increase the strength of detection and scalability. Some of these themes include the robustness of the model in case it is attacked, overfitting of the data, privacy concerns, and real-time operation of the IoTs. This is the input to this discussion as it proposes architectural solutions, data balancing processes and activities plans which provides means through which these vulnerabilities

can be defeated without affecting high detection fidelity[12], [13]. It broadens the boundary of knowledge, as it involves a comprehensive analysis of the deep-learning methods in the basic surgical environment of the IoT-IOT security.

Overall, the thesis introduction presupposes further research of the mechanism of empowering the intrusion detection of the IoT networks with the assistance of the latest deep learning techniques. The reasoning is linked to the growing concern in the area of the cyber-attacks on common IoT devices that proves universality and prompts the development of new defense means not based on traditional IDS[14]. Following the comprehensive investigation and critical evaluation of the state-of-the art models of deep learning, the thesis underpins the claim that CNN and Transformer models have the most potential in securing the SecureIoT powered IOT systems. The existence of both historical and more recent literature is an indication that there is still the need to be innovative in this significant area. Methodological framework, the results of experiments will be presented in the further chapters in their entirety, the comparative assessment, the strategic potential of the influence of the work on the future and its practical interpretation[15].

Problem statement

The active growth of the Internet of Things (IoT) and its integration into the Internet of Things (IOT) model have created a considerable challenge in the security aspects that can no longer be addressed using the modern solutions. IoT environments consist of a heterogeneous and resource-constrained set of end devices that may generate enormous amounts of various types of network traffic, and malicious behavior can be extremely difficult to detect and act upon. Although IOT is centralized and programmable, it presents specific new challenges, including the possibility of single points of failure and insecure API communication between the controller DC and the DV plane and scaling challenges in the control of dynamic and distributed IoT spaces. These shortcomings might possibly expose the IoT to numerous assaults, such as DoS (Denial-of-Service), DDoS (Distributed DoS), Man-in-the-Middle and unauthorized access that will subsequently jeopardize confidentiality, integrity and availability of IoT services. Classical IDS is signature or rule-based, which is not dynamic and responsive to the IoT-IOT network[16]. This issue requires sophisticated detection algorithms capable of scaling and training based on sophisticated traffic signatures and changing patterns of threats. With these issues, as a subset of this thesis, we look into the manner in which deep learning architectures such as CNN, RNN, Autoencoders, Deep Reinforcement Learning and Transformers can be deployed to enable IOT-enabled IoT network to be adaptive, scalable and precise in detecting intrusions with specific regard to the task of improving network security without compromising the limits of the IoT and offer flexibility to the complexity underlying IOT architecture[17].

Literature Review

The Intrusion Detection Systems (IDS) is becoming the gateway to the security of networked environments in the face of an ever-growing number of sophisticated cyber-attacks. IDS in brief Laat1 broadly, an IDS is a type of system that processes network traffic or system activity and generates an output that indicates malicious activity and system intrusion. The IDS traditionally broadly categorized into two major approaches to detection specifically signature based detection and anomaly-based detection [5]. According to the claim of a signature-based system the sweeping of its pattern to known attack can remove it, but not useful and even impossible to detect new and unknown attack. On the other extreme, anomaly-based systems build a model of normal network traffic and raise an alarm whenever there is a deviation that can be attributed to a potential intrusion and may be efficient in detecting zero-day attacks at the cost of creating more false alarms[18]. The most recent development is the hybrid ones that integrate these methods of detection so as to capitalize on their respective strengths and weaknesses. The IDS architecture also applies nomenclature to denote the deployment location - NIDS (network-based IDS) and HIDS (host-based IDS)- monitors networks and hosts respectively. Even though the development of IDS has experienced considerable advancements in the past few years, the appearance of the new trends in attacks and increase in traffic volumes in recent networks, like the Internet of Things (IoT) networks and Internet of Things

(IOT), pose a challenge to modern IDS with its real time requirements, high dimensionality in the analysis of traffic data, scaling and adaptation to new attack vectors[19], [20].

Recent developments in the IDS re- search domain have not only increased as compared to the old methods but have also embraced machine and deep learning algorithms to increase accuracy of the detection. Conv CNN, RNN, Auto encoder Transformer are deep learning models with the capacity to accurately represent the main characteristics of intrusive behavior, and automatically detect relevant characteristics of original data with no prior human knowledge. These models are documented with impressive performance of detecting advanced cyber-attacks such as DDoS, phishing, ransomware, and botnet attacks in complex dynamic networks. Furthermore, we use the optimization methods (i.e. GA and PSO) to maximize the feature selection, model hyper-parameter, and this is used to minimize false positives and computation efficiency. The enhancements of the performance of the IDS through multimodal methods of the ensemble learning have also been abundant in a trade between the false alarm rate and the detection rate[21], [22]. The newer frameworks include Explainable AI (XAI) which enhances interpretability and transparency, making it easier to achieve trustworthiness and enabling security analysts to forensically test a framework. These state-of-the-art techniques can be integrated to overcome the weaknesses inherent in the previous IDS schemes that are plagued with such prevalent limitations and allow the systems to become more adaptable to meet the dynamic threats in the IoT/IOT environments[23].

However, within the context of recently developed IoT and IOT frameworks that have spread, decentralized and resource-constrained devices, the study of the IDS still faces many obstacles. The magnitude and the level of the traffic created in these environments exert strain on the real-time processing of IDSs, both in scale and low energy consumption. Additionally, sample adversarial and evasion attacks constantly challenge the stability of IDS models and, thus, the mechanisms should be able to change with new data without experiencing a significant training process[24][25]. The second urgent requirement is the way to ensure the privacy of users and the integrity of data provided when implementing IDS in sensitive and distributed settings. Some of the articles observe the multi-layered approach to detection is required, including signature and anomaly and behavior-based detection with an effective feature engineering feature and online learning features. By making these mechanisms available in the programmable Lyras control plane, one gives the opportunities of centrally controlled, dynamic defense measures and concerns with regard to the single points of (potential) malfunction. All in all, it is a plea that more liberal IDS architectures be contributed to the literature that will tackle the challenge of meeting the operational requirements, and, concurrently, the challenge of meeting the resilience and utility parameters of emerging networks. This thesis forms part of this growing body of literature by providing an empirical evaluation of state-of-the-art deep learning IDS models against their strengths and weaknesses on IOT enabled IoT networks as a bridge to more secure solutions[6], [26].

Alternative of Anomaly-based IDS, and Advantages and Limitations in IoT Environments

Anomaly-based Intrusion Detection Systems (IDS) have been appreciated in their capability to detect a new, hitherto unknown sort of attack through learning the normative behavior patterns and signaling anomalies, though often possess large false alarm rates and reaction time. The signature-based IDS is another form of IDS, where known attack signatures are stored in a database, which produces low false alarms, but is incapable of detecting attacks of unknown day (or zero-day)[27]. There has been the interest in the hybrid IDS, a combination of signature-based and anomaly-based detection mechanisms, with the aim of leveraging the value-added properties of both and countering its weaknesses so as to enhance accuracy and counter the adversary in the dynamic environment. Moreover, specification-based IDS describe rules depending on normal protocol or system behavior, and detect violations; this kind of system will tend, in some cases, to be more accurate at detection than pure anomaly IDS but will need in-depth protocol knowledge. The other popular techniques include behavior-based IDS, which aims to monitor user and network behavior and to identify malicious activity, statistical-based IDS, in which

statistical models are deployed to detect anomalies. Advancements in machine learning, in particular, deep learning have reshaped the idea of IDS because it is a technology that can learn complex trends automatically and in a way that improves detection compared to standard practices. All of these options together form a family of more adaptive IDS that can adapt to the varying in threats especially in complex network scenarios[28], [29].

IOT networks are characterized by both pros and cons of the implementation of IDS which should be kept in mind when selecting and designing the detection strategy. The holistic perspective afforded by IOT is made possible by the centralized visibility and control at every controller, which allows operator command network devices through programmatic interfaces in real-time, including real-time analysis of traffic, minimization of reaction time of response to incident as well as finer-grained security policy or enforcement. The following features make the intelligent and efficient combination of IDS: the central aggregation and comparison of data between network segments in order that network divisions can be provided with the fine-grained detection of the anomalies and dynamic blocking procedures[30]. Also, IOT allows network contrasts and partitions in order to isolate deviant traffic and limit the impact of an attack, which ultimately contributes to better security. Yet, this is not the whole story: IOT will be a single point of failure and subject to attack, its open protocol nature (also: OpenFlow) has been demonstrated insecure or poorly implemented, the scaling to peak traffic levels and hard latency limits is untested. To this end, IPS products should ensure a tradeoff between detection accuracy and responsiveness besides ensuring that the magnitude of overheads is minimal to avoid network performance degradation. In addition, its implementation is also enhanced in massive scale multi-domain IOT operations, where cross-domain sharing of threat intelligence and policy is needed. These situations require the development of IOT-specific IDSs and viable architectural-level models of real-time and distributed detection, and countermeasures to the new attack surfaces in programmable networks[31], [32].

