© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720213

Deep Learning – Based Network Intrusion Detection for Internet of Things (IoT) Using Bidirectional Long Short-Term Memory (BLSTM): A Review

ALENG E. A.[1], SARJIYUS O.[2], YUSUFU G.[3]
[1,2,3]*Computer Science Department, Adamawa State University, Mubi*

Abstract- ***Deep Learning works by copying how the human brain operates. To get these features, the deep learning method uses strong neural network algorithms, like clustering algorithms, Bayesian algorithms, and artificial neural network algorithms. Deep learning algorithms are very powerful in terms of processing power, which makes them better suited for handling complicated and mixed data sets from IoT devices than traditional machine learning methods. The use of deep learning in the Internet of Things, especially when it comes to securing IoT networks, is still in the early stages of research and has a lot of promise for identifying security threats within IoT systems. Even though the structures of recurrent neural networks can be pretty complicated, adjusting the hyper parameters can help make them work well for IoT applications. This idea encourages using deep learning techniques to improve the safety of IoT networks. The fast growth of the Internet of Things (IoT) has created a large area where cyber threats can spread, putting important systems and personal information at risk from more advanced attacks. Traditional network intrusion detection systems (NIDS) use fixed signatures and require manual setup of features. Because of this, they can't find new types of attacks, like zero-day exploits and changing malware, which are common now. The different types of data from IoT devices, which use various communication methods like MQTT and CoAP, move quickly and vary a lot. This makes the data patterns complex and not straight forward, making it hard for regular systems to properly organize or understand them. There is a big need for a detection system that can: look at network traffic as a ongoing, two-way flow to get a complete picture. Lower the number of false alerts that cause "alert fatigue" for network administrators. Work well against the changing and urgent attack methods that are specific to IoT systems. The method to be used for collecting data is the secondary approach. Because I will use literature reviews from other authors to fill in the gap that has been identified. Research shows that there is a big need to develop good Deep Learning models that can detect attacks in data sets. The NSL-KDD dataset will be studied and used to train four different deep learning methods.***

Keywords: Artificial Neural Network, Attack Vectors, Cyber Threats, Deep Learning (DL), Internet of Things (IoT), Network Intrusion Detecting System (NIDS) and Polymorphic Malware.

I. INTRODUCTION

Background to the Study

Deep Learning works by copying how the human brain operates. To get these features, the deep learning method uses strong neural network algorithms like clustering algorithms, Bayesian algorithms, and artificial neural network algorithms. Deep learning algorithms have strong computing power, which makes them better suited for handling complicated and mixed data sets from IoT devices compared to older machine learning methods. (Mustafizur, 2024) Using deep learning in the IoT area, especially for securing IoT networks, is still in the early stages of research, but it shows a lot of promise for identifying security threats within IoT systems. Recurrent neural networks can use information from earlier steps in the input data to improve their learning. At each time step, the information is processed and saved so it can be used in the next time step (Bipraneel, 2018). The next time step uses the data that was stored earlier to continue processing the information. Even though recurrent neural network structures can be quite complex, adjusting the hyper parameters can help make them work well for IoT applications. This idea encourages using deep learning methods to improve the security of IoT networks (Mustafizur, 2024).

In today's connected world, keeping things secure means looking at and handling a huge amount of

different kinds of data. In today's world, businesses rely on computer networks to send information quickly and well inside the company (Qin et al., 2016; Vimalachandran et al., 2020).

The fast growth of the Internet of Things has created a lot of opportunities for cyber-attacks, making important systems and personal information more at risk from advanced threats. Traditional network intrusion detection systems (NIDS) depend on fixed signatures and manual setup of features. Because of this, they can't find new types of attacks, like zero-day exploits and changing malware that are common now.

Deep Learning has become a hopeful option for automatically detecting threats, but many current models have trouble keeping high accuracy in the special conditions of IoT settings. Most standard neural networks and one-way LSTM models can't properly understand the complicated, two-way time connections that exist in network traffic. Because cyber-attacks usually happen in steps, and the information from future packets is just as important as past ones, models that work in only one direction often have a high rate of false alarms and aren't good at catching multi-step attacks.

(Dash et al. 2025) suggested in their work that future research should look into using more deep learning methods, different versions of LSTM, and optimization techniques inspired by evolution to better understand complex patterns in network traffic. (Zhang et al,. 2019) also mentioned in their work that future studies should focus on combining learning-based approaches to protect expanding smart environments.

Moreover, the different types of data from IoT devices, which use various communication methods like MQTT and CoAP, come in fast and varied forms. This makes it hard for old systems to properly understand and group this data.