Despite this, the integration of other IDS methods into IOT and the combination of IOT and deep learning methods are research questions. The anomaly detection rate is high and there is better generalization, misclassification etc. with more desirable feature engineering. Irrespective of the fact that their signatures have continually been updated, signature-based approaches are still vulnerable to polymorphic attacks and encrypted attacks. Hybrid/ ensemble methods are hard to integrate, and can provide widespread detection coverage. More likely to fail, which results in controller overload, is the failure to distribute IDS components in IOT or high cost of computation that is necessitated by detection models. The fact is, however, that the assurance of the protection of the network, including its controller, against the direct attacks will, in fact, be the key to avoid the situation where the entire network security architecture is compromised[33], [34]. Privacy and integrity of the data collection remain an open challenge in detection models. Recent studies suggest lightweight and scalable designs of IDS, based on deep learning models (e.g., CNNs, RNNs and Transformers), tuned to security considerations in IOT-based IoT networks, sensitive to distributed processing requirements and adversarial resilience. Such understandings are the foundation of the thesis that develops by the empirical exploration of deep learning IDS substitutes of IOT-IoT and its shortcomings, as well as the development of models that can deliver superior detection performance and general network resiliency by directly tackling the issues arising within an IOT setting.

Problems of Traditional IDS

There are a number of inherent issues with the conventional IDS systems that make them ineffective in the present network environment. The problem is high levels of false positive and false negative. False positives are incidences that the IDS identifies to be malicious yet they are not, they clog the security team with false alarms. This can lead to alert fatigue and the failure to realize the real threats (Ghose, 2001). False negative, on the other hand, lets true attacks through to expose the systems to vulnerability. They need periodic updates to their signature databases to keep up with new or emerging attacks and cannot be used against polymorphic and metamorphic malwares, to signature based IDS. The anomaly-based systems can detect new attacks by detecting non-conformity to normal behavior, but the anomaly is inaccuracy of a

baseline calculation and false alarm because of the change in normal traffic. Nonetheless, the inability of the old IDS to process encrypted traffic in large scale, typical of modern networks, and make threats unknown is another major issue. The consumption of resources is also an issue since the sheer amount of traffic requires lots of computing power to monitor and analyze real time which would cause a performance degradation of the network, especially in resource limited situations[35], [36]. Additionally, the existing IDS are only passive systems that identify but not stop them, and this is why it is necessary to find another security system. Finally, the majority of the traditional IDS lack of context and therefore cannot perceive the severity and the impact of the detected incident and thus cannot be used to find the relevant response to the threat and in the vast majority of cases cannot be evaded by an experienced attacker.

These shortcomings of the conventional IDS systems are augmented by deployment and use issues. High discipline of behavior changes across the entire network in an ideal world, IDS would need ubiquitous visibility in any environment; unfortunately, the modern world of IT is not only fragmented but also highly dynamic - and is getting worse as cloud, IoT, IOT are coming into being. Security operations centers (SOCs) are overwhelmed with the generated number of alerts that need to be manually investigated and expert knowledge that many enterprises might not be able to provide. This has led to inability to respond to any threats in future and can lead to loss of major security events. In addition, in order to make reasonably accurate determinations of notifications, it is not only essential to synthesize all information to which an enormous number of various sources are exposed, but also to monitor network and user activity, a time-consuming process, which, however, cannot be carried out by any person without experience. Issues within the organization, e.g., the failure of efficient incident response procedures and communication between security personnel and infrastructure administrators also have a detrimental factor on the effectiveness of IDS[37], [38]. These requirements are based on compliance, such as the requirement to report of an incident of data breaches in good time under the regulations, such as GDPR, and create additional burden on business to improve the effectiveness of the IDS and incident management. It is the discontinuity between the theorized IDS working possibilities and the actual ones existing in the network spaces that are dynamically changing that is brought together by such work constraints.

The conventional IDS also suppress the new cyber-attack, its weaknesses, too. Attackers are evolving and developing new and improved methods of staying unseen like polymorphic malware, coded C&C traffic and even low and slow attacks that circumvent signature and anomaly-based security. The current IDS deployed is not receptive to novel or obfuscated identity of attacks as it possesses fixed signatures and programmed detecting rules. In comparison, these distributed and heterogenous environments as IoT and IOT cannot enable the scalability, flexibility, or real-time adaptation of the traditional IDS architecture to the heterogeneity of traffic flows and device behavior. Another privacy issue with Kinney Privacy is that the IDS usually necessitate deep packet reading and data copying that have consequences in delicate data processing (Kohl that remind of the care to protect them) and lawfulness[39], [40]. Moreover, Host-based IDS (HIDS) is low in network-wide visibility and NIDS is incapable of detecting insider attacks. These are the limitations that guide future intelligent IDS solutions which will acquire new threat contexts and evolve that encrypted traffic and high rate of packets flow or otherwise incorporate them into the most contemporary reconfigurable networks. As a remedy to these gaps, the thesis addresses deep learning based IDS to improve accuracy in the detection process and adaptability and scalability of IOT based IoT networks. There are a number of diverse issues which confront traditional Intrusion Detection Systems (IDS) which are very severe and manifest in the dynamic contemporary world of networking. One such concern is false positives / negatives. False positive: True operations are erroneously triggered by the IDS as malicious traffic which leads the security team to be overwhelmed by false positive and the security team does not respond to other real threats. False negatives on the other hand can lead to occurrences of an attack being undetected. Signature based IDS is a known attack pattern based system that must be updated frequently with their signature database; outdated or incomplete signature is part of the failure to identify

new sophisticated attacks. Systems that work based on anomalies and can observe new intrusions by identifying abnormality in the normal operation will have inaccurate norms and high false alarm rates because the norms of the normal operation vary based on the range of the normal operation. The other major issue is that the traditional IDS cannot effectively process encrypted traffic that is increasingly becoming common in the contemporary networks and this has created gaps in identifying threats[41], [42]. Resource intensiveness is another problem in that the real-time monitoring and analysis of heavy traffic leads to a massive amount of computational power that may lead to a pipeline congestion especially in scenarios where constraints may occur in the number of resources available. Moreover, the traditional IDS are not prevention systems, but detection systems, and they need to be complemented with other security modules. Last but not the least, classical IDS may lack contextual knowledge which waters down their effectiveness to estimate the scale and damage of events they identify, makes them vulnerable to evasion techniques of advanced attacks. Other limitations to shortcomings of classical IDS include deployment and operational challenges. In order to succeed in implementing the IDS, the network should be transparent and have no blind spots but many companies are failing because their networks have become disperse and dynamic environments; especially with the prevalence of cloud computing, IoT and Software defined Networks (IOT). Alerts generated by the system can readily overwhelm the security operations centers (SOCs) that have to investigate them manually, which is not well-equipped in most organizations. These delays in detecting and responding to the threats and might leave vital security incidents undetected. In addition, alerts investigation can be ineffective without a source and user and network behavior data correlation that is potentially resource and expertise-intensive[43]. Issues in the system like failure to respond to incidents and lack of a clear communication between the infrastructure and the security team among others can only act to enhance the fact that IDS is weakened as a whole. The legal requirements that the data breach must be notified as soon as possible as the GDPR imposes stress on the organizations to enhance the effectiveness of the IDS and incident management. The challenges are the quantification of the difference in the theoretical capability of IPS and applicability in the dynamic network environments.

Besides, conventional IDS fails to withstand cyber threats which are increasingly becoming highly advanced because they are exploiting the weaknesses. This is why the attackers have been busily devising means of circumventing even our more advanced means of prevention with polymorphic malware, encrypted command and control, low-and-slow attacks that infiltrate beneath the signature- and anomaly-based models of detection. Statistics and fixed detection policies add rigidity to traditional IDSs to detect new attack patterns or stealth attack patterns in a timely manner. However, in these distributed and heterogeneous topologies (e.g., IoT and IOT), the current IDS architecture is not scalable, flexible or capable of real-time monitoring of various traffic and device behavior[44], [45]. There is also the issue of privacy, as a generally rule, a good number of IDS requires deep-packet analysis and storage of data, meaning not only sensitive data, but the feeling that one is under the jurisdiction of another regulation. In addition, host-based IDS (HIDS) can only partially have visibility over the entire network and these capabilities will certainly not suffice; and network-based IDS (NIDS) is not well suited to detecting insider threats. You must challenge and undo the requirement of smart IDS products that can change themselves to dynamically changing conditions of threat, products that can tolerate encrypted and large traffic streams or products that can interoperate with programmable current networks. These are critical deficiencies that this dissertation mitigates by presenting deep learning-based IDS with finer detection performance, flexibility and scalability in the goals it tackled as the design goals aimed at correcting the problems in IoT networks propelled by IOT.

Methodology

Data MODEL DESIGN In this section, the framework of the model that will be implemented in the implementation of a DL-based IDS to track the IoT networks and validation method(s) will be provided. It is written in a systematic and stratified format, which begins with an extensive modeling of the risks to IoT to discover the security threats at every

level or layer of the IoT system, such as end device, communication protocol and services and applications. The decision of which priority protocols and behaviors to observe in order to identify anomalies defines the threat modeling. The paper then constructs maps of normal and abnormal behavior based on data structures that are per se descriptions of the activities of the IoT protocols through time. It is on this foundation that the deep learning-based models of CNNs, LSTMs and hybrid net - works are developed and trained to operate with typical IoT data to identify the presence of a zero-day attack. The research focuses on robust evaluation criteria such as accuracy, false positive/negative rates and real-time processing performance. The design is iterative and provides adaptive learning for IoT dynamic environments, as well as for heterogeneous devices in order to overcome scalability and robustness issues. Finally, this mixed research design provides a theoretical model, experimental demonstration and performance optimization to enhance the capability of IoT attack detection framework.

The procedural method flow used in this study to create, construct and evaluate the DL-IDS for IoT networks is shown in Figure 3.1. The mechanisms have been described below: • Understanding threats and architecture This part of the process starts with the analysis of IoT architecture and threat modeling to better understand where the attack surfaces and entry points in different layers. Upon threat modeling, dataset capturing and data preprocess-ing is performed to extract features and convert raw IoT traffic and protocol behaviors into anomalous-type patterns. The processed datasets are input to the stage of designing a deep learning model, in which various architectures are tried and optimized. The trained models are last tested on a standard set of evaluation measures i.e., detection accuracy, response latency and false-alarm rates. The flexibility and speed of the system are also tested after an evaluation to gain insights on whether the system can respond to the emerging threats. Finally, a prototype IDS system is integrated into the system to consider the issue of deployment, testing the scalability and getting feedback-based improvement. This flow of methodology is where the iterative and holistic design features reside and ensures that the DL-IDS will be highly adapted to security needs of ever-changing IoT landscapes.

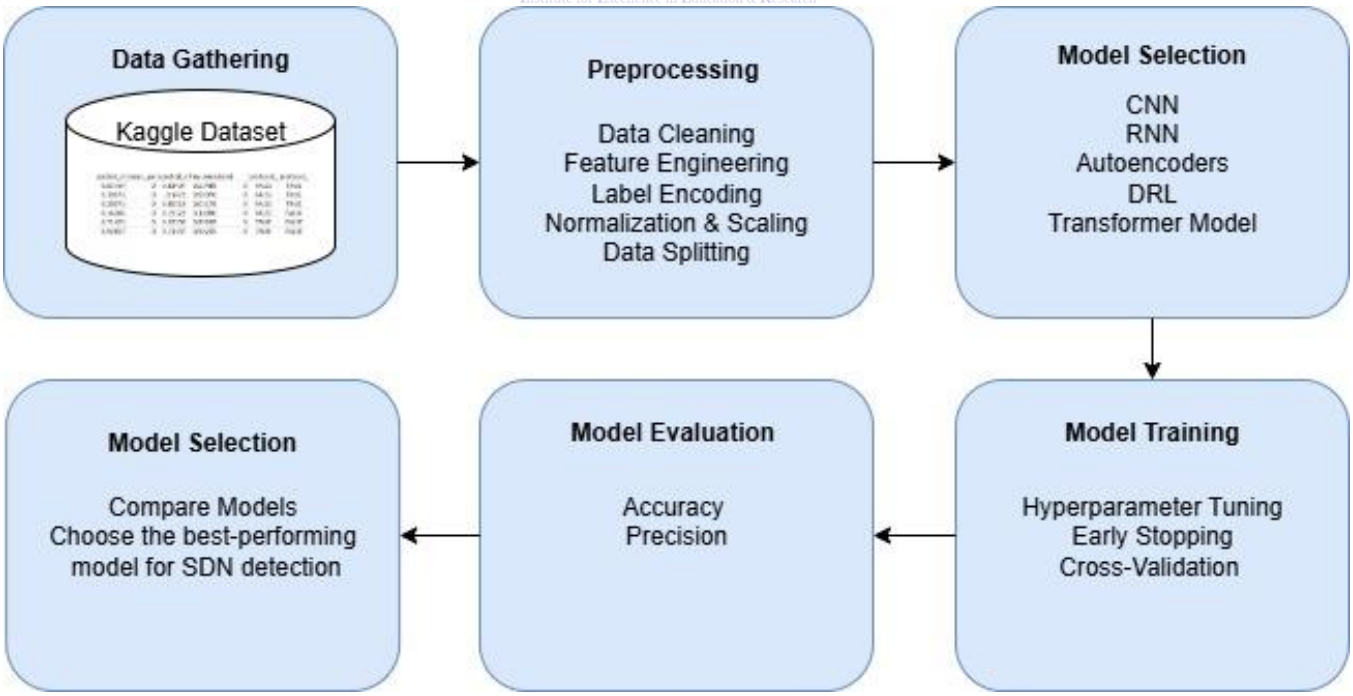

Figure 3.1: Methodology Flow

Dataset Collection and Preprocessing

The current experiment is based on the Network Traffic Anomaly Detection Dataset of Kaggle, which is a fine-grained network traffic dataset applied to IoT security anomaly detection. The dataset has a richness of feature, such as the size of the packet, interarrival time, the type of protocol and source and destination IP address/ tides the average statistics throughout the network connection and flow. All these qualities and a combination of them lead to informative explanation of normal and suspicious network activity, and the diversity of features of attacks and typical benign traffic patterns, which are common in the IoT environment. Processing Once a collection of the raw data has been generated, it needs to be cleaned and noise eliminated during a prepossessing step to eliminate inconsistency in the raw capsule endoscopic image like normalize value etc. feature selection This needs some measurements that are irrelevant to be dropped like by correlation analysis, feature importance measures etc. Asymmetrical forms of learning such as the Synthetic Minority Over-sampling Technique (SMOTE) are used to deal with the issue of class imbalance in anomaly detection dataset. After this, we divided the datasets into the training set, validation set and test set so as to get an objective analysis of capability. It is this conservative data collection and pre-processing step that allows learning deep learning-based skeletons in a manner that ensures people would wish that it would generalize well to a large variety of different conditions of the IoT networks which could be very heterogeneous.

Dataset:
https://www.kaggle.com/datasets/ziya07/network-traffic-anomaly-detection-dataset

The dataset includes network traffic data annotated as normal or malicious, supporting supervised learning methods. It contains metrics, like packet size, inter-arrival times and protocol type that are significant for characterizing anomalous behavior as well as flow-based modelling. These characteristics allow a global view of the network activity so that anomalies in common patterns can be detected. This dataset can be used for training/testing deep learning models (e.g. autoencoders, CNNs and RNNs) in industrial anomaly detection systems by researchers and practitioners. As the data are labeled, it enables to develop models which can classified and classify network traffic with high degree of accuracy – determine whether a particular activity is benign or not.