Corporate computer networks are getting bigger and more common. A big company might have thousands of workstations and many servers linked to the network. If each employee has their own workspace, these workspaces are usually not controlled from a central location and are not safe from outside dangers. They might use different types of operating systems, hardware, software, and ways to send and receive messages, and the people using them might know different amounts about staying safe online. Picture this: thousands of workstations in your company's network are all linked straight to the Internet. A network that isn't well protected can be attacked because it holds valuable information and has weaknesses (Zhang et al., 2020).

A network is composed of multiple computing devices that are connected to each other to efficiently distribute resources. This study is about creating a deep learning system to detect and identify different kinds of cyber-attacks in IoT networks. It uses a Bi-directional Long Short-Term Memory Recurrent Neural Network, called BLSTM, to make the detection more accurate and effective.

II. REVIEW OF RELATED LITERATURES

The Internet of Things (IoT) has been important in modernizing systems, which has caused fast growth in the creation of wireless and communication technologies.

It presents a new approach where many small devices, often called 'things', are linked to the internet. These links let people connect and work with other devices and systems using these tools. Because they are so well-known, these frameworks are now commonly used in many areas such as smart homes, smart factories, manufacturing, and other industrial uses (Zeeshan et al., 2021). Industrial IoT, or IIoT, is a rising group of technologies that use the Internet of Things in industrial settings. When used correctly, these technologies can greatly improve how well systems work, how dependable they are, how flexible they are, and how well different systems can work together, according to Long et al.(2018). However, as IoT devices are used more in both industrial and home settings, they have become targets for many new kinds of threats (Hafeez et al., 2020). Among these threats is malicious activity that can cause significant security issues and disrupt wireless communication. Hackers can quickly take

information from computers and networks, which can start a cyber-war. Some usual kinds of attacks are port scanning, checking the network, sweeping addresses, intercepting communications in the middle, finding weaknesses, stealing data, and attacks using botnets. In May 2020, two government-owned oil companies in Taiwan, CPC Corporation and Formosa Petrochemical Corporation, were attacked by ransomware. In July 2020, Swvl, a transportation booking app based in Cairo, faced unauthorized access to its IT systems. These examples show how weak network security can be. The lack of security in Machine-to-Machine (M2M) and Machine-to-People (M2P) connections makes a significant amount of information susceptible to theft by hackers, which compromises the privacy and safe use of IoT devices. To find harmful activities and keep the network traffic safe, an Intrusion Detection System (IDS) is seen as a good way to spot dangers, especially when it can identify threats accurately without many false alarms (Hawawreh et al., 2018).

Anomaly detection systems have made big progress in research. Deep learning methods can look at how network packets behave, even if they don't have labels. Some commonly used methods for this task are Random Forest (RF), Support Vector Machine (SVM), K-Nearest-Neighbors (KNN), fuzzy interpolation, Multi-Layer Perceptions (MLP), Artificial Neural Networks (ANN), and various other machine learning techniques (Hafeez et al., 2020; Kasongo et al., 2019). Artificial Neural Networks (ANNs) are a group of algorithms that help create artificial intelligence by learning from training. They are made to copy how the human brain works and learns. Currently, ANNs are utilized to detect undeclared activity within network traffic. In a study by Hanif et al.in 2019, a threat detection system based on an artificial neural network was suggested, using the UNSW-15 dataset in an IoT setting, and it achieved an 84% accuracy in detection. Taher and their team in 2019 used two artificial neural network models with the NSL-KDD dataset and got identification accuracies of 94.02% and 83.68%, respectively. In this paper, an artificial neural network model is used to find harmful activities and boost system performance to achieve better accuracy in detection.

Network Intrusion

Unauthorized access to your network or a particular address in your domain is called a network intrusion. An intrusion can be passive, which means it happens without anyone noticing, or active, where the attacker sneaks in secretly and changes things on the network. Intrusions can come from inside or outside the network, like from employees, customers, or business partners. Certain intrusions are just warnings of an unauthorized user who has infiltrated or is ruining your network with messages or inappropriate content. Some people are more dangerous because they try to get sensitive information either all at once or over a long time. Some people who break into your system might try to put bad software on your computer to get your passwords, record what you type, or copy your website so they can trick users into going to their own site. Some people might get into a network to take data or change the messages on websites that are open to the public (Vacca, 2013).

A hacker might get into your system by physically messing with locked computers and their hard drives or BIOS, or by attacking your web servers or getting past your firewall from the outside.

They might also get access from inside by touching or using parts of machines that are supposed to be kept secure, like hard drives or the BIOS, through people such as your users, customers, or partners.
There are several examples that show how network risks and attacks can greatly affect the security and performance of your network and applications (Yin et al., 2021).

Moreover, as people rely more on digital communication tools, the number of various network attacks is increasing (Thamilarasu et al., 2019). Here are the top ten networking threats and attacks that are covered in this discussion.