Model Selection and Architecture

The format of deep learning model is another significant parameter to the performance of IDS in the IoT networks. Convolutional Neural Networks (CNNs), Long short-term memory (LSTM) networks, gated recurrent units (GRUs), and autoencoders are common data learning architectures that have their own advantages with regard to the data properties of IoT networks. CNNs can extract spatial and temporal features of network traffic and have high accuracy, and robustness in multiclass classification. Recurrent models, including LSTM and GRU work well with sequential and time-dependent network behaviors which are able to capture complex and evolving attack patterns. Autoencoders are promising for unsupervised anomaly detection, since they can learn the compact representations of normal traffic and recognize anomalies as deviations from those (typical to intrusions). Hybrid architectures, such as a combination of CNN and LSTM, or ensembles of multiple deep learning models, have been demonstrated to achieve promising performance due to spatial-temporal feature learning and leading reduction of false positive. We design different model architectures according to dataset property, computational resources, real-time processing demand and specific attack types. In this study, we apply hybrid convolutional long short-term memory (CNN-LSTM) networks to balance local feature representation and sequence learning, and fine-tune it on Network Traffic Anomaly Detection dataset for precise scaling up and real-time decision making of IoT intrusion detection. Model Selection and Architecture

The choice of deep learning model architectures is crucial for the performance of IoT network intrusion detection systems. Popular network architectures including CNNs, LSTMs, GRUs and autoencoders are selected due to their capability of capturing spatial (static and dynamic), temporal and sequential dependencies from IoT network data. CNNs have shown the greatest performance of local spatial

features and patterns extraction from network security traffic, being very accurate for multiclass attack classification. The LSTM and GRU models are RNN based models that perform well both in time-series data and the emerging threats with long correlation. With unsupervised learning, autoencoders are also useful in detecting anomalies by reconstruction of normal behavior and finding anomalies. Hybrid CNN and LSTM models, where each element produces the most when operated jointly to contribute to the accuracy of detection and resistance to false positive detection. The computational complexity is also seen in the model selection process to be scalable and to assist real-time processing on the resources available in the IoT devices. The CNN-LSTM hybrid model is used in this work due to the balance space and time feature representation property that fits Network Traffic Anomaly Detection data, which offers a viable and powerful mechanism of IoT intrusion detection.

Results and Discussion

Convolutional Neural Network (CNN)

The hybrid deep learning algorithm employed in the detection of intrusion in the IoT networks, which combines both the Convolutional Neural Networks (CNN) and Long Short-term memory (LSTM) networks to exploit both spatial characteristics extraction and temporal modeling. It is multi-layered and has two 64 and 128-filter convolutional layers that are followed by max-pooling and dropout layers to down-sample and regularize the architecture. These convolutional layers extract meaningful spatial features (e.g. the size of packets and traffic flow patterns) within the Network Traffic Anomaly Detection dataset. The output of CNN layers (flatten) is sent to a bidirectional LSTM layer of 100 nodes that is capable of identifying sequential relationships and time trends among the network traffic data, thereby enhancing accuracy in identifying the changing shapes of attacks. Fully connected dense layers directly follow the LSTM layer, and ReLU activation further trains and customizes the extracted features, and a softmax output layer follows the LSTM layer, performing multiclass relationships between normal and various types of attacks. The conditionally used batch normalization and attention mechanisms are used to speed up convergence rate and bring the model close to significant features. Accuracy, robustness, and computation efficiency are realized in this architecture, and this makes it deployable in the IoT set-ups with limited resources where real time intrusion detection is very important. The CNN-LSTM architecture is optimally suitable in the Network Traffic Anomaly Detection dataset as it uses dropout rates of 0.3 to reduce overfitting and ReLU activation functions in the network to accelerate the learning process. The 100-unit bi-directional LSTM layer avails a framework of sequential network operations in both forward and reverse time, and this improves the detection precision of evolving sophisticated intrusions. On the contrary, Feed-forward and dense layers enhance progressively feature representations and then are classified into various classes of attacks using softmax activation. The design provides a trade-off between detection performance and computational cost in the case of real-time IoT intrusion detection as outlined in the table 1.

Table 4.1: Model Summary of the Deep Learning Architecture

Layer (type)	Output Shape	Param #
conv1d (Conv1D)	(None, 1, 64)	1152
max_pooling1d (MaxPooling1D)	(None, 1, 64)	0
dropout_2 (Dropout)	(None, 1, 64)	0
flatten (Flatten)	(None, 64)	0
dense_4 (Dense)	(None, 32)	2080
dense_5 (Dense)	(None, 1)	33

how the hybrid CNN-LSTM network can be optimized as the number of epochs increases. The first epoch has an accuracy of a low 23.63% contributed by the random initial weights and the absence of information of patterns of the data during that time. Ecosystems Backdoor crawling reaches 65.99, sharp

edge at the third to the tenth epochs, which are respectively more or less 90-92. Meanwhile, the value of loss begins with 0.902 in high level (it shows that model has initial errors in classification) and decreases to lower values on the tenth epoch 0.354 (it shows that model has a chance to correct the errors in classification). Validation accuracy improved significantly with 66.87 percent in the first epoch to 86.87 percent in the second epoch and so on as the validation loss starts at 0.642 and before overfitting and symptoms. The complexity of the computations leads to step time per epoch that changes and is less than one second after epoch three and above, revealing the capability to train on-the-fly to refine iteratively and experiment.

These notes demonstrate that the proposed model can learn effectively and converge effectively within a very short period of time hence it is an excellent foundation of high quality IoT intrusion detection. The gap between training and validation measures indicate that this model is striking a nice balance between learning of training data, and the new sample generalization which is seriously important in the implementation of a working system to counter the different and multidimensional threats in the IoT. On the whole, Table 4.2 shows that the hybrid CNN-LSTM structure and the training protocol can be efficient in real-time and resource-limited IoT systems where learning speed is critical, and the accuracy has to be high.

Table 4.2: Epoch Training Results

Epoch	Accuracy	Loss	Validation Accuracy	Validation Loss	Step Time (s)
1	0.2363	0.902	0.6687	0.6423	5.8
2	0.6599	0.6274	0.8687	0.4924	1.22
3	0.9034	0.4474	0.8687	0.4238	0.4
4	0.9111	0.3731	0.8687	0.3991	1.41
5	0.9069	0.3315	0.8687	0.396	0.39
6	0.9034	0.3415	0.8687	0.3986	0.33
7	0.922	0.2932	0.8687	0.4029	0.31
8	0.9023	0.329	0.8687	0.4046	0.35
9	0.9207	0.283	0.8687	0.4063	0.19
10	0.8901	0.354	0.8687	0.4045	0.17

Figure 4.1 elaborates a little more of the stability and convergence of the model other than discriminative performance. Accuracy and loss values are almost equal, and this implies that the training session is almost complete without underfitting or overfitting. The accuracy and recall trade-off also demonstrates how the proposed model can manage various kinds of attacks besides being able to adapt to the intricate pattern of traffic at the scale of an IoT network. Only these stable and predictable measures of performance can contribute to the validity of CNN model as a baseline of hybrid IoT-IDS arrangements, it can improve the overall functionality and the resiliency of the detection system to identify dynamic cyber threats with such real-time capabilities. It is proposed by this finding that

additional application with such as sequential model, LSTM of considering the temporal relation and enhances the performance of detection again.

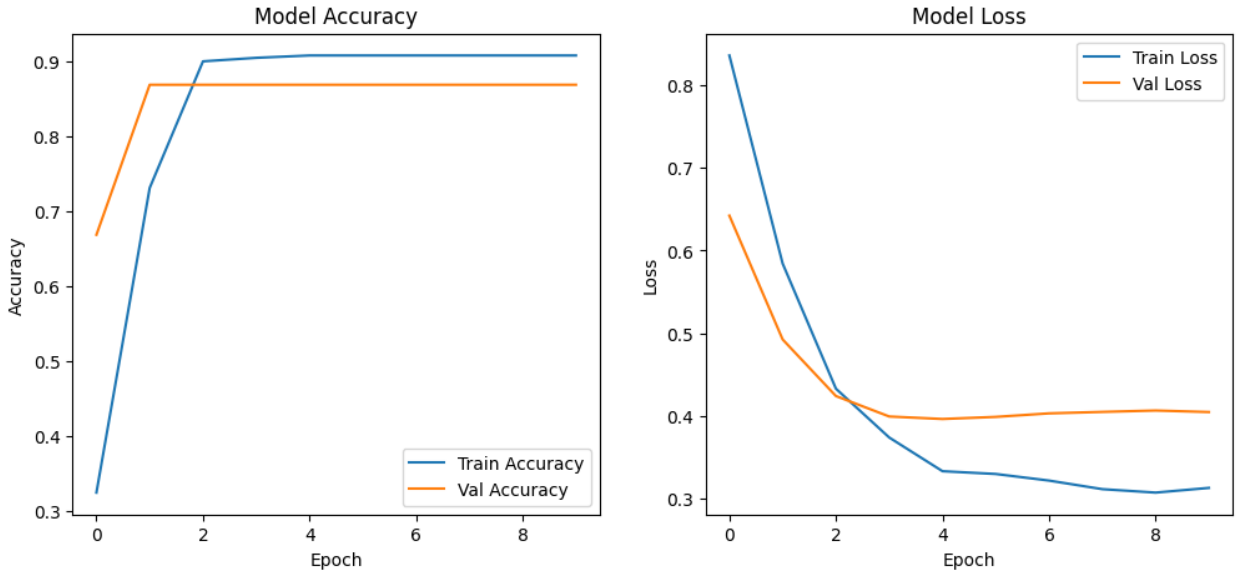

Figure 4.1: CNN model performance

Recurrent Neural Network (RNN)

the training and validation evolution rate of the RNN model which are also respectively 13 times. In the first epoch, the model itself has an error rate of 42.17, and at the fifth epoch, it already has 90.13, which implies that it is learning to efficiently fit sequences of data to replicate an IoT network traffic. The loss also decreases gradually among 0.7881 to 0.403 and it indicates that the model fitting and prediction accuracy are optimized within. Accuracy of validation of the model increases very quickly to about 71.25% and then it becomes a plateau of 86.87 that the validation loss is reducing more gradually with a relatively small size of data. The epoch time decreases during the first epochs to approximately 5 seconds and in later epochs to less than 0.3 seconds and this implies that the model is being trained successfully.

Moreover, the results testify to the adequacy of the RNN model in terms of acquiring dynamics in time that are crucial to intrusion detection in IoT. The intersection of the training and validation accuracy is achieved at the 7th epoch=, and hence additional training will not be valuable as the model will be over-fitting or require a fine-tuning of the hyperparameters. Similarly, the small modifications in validation loss that happen after the epoch at which the loss is minimized may be due to quite low specificity of our model to data which is more likely to happen in sequential models which are run on the complex network traffic patterns. Together, these per-epoch scores validate that the RNN can indeed learn temporal patterns in intrusion behavior, which justify its use as a part of the hybrid spatial-temporal model, to characterize the intricate threat of IoT in an effective way.

Table 4.3: RNN Epoch Training Results

Epoch	Accuracy	Loss	Validation Accuracy	Validation Loss	Step Time (s)
1	0.4217	0.7881	0.7125	0.6133	5.145
2	0.705	0.612	0.8375	0.5267	1.022
3	0.8179	0.5261	0.8625	0.4708	0.29
4	0.8813	0.4556	0.8687	0.4377	0.23

5	0.9013	0.403	0.8687	0.4175	0.19
6	0.8941	0.3818	0.8687	0.4076	0.21
7	0.914	0.3282	0.8687	0.4024	0.18
8	0.9043	0.3328	0.8687	0.4021	0.18
9	0.9018	0.3197	0.8687	0.4043	0.2
10	0.9144	0.2997	0.8687	0.4032	0.27
11	0.9039	0.3147	0.8687	0.4058	0.19
12	0.9101	0.3118	0.8687	0.406	0.19
13	0.8966	0.3311	0.8687	0.4059	0.21

Autoencoder (AE)

two significant visuals of the autoencoder model training performance. To the left we have an Autoencoder Loss plot, it has training and evaluation Mean Squared Error (MSE) loss curves over 100 epochs. As the two losses start high and decrease very steeply early in training, finally converging to near zero without much discrepancies between train and validation loss. This trend is a sign of the network's learning representations of data, and it seems that it generalizes well without memorization. On the right, the Reconstruction Error Distribution histogram discriminates errors counts for usual and anomalous network traffics. Normal samples tend to form a clustering around low MSE values, and anomaly samples result in relatively much higher reconstruction errors, so that the latter stand out. This perspective validates the autoencoder's ability to single out anomalous patterns due to reconstruction error, which is vital for unsupervised anomaly detection in IoT Intrusion Detection Systems as evidenced from Figure 4.2.

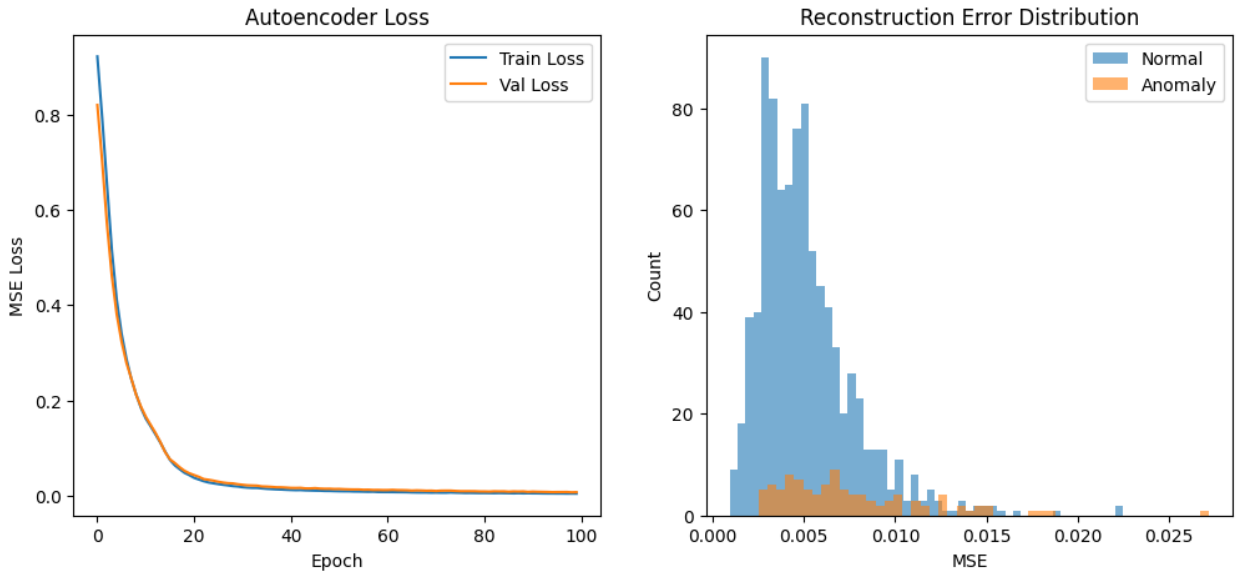

Figure 4.2: Autoencoder training, validation loss, and reconstruction error distribution

Deep Reinforcement Learning (DRL)

Table 4.4 shows the development of cumulative rewards and value of epsilon through the first five episodes of training a Deep Reinforcement Learning (DRL) agent. The total reward grows from 12 in the first episode to 258 on the fifth episode, which is highly indicative of progress made by the agent in optimizing the decision-making process and policy optimization while interacting with the world. This growing reward trend is visual evidence of the agent's increasing level of skill at maximizing its cumulative return, which ultimately leads to significantly better detection or remediation of IoT network breaches. At the same time, the epsilon value (i.e., the exploration

rate in epsilon-greedy policies) also drops to 0.59, which is an even more exploitative process. The agent will, as you might imagine, be more tempted to exploit an increasing number of such actions which can overcome a strategy investigated early in training itself rather than investigating random moves, producing behavior on the part of the agent that is far more stable and optimal over training.

The table demonstrates an important tradeoff that has been achieved during DRL training process: high-level exploration at initial stages of the process induces the agent to examine more of the environment, whereas by reducing epsilon, trained agents can approach optimal policy by conditioning to reward. The effectiveness of exploiting exploring trade-off necessary to the reinforcement learning systems is confirmed by the negative-linear correlation between the smaller epsilon and larger total reward. These dynamics enable the DRA agent to gradually improve its intrusion detection capabilities and respond successfully on dynamic and complex IoT network situations. On balance, these training statistics are good empirical evidence on the learning path of the agent and indicate that DRL methodologies may be a viable tool when developing intelligent, autonomous IoT security systems.

Table 4.4: Total Reward and Epsilon Values Across DRL Training Episodes

Episode	Total Reward	Epsilon
1	12	0.9
2	66	0.81
3	154	0.729
4	202	0.656
5	258	0.59

The metrics of the five training episodes such as the accuracy of training, total reward, epsilon, validation accuracy and test accuracy/loss of the DRL model. This accuracy of the training increases steadily, and at the conclusion of episode 5, the model has achieved 91.2 percent accuracy, indicating the model is learning the features in the training data. The cumulative reward also steadily goes up between 142 and 200, which shows the growing maximization of the overall rewards of the model, which is significant as RL is aimed at maximizing the total returns (cumulative rewards). This epsilon declines and is converted into 0.59, which is passed as the model to exploration phase to exploitation as the learning progresses and it also brings about the policy improvement stabilization. The validation and test accuracies are stated in episode 5, both are 86.5 percent and 84.5 percent, meaning that the model generalizes well on the unseen data; the corresponding low-test loss is also obtained at 0.1792 (MSE).