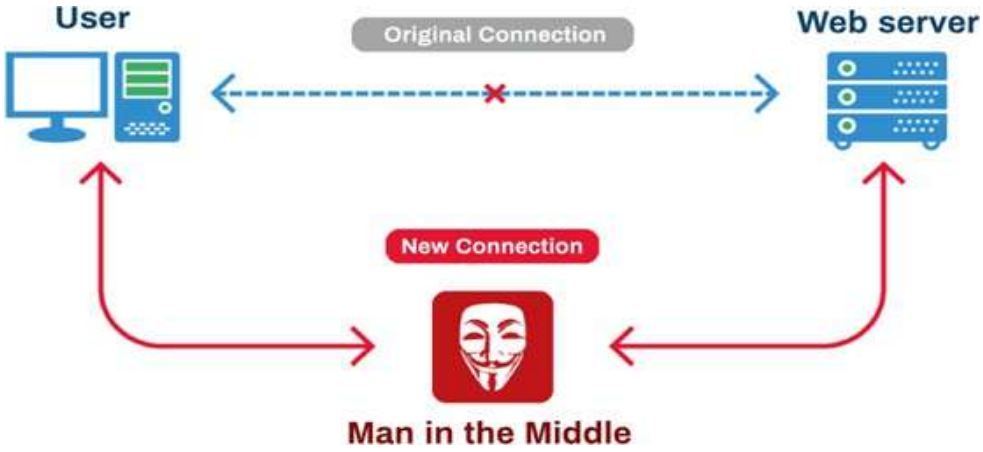
The fast and uncontrolled spread of harmful software is a major concern for keeping computer systems safe. This makes ransomware look like a common and harmful danger (Aleng et al., 2025). Bad software created to cause problems with electronics is always getting better and making it harder to fix the issues. The reason public information about malware

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720213

attacks is limited is because of worries about harming sensitive data and damaging the organization's reputation.This lack of transparency makes it harder for people to work together to prevent attacks and slows down thorough research (Yasmeen, et al.2022). In this area, ransomware is a type of harmful software that stands out on its own. Hackers use this method on purpose to lock files and ask for money in exchange (Aleng et al., 2025).

Man-in-the-Middle

A Man-in-the-Middle attack happens when someone not allowed secretly listens in on messages being sent between two people or systems. The attacker wants to eavesdrop on the conversation or pretend to be one of the real people involved without getting caught. The main purpose of a Man-in-the-Middle attack is to catch private or important personal data, like usernames and passwords, account info, or credit card details (Zhang et al., 2015). MitM attacks usually target businesses that deal with money or need users to log in, like online stores and banking websites. The stolen data can be used to steal someone's identity, make unauthorized money transfers, or sold to other people (Chordiya et al., 2018).



Man-in-the-middle attack (Chordiya et al., 2018).

Ransomware attack (Chordiya et al., 2018).

Ransomware

Ransomware attacks have been happening more and more often in 2022. These dangers have caused big problems for a lot of companies. Ransomware is a harmful computer program that locks up all the files on someone's computer, network, or server. Some

types of ransomware use bad passwords and weaknesses in systems to get into a network and lock files until a ransom is paid for the key to unlock them. Ransomware is a type of malware that poses a risk of exposing or restricting access to data or a computer system, usually through encryption, unless the victim pays a ransom. The ransom demand usually comes with a specific time limit. If the victim doesn't pay the ransom on time, the data could be lost forever, or the amount they have to pay might go up, according to (Kumar et al., 2018).

Cybercriminals aim at both people and businesses in many different types of industries. Authorities like the FBI and the No More Ransom Project say not to pay the ransom because it might make attackers do more harm. People who pay the ransom are more likely to be targeted again by ransomware, especially if the harmful software is still present in their system.

Table 2: Summary of Related Literature

S/N	Author(s)	Title of the Work	Methodology	Findings	Limitations
1	Marwa (2022)	*Machine Learning for IoT Based Networks Intrusion Detection: A Comparative Study*	Machine learning (ML) and deep learning (DL) approaches are solutions used by many researchers in IDS.	Decision Tree with Fisher Score achieved 99.26% accuracy with a prediction time of 0.4 seconds.	Future work intends to evaluate more high-performing deep learning techniques for IDS.
2	Neha et al. (2022)	*Intrusion Detection System on IoT with 5G Network Using Deep Learning*	Proposed customized Autoencoder (AE) and Deep Neural Network (DNN) detection model.	Achieved 99.76% accuracy.	Further optimization of computational time is required.
3	Güneş et al. (2024)	*Deep Learning Based Network Intrusion Detection*	Proposed methods for detecting both internal and external attacks.	Over Sampling achieved about 77% accuracy, while Random Under Sampling achieved 76–77% accuracy.	Additional improvement is needed based on accuracy, precision, recall, and F1-score.
4	Albara (2023)	*A Novel Deep Learning-Based Intrusion Detection System for IoT Networks*	Feature extraction followed by deep neural network classification.	Average Precision: 93.71%, Recall: 93.82%, F1-score: 93.47%.	Several limitations were identified, providing opportunities for future improvements.
5	Gopalkrishna et al. (2014)	*Network Intrusion Detection System*	NIDS executes an output module after detecting intrusions to record and notify attacks.	IDS commonly employs statistical anomaly detection and rule-based misuse detection.	Survey-based study without proposing a new integration model.
6	Mustafizur et al. (2024)	*Deep Learning for Internet of Things (IoT) Network Security*	Random Forest, Decision Tree, SVM, KNN, ANN, and Gaussian Naïve Bayes.	Generated realistic synthetic bidirectional flows with promising performance.	Limited by the small dataset used.
7	Bipraneel	*A Deep Learning*	Bi-directional LSTM-	Detection accuracy	Requires constant-time