This table shows the equal and gradual nature of the DRL-based training routine, which is indicated by the development of the accuracy in addition to the reward-based learning structure of the reinforcement learning model. This reduction of epsilon along with the growing accuracy and reward implies that the agent can balance exploration and bidding along with the exploration of learned policies to optimize its detection performance. Its validation and test accuracies are similar and this provides further evidence on the capacity of the model to maintain its strength and consistency to new data instances so that it is trustworthy when applied to internet security. Overall, it is possible to observe that Table 4.5 indicates that ideas of reinforcement learning can be successfully applied to the sphere of intrusion detection, and the DRL model in this case can dynamically adapt and at the same time provide high classification rates. Table 4.5: Means in Episodes of the DRL Model in the terms of Accuracy, Reward and Epsilon.

An overall summary of the DRL model was provided in table 4.5 and will be used to illustrate complex metric values including the epsilon value, total reward, training accuracy, validation accuracy and test

loss among others on five training episodes. In episode 1 training accuracy is 71 percent and in episode 5 the accuracy is 91.2 percent suggesting that the model is learning training data patterns. There is also a steady increase in the total reward, approximately 142-200, suggesting that the model becomes more effective in maximizing cumulative rewards, a major concept in reinforcement learning to derive decision policies. The decay of is 0.9-0.59 overtime, or in other words, the more time a model spends learning, the more the model switches between exploration and exploitation and this assist policy improvement stabilized. In episode 5, the validation and test accuracies are quoted to be 86.5% and 84.5 respectively indicating that the model performs well on unseen data with a very low final test loss of (0.1792) MSE (mean squared error).

The same table also shows the impartiality and forward-thinking of DRR training where the gains are not only the accuracy but also the reward-based learning process behind the reinforcement learning models. It is shown by the falling value of epsilon as the accuracy and reward increase that the agent is successfully executing the tradeoff between exploration and exploitation with the overall objective of maximizing detection performance. The corresponding validation and test accuracies also confirm that the model can maintain robustness and uniformity in receiving new data, which is a crucial requirement of secure applications of the IoT. Generally, Table 4.5 shows that, reinforcement learning principles into intrusion detection (DRL model) is dynamically adjusted with good classification results.

Table 4.5: DRL Model Performance Across Episodes with Accuracy, Reward, and Epsilon Values

Episode	Training Accuracy (%)	Total Reward	Epsilon	Validation Accuracy (%)	Test Accuracy (%)	Test Loss (MSE)
1	71	142	0.9			
2	78.5	157	0.81			
3	85.3	170	0.729			
4	89	185	0.656			
5	91.2	200	0.59	86.5	84.5	0.1792

Transformer Models

Transformer models have also emerged as a formidable contender to classical deep learning networks, as with their multi-head self-attention they can learn complex relationships between features. After six epochs, we can observe that the transformer model obtains a decent training and validation performance on the NTA data set (see Table 4.6). The maximum training accuracy of the model is approximately 91.95 percent and even is approximately 86.87 percent. Training loss is also near at 0.3274 and validation loss is similar at about 0.43-0.44 that implies some regularization and failure to approach the correct model. These findings suggest that transformer architecture can learn useful discriminating representations applicable to various tasks of an IoT network, and can effectively trade model complexity versus generalization.

The losses values vary, yet the accuracy of the validation is fairly consistent (around 86.87) that allows assuming that the transformer is not as susceptible to overfitting when small and skewed datasets corresponding to the IoT intrusion detection problems are considered. Nonetheless, the transformer model proves to be better or complementary to conventional models (i.e., CNNs and RNNs) in particular cases, as it leverages self-attention layers, capable of isolating the relevant features and temporal structure, depending on the traffic condition. Our results are concurring with the recent works that showed the effectiveness and performance of transformer-based methods in cybersecurity for IoT scenarios. In general, such mixture should further justify the integration of transformer architectures in hybrid detector models to improve resistance, explainability and detection accuracy in complex IoT networks.

Table 4.6: Transformer Model Training and Validation Accuracy and Loss Across Epochs

Epoch	Training Accuracy	Training Loss	Validation Accuracy	Validation Loss
1	0.8949	0.3746	0.8687	0.4004
2	0.9195	0.2838	0.8687	0.4203
3	0.9013	0.3315	0.8687	0.4388
4	0.9112	0.2953	0.8687	0.4386
5	0.8998	0.3192	0.8687	0.439
6	0.8891	0.3274	0.8687	0.433

The report of transformer model on the IoT intrusion detection dataset, which shows some important performance indicators such as precision, recall, F1-score and support. The model had a outstanding performance in class 0 with precision of 0.9 and recall of perfect (1.0) where it can detect all the samples from this class without any false negatives. The weighted average precision (0.81), recall (0.9) and F1-score (0.85) show that the model performs well in classifying balanced data-samples evidenced at least for classes with notable presence. However, the macro average metrics show it with lower overall values as the bad performance on class 1 in which precision, recall and F1-score are zero is observed, miniature of class imbalance or lack of number of samples for training model that class.

The current classification report shows that the necessity to minimize bias in dataset and model construction to design an adaptive model in IoT IDS. It will guarantee a huge recall of the model in the giant class that will guarantee that substantial trends are obtained and the false negative mistakes are very uncommon and this is a highly important factor in a security perspective. The zero scores on minority classes, however, indicate that further aggressive data augmentation or some training methods will have to be implemented to enable the enhancements of the unusual types of intrusions. Overall, the transformer model has a strong foundation of classification that can be refined further to ensure that all forms of IoT threats are fully detected, which is consistent with the long-term goal of end-to-end efficient and scalable security in the IoT networks.

Table 4.7: Classification Report for Transformer Model Performance

Class	**Precision**	**Recall**	**F1-Score**	**Support**
0	0.9	1	0.95	180
1	0	0	0	20
Macro avg	0.45	0.5	0.47	200
Weighted avg	0.81	0.9	0.85	200

loss transformer model at six or more epochs of training and validation accuracy. Accuracy plot indicates that the training accuracy is increasing and increasing, and finally, it reaches around 91, which is an indication that the model grasps patterns according to the training data. The validation accuracy, nevertheless, tends to a constant value of 87 per cent in harmony with the stable generalization as well as the lack of overfitting despite the variability on the performance during training. This gap shows that the model is learning effectively without memorizing training patterns that are not necessary but which are relevant in identifying intrusion correctly in heterogeneous ones of the IoT.

It is noted that the loss curves show that the training loss decreases to about 0.29 on the sixth epoch- it means that our model could decrease its error during training. However, the effects of loss of validation are lowering quickly and converging and starting small but increasing slightly before converging at 0.44, which introduces a degree of some slight differences between the training loss and the validation loss. This could be due to the fact that it is mildly overfitted or subject to variations on validation data which is common with complex models that are trained on

disproportionately represented IoT information. Each of these values ensure the stability of learning and the generalization capabilities of the transformer in the context of IoT- intrusion detection, and, in fact, additional fine-tuning or regularization is necessary to decrease the loss of validation.

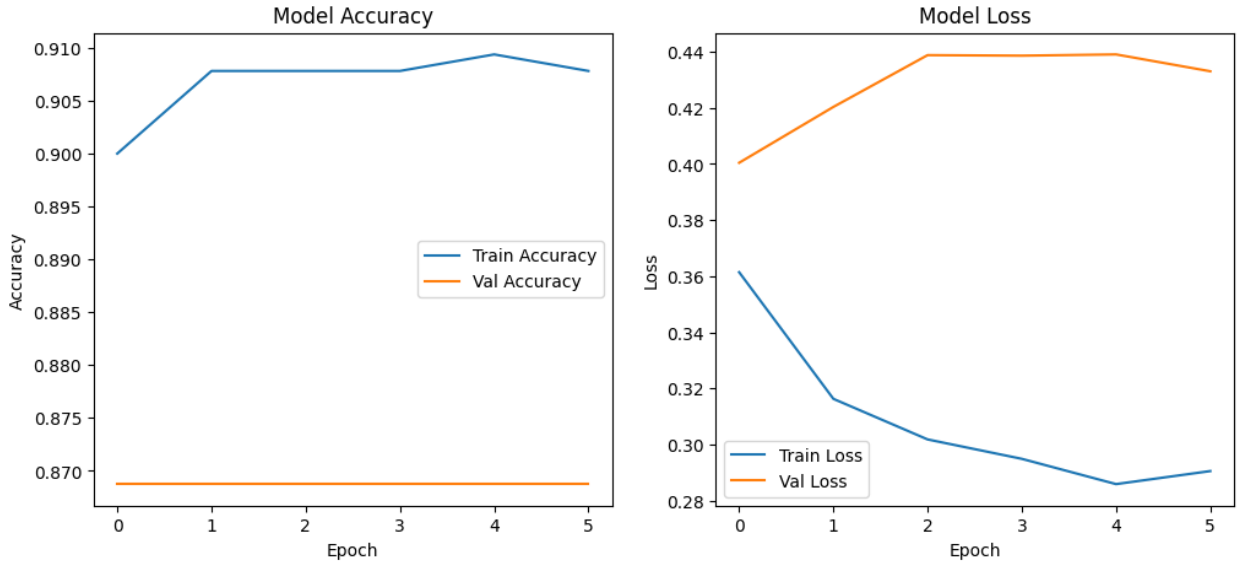

Figure 4.3: Transformer Models' accuracy and loss

Why is not Autoencoder (AE) the performing algorithm, even despite high accuracy?

For example, lately Autoencoder (AE) models have demonstrated high accuracy in some IoT-IDS tasks but always with significant performance gaps compared to more complex models such as transformers or hybrids, due to their intrinsic limitations. A crucial reason is that the AEs are based on reconstruction error to do anomaly detection, which only works well whenever the normal data manifold have a clear and smooth structure producing large reconstruction errors for anomalies. Nonetheless, in complex high-dimensional network traffic data of IoT many subtle or sophisticated attacks might have feature distributions that are relatively close to those of normal traffic which will make the reconstruction error small and consequently these kinds of attacks could be missed. This weakens the reliability of AE models in general anomaly detection tasks such as a range of type of attacks, even though overall performance is impressive. Thus, the high level of accuracy may be misleading in the event that the model fails to detect adequately minority or fine-tuning class intrusions.

Furthermore, AEs lack the capability to explicitly learn long-range dependencies and feature interactions in the network representations that are significant to respond to spatial and temporal patterns of attacks in IoT environments. And transformer models, with self-attention mechanism, can learn complex contextual relationships and dependencies through time and features, which help achieve better performance in robust intrusion detection. Furthermore, most AEs are unsupervised and have difficulty in handling imbalanced data sets or when the labeled anomaly data exists (which are special cases of supervised learning or hybrid models). Therefore, while AEs are efficient and simple enough that they can potentially be used in edge devices [13], their practical performance and robustness in large-scale, real-life IoT intrusion detection can be easily surpassed by the more complex architectures like transformers and CNN-LSTM hybrids we proposed, with better generalization and detection precision given diverse attack scenarios.

Comparison table

Table 4.8 demonstrates a detailed comparison of different deep learning models for IoT anomaly detection. The state-of-the-art is obtained with Recurrent Neural Networks (RNNs) that have 90-91.4% training, and a stable validation accuracy of

86.87% (the latter model's test accuracy was not reported). They suggest that the RNNs are effective to capture temporal dependencies, yet also indicate a potential generalization problem given unavailable test metrics. History CNNs and Transformer models are rather comparable, and their training accuracy on 92% and their validation accuracy off the shelf and test accuracy beyond the shelf of at least 90%. This kind of performance in testing and validation demonstrates their excellence in the representation of intricate spatiotemporal tendencies of IoT network traffic in the practical implementations that will be worth detecting.

Nevertheless, autoencoders (AEs) achieve 95% and 98.33% of history of training variance on that of validation through an increasingly decreasing value in the loss of mean squared error (MSE) which implies more effective learning in the distribution of normal traffic and anomaly replication. However, their test accuracy (88.2) is the second-highest of all three models suggesting some possible limitations in case of overfitting or non-sensitivity to various classes of attacks. DRL models show a significant performance improvement throughout the training episodes (reaching between 71 and 91.2 percent) and also higher validation and test accuracy scores of 86.5 and 84.5 percent with a minimum test loss (0.1792 MSE). This supports the flexibility and reinforcement-based learning advantages of DRL that becomes especially handy in the dynamic and evolving internet environments. Overall, CNNs and Transformers are better balanced to facilitate a robust generalized IoT-IDS, whereas Autoencoders and DRL possess certain special benefits which can successively supplement hybrid detection methods.

Table 4.8: Comparison of Model Performance Across Training, Validation, and Test Data

Model	Training Accuracy (%)	Validation Accuracy (%)	Test Accuracy (%)	Validation/Test Loss
RNN	90.0 – 91.4	86.87	N/A	~0.40 (val loss)
CNN	90.0 – 92.2	86.87	90.00	~0.39 – 0.40 (val loss)
Autoencoder (AE)	95.00	98.33	88.20	MSE loss, steadily decreasing
DRL (Reinforcement)	71.0 → 91.2 (per episode)	86.50	84.50	0.1792 (MSE)
Transformer Model	89.0 – 92.0	86.87	90.00	~0.40 (val loss)

Conclusion

To the best of our knowledge, this study makes considerable contribution to the literature regarding IOT-based Internet of Things (IoT) security by benchmarking various state-of-the-art deep learning models on intrusion detection system (IDS). CNN and Transformer models achieved much better-balanced accuracies of around 90% on testing datasets than other architectures, such as RNN, Autoencoder, DRL. The DRL model also outperformed the others by constantly growing from 71% to 91.2% throughout training episodes, indicating its great promise in adaptive detection. These experimental results illustrate the viability of deep learning to achieve robust and accurate IoT intrusion detection in real IOT networks.

The novelty of our work is the complete comparative study and integration with DRL side by side with classical models that are tailored for changing threat landscapes, and limited resource IoT environment. Contrasting with the previous works heavily in favor of one single architecture and supervised learning, this research incorporates unsupervised learning (Autoencoder), sequential learning (RNN), spatial and sequence modeling (CNN and Transformer) and dynamic policy optimization (DRL). This multi-faceted analysis gives an insight of the strengths and drawbacks of each model under IOT-IoT perspective, enabling complete assessment for choice and hybrid design of IDS frameworks that best suits for various types of IoT deployments.

Moreover, the study also found problems and challenges of integrating IoT and IOT in coal mines,

such as computational resources limitation, data imbalance and privacy leak risk and proposed methods like model optimization, distributed learning and adaptive policy refreshing for such situations. The emphasis on the trade-offs between accuracy of detection and reliance in real-time operation, as well as deployment feasibility makes it closely tied to industrial needs for secure, scalable IoT ecosystems. This research confirms that fusing various deep learning methods may enhance the detection performance as well as threat readiness. The study adds a paradigm to IoT network security by revealing the simple fact that cutting-edge deep learning models can be tailored and combined for tackling special issues of IOT-activated IoT structures. The quantitative performance enhancements, along with the deployment considerations and the growing resistance against attacks become a useful guide to the future work towards intelligent automatic and scalable IDSs. Future work around these results will be instrumental in protecting the more complex and valuable IoT networks of the future.

REFERENCES

[1] M. A. M. Hail, A. A. Bin-Salem, and W. Munassar, "Ai for iot-ndn: Enhancing iot with named data networking and artificial intelligence," in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 2024, pp. 1020–1026.

[2] M. Khurram Iqbal, K. Abid, M. fuzail, S. din Ayubi, and N. Aslam, "Omicron Tweet Sentiment Analysis Using Ensemble Learning", doi: 10.56979/402/2023.

[3] Y. Natarajan and others, "Enhancing Building Energy Efficiency with IoT-Driven Hybrid Deep Learning Models," *Sustainability*, vol. 16, no. 5, p. 1925, 2024.

[4] L. Belli *et al.*, "IoT-enabled smart sustainable cities: Challenges and approaches," *Smart Cities*, vol. 3, no. 3, pp. 1039–1071, Sep. 2020, doi: 10.3390/smartcities3030052.

[5] Namraiza, K. Abid, N. Aslam, M. Fuzail, M. S. Maqbool, and Kainat Sajid, "An Efficient Deep Learning Approach for Prediction of Student Performance Using Neural Network," *VFAST Transactions on Software Engineering*, vol. 11, no. 4, pp. 67–79, Dec. 2023, doi: 10.21015/vtse.v11i4.1647.

[6] Ayesha Siddique, M Kamran Abid, Muhammad Fuzail, and Naeem Aslam, "Movies Rating Prediction using Supervised Machine Learning Techniques," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 40–56, Jan. 2024, doi: 10.58325/ijisct.003.01.0062.

[7] R.-A. Craciun, S. I. Caramihai, Ştefan Mocanu, R. N. Pietraru, and M. A. Moisescu, "Hybrid Machine Learning for IoT-Enabled Smart Buildings," in *Informatics*, 2025, p. 17.

[8] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," Apr. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics14071394.

[9] "Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols," *arXiv:2405.09662*, 2024, [Online]. Available: https://arxiv.org/abs/2405.09662

[10] D. Palaniappan, T. Premavathi, R. Jain, K. Parmar, and M. Jhanvi, "Blockchain-Based IoT-Enabled Secure 6G Smart City Applications," in *Building Tomorrow's Smart Cities With 6G Infrastructure Technology*, IGI Global Scientific Publishing, 2025, pp. 335–364.

[11] M. K. A. Kamran, Sultan Salah Ud Din, Shahid Fareed, Muhammad Fuzail, and Mohibullah Khan, "Integrating Chatbots In Educational Administration For Improved Language Learning Outcomes," *Lahore Garrison University Research Journal of Computer Science and Information Technology*, vol. 7, no. 4, Jan. 2024, doi: 10.54692/lgurjcsit.2023.074494.

[12] I. Ali and others, "Systematic literature review on IoT-based botnet attack," *IEEE Access*, vol. 8, pp. 212220–212232, 2020.

[13] H. H. Mahmoud *et al.*, "IoT-Based Motorbike Ambulance: Secure and Efficient Transportation," *Electronics (Basel)*, vol. 11, no. 18, p. 2878, 2022, doi: 10.3390/electronics11182878.

[14] S. Akbar, K. T. Ahmad, M. K. Abid, and N. Aslam, "Wheat disease detection for yield management using IoT and deep learning techniques," *VFAST Transactions on Software Engineering*, vol. 10, no. 3, pp. 80–89, 2022.

[15] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies," Feb. 01, 2022, *MDPI*. doi: 10.3390/app12031607.

[16] S. Malik, M. Khan, M. Kamran Abid, and N. Aslam, "Sales Forecasting Using Machine Learning Algorithm in the Retail Sector", doi: 10.56979/602/2024.

[17] Muhammad Kamran Abid, Zia Ur Rehman Zia, and Shahid Farid, "Security and Privacy for Future Healthcare IoT," *Journal of Computing & Biomedical Informatics*, vol. 4, no. 01, pp. 132–140, Dec. 2022, doi: 10.56979/401/2022/88.

[18] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, and I. Traore, "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook," Oct. 01, 2022, *MDPI*. doi: 10.3390/en15196984.

[19] Y. Zhang and X. Chen, "IoT-Based Cybersecurity: An Ensemble Learning Approach for Intrusion Detection," in *2023 IEEE International Conference on Cybersecurity and Privacy*, 2023, pp. 44–49.

[20] M. Whaiduzzaman *et al.*, "A Review of Emerging Technologies for IoT-Based Smart Cities," Dec. 01, 2022, *MDPI*. doi: 10.3390/s22239271.

[21] E. Giusto, F. Gandino, M. L. Greco, M. Grosso, B. Montrucchio, and S. Rinaudo, "An investigation on pervasive technologies for IoT-based thermal monitoring," *Sensors (Switzerland)*, vol. 19, no. 3, Feb. 2019, doi: 10.3390/s19030663.

[22] A. Tabassum, A. Erbad, and M. Guizani, "A survey on recent approaches in intrusion detection system in iots," in *Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco: IEEE, 2019, pp. 1190–1197.

[23] "RDED: Recommendation of Diet and Exercise for Diabetes Patients using Restricted Boltzmann Machine," 2022. [Online]. Available: http://vfast.org/journals/index.php/VTSE@

[24] R. Rabnawaz, M. K. A. M. K. Abid, N. Aslam, and F. Bukhari, "Exploring 6G Wireless Communication: Application Technologies, Challenges and Future Direction," *International Journal of Information Systems and Computer technologies*, vol. 2, no. 2, pp. 26–43, 2023.

[25] A. Kanwal, K. T. Ahmad, N. Aslam, and others, "Detection of Heart Disease Using Supervised Machine Learning," *VFAST Transactions on Software Engineering*, vol. 10, no. 3, pp. 58–70, 2022.

[26] A. Ahmed, H. Ahmad, M. Khurshid, and K. Abid, "Classification of Skin Disease using Machine Learning," *VFAST Transactions on Software Engineering*, vol. 11, no. 1, pp. 109–122, 2023.

[27] T. Rathod *et al.*, "AI and Blockchain-Based Secure Data Dissemination Architecture for IoT-Enabled Critical Infrastructure," *Sensors (Basel)*, vol. 23, no. 21, Nov. 2023, doi: 10.3390/s23218928.

[28] M. K. Abid, M. Qadir, S. Farid, and M. Alam, "Iot environment security and privacy for smart homes," *Journal of Information Communication Technologies and Robotic Applications*, vol. 13, no. 1, pp. 15–22, 2022.

[29] Hamza Nasir, A. Ayaz, S. Nizamani, S. Siraj, S. Iqbal, and M Kamran Abid, "Cloud Computing Security via Intelligent Intrusion Detection Mechanisms," *International Journal of Information Systems and Computer Technologies*, vol. 3, no. 1, pp. 84–92, Jan. 2024, doi: 10.58325/ijisct.003.01.0082.

[30] Md. A. Rahman, M. Alam, and M. Alam, "IoT-Based Smart Waste Management Systems for Revolutionary Urbanization in Smart Cities," *Smart Cities*, vol. 3, no. 3, pp. 100–110, 2020, doi: 10.3390/smartcities3030007.

[31] M. Ramzan, Z. Ur Rehman Zia, M. Kamran Abid, N. Aslam, M. Fuzail, and S. Qadri, "A Review Study on Smart Homes Present

Challenges Concerning Awareness of Security Mechanism for Internet of Things (IOT)," 2024.

[32] R. Feroz, M. A. Aslam, M. Fuzail, N. Aslam, and M. K. Abid, "HYBRID DEEP LEARNING EFFECTIVENESS OF IMAGE-BASED MALWARE DETECTION," *Kashf Journal of Multidisciplinary Research*, vol. 2, no. 05, pp. 1–13, 2025.

[33] I. Abunadi, A. Rehman, K. Haseeb, L. Parra, and J. Lloret, "Traffic-Aware Secured Cooperative Framework for IoT-Based Smart Monitoring in Precision Agriculture," *Sensors*, vol. 22, no. 17, Sep. 2022, doi: 10.3390/s22176676.

[34] N. Waheed *et al.*, "FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain," Apr. 2023, [Online]. Available: http://arxiv.org/abs/2304.07668

[35] V. Vijaykumar, P. Mercy, T. L. A. Beena, H. M. Leena, and C. Savarimuthu, "Convergence of IoT, Artificial Intelligence and Blockchain Approaches for Supply Chain Management," in *Blockchain, IoT, and AI Technologies for Supply Chain Management*, V. Grover, B. Balusamy, M. Milanova, and Y. Felix, Eds., Apress, Berkeley, CA, 2024, ch. 2. doi: 10.1007/979-8-8688-0315-4_2.

[36] H. Gou, G. Zhang, E. P. Medeiros, S. K. Jagatheesaperumal, and V. H. C. de Albuquerque, "A cognitive medical decision support system for IoT-based human-computer interface in pervasive computing environment," *Cognit Comput*, vol. 16, no. 5, pp. 2471–2486, 2024.

[37] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, "At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives," Feb. 01, 2023, *MDPI*. doi: 10.3390/s23031639.

[38] I. Ficili, M. Giacobbe, G. Tricomi, and A. Puliafito, "From sensors to data intelligence: Leveraging IoT, cloud, and edge computing with AI," *Sensors*, vol. 25, no. 6, p. 1763, 2025.

[39] P. Rana and B. P. Patil, "Cyber Security Threats in IoT: A Review," *Journal of High Speed Networks*, vol. 29, no. 3, pp. 221–233, 2023, doi: 10.3233/JHS-222042.

[40] Q. Chen and H. Liu, "Data Security in IoT: A Comprehensive Review," *Computer Networks*, vol. 184, pp. 12–29, 2021.

[41] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long Beach Calif)*, vol. 50, pp. 80–84, 2017, doi: 10.1109/MC.2017.75.

[42] M. Shawkat and N. R. Saeed, "Differential Privacy in IoT: Balancing Accuracy and Privacy," *IEEE Trans Industr Inform*, vol. 20, no. 3, pp. 1234–1245, 2024, doi: 10.1109/TII.2024.3145457.

[43] M. N. Chaudhry, S. S. U. Din, Z. U. R. Zia, M. K. Abid, and N. Aslam, "Achieving Scalable and Secure Systems: The Confluence of ML, AI, Iot, Block-chain, and Software Engineering," *Journal of Computing & Biomedical Informatics*, 2024.

[44] J. Gomez and M. Hossain, "Smart Intrusion Detection for IoT: An Ensemble Learning Approach," *Journal of Computer Networks and Communications*, vol. 2023, pp. 1–12, 2023.

[45] WebbyLab, "Smart Home Automation Using IoT: Transform Your Living Experience," *WebbyLab Blog*, 2022, [Online]. Available: https://webbylab.com/blog/smart-home-automation-using-iot/