S/N	Author(s)	Title of the Work	Methodology	Findings	Limitations
	(2018)	*Approach for Intrusion Detection in Internet of Things Using Bi-Directional Long Short-Term Memory Recurrent Neural Network*	based intrusion detection at the transport layer.	exceeded 97% with strong recall, precision, FAR, and F1-score.	compression implementation, reducing efficiency.
8	Nithish Babu (2021)	*Network Intrusion Detection Using Machine Learning*	Machine learning implementation using Python.	Some dataset attributes contribute little to intrusion detection and can be ignored.	Future work will apply soft computing techniques for feature selection in adaptive environments.
9	Oumeima et al. (2023)	*An Overview of Machine and Deep Learning-Based Intrusion Detection Systems in the Internet of Things*	CNN, LSTM, and DNN approaches.	Reported accuracies of 99.93% and 98.98% using the same dataset.	Not suitable for existing software-upgradable IoT deployments; high non-recurring engineering (NRE) cost.
10	Baraa et al. (2022)	*Survey of Intrusion Detection Using Deep Learning in the Internet of Things*	Survey of AE, VAE, DBN, CNN, and RNN approaches.	Evaluated previous work using CSE-CIC-IDS2018 and Bot-IoT datasets.	IoT continues to face numerous evolving security threats and attacks.
11	Shaashwat et al. (2024)	*Temporal Weighted Averaging for Asynchronous Federated Intrusion Detection Systems*	Federated learning architecture with model training and testing.	Achieved 99.5% accuracy while improving system throughput.	Additional improvements are still possible.
12	Jiqiang et al. (2024)	*Network Intrusion Attack Detection Based on Deep Learning and URL Analysis in Industrial Internet of Things*	Deep learning with automotive data compression secured using AES-CCM.	Average test accuracy exceeded 98%.	Future work should develop adaptive spatial pyramid structures for improved contextual feature extraction.
13	Nitu et al. (2023)	*An Optimized LSTM-Based Deep Learning Model for Anomaly Network Intrusion Detection*	NSL-KDD, CICIDS, and Bot-IoT datasets with preprocessing and SSA-LSTMIDS.	SSA-LSTMIDS outperformed all comparison models across all datasets.	Reinforcement learning's black-box nature makes prediction and certification difficult.
14	Amjad et al. (2022)	*Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions*	Analysis of feature-, label-, and instance-based challenges in IoT security.	Achieved 95.4% accuracy, 94.81% precision, 97.25% recall, and 96.01% F-measure on NSL-KDD.	Infrastructure, real-time updates, computational constraints, algorithm exploitation, and privacy leakage remain challenges.
15	Geethapriya	*Towards Deep-*	Evaluation using real	Average 95%	Requires industry-wide

S/N	Author(s)	Title of the Work	Methodology	Findings	Limitations
	et al. (2019)	*Learning-Driven Intrusion Detection for the Internet of Things*	network traces.	precision and 97% recall across attack scenarios.	adoption, which may limit innovation.
16	Brook et al. (2024)	*Flow-Based and Packet-Based Intrusion Detection Using BLSTM*	BLSTM models evaluated using the UNSW-NB15 dataset.	Flow-based BLSTM achieved 96% accuracy, outperforming DNN (93%).	BLSTM can provide better protection when deployed in a cascaded configuration.
17	Vandana (2024)	*A Critical Review of Performance Metrics in Intrusion Detection System*	Empirical testing, simulations, and comparative analysis using benchmark datasets.	Provides a comprehensive framework for future IDS evaluation.	Requires extensive field validation under diverse organizational environments.
18	Selvam (2023)	*Deep Learning Towards Intrusion Detection System (IDS): Applications, Challenges and Opportunities*	Survey of DNN, CNN, optimization methods, and related approaches.	Found that 54% of reviewed studies employed Deep Neural Networks.	Presents the categorization methods, toolkits, datasets, and assessment metrics used in the survey.

III. RESEARCH METHODOLOGY

This chapter explains the methods and techniques used to carry out the research in this project. It explains the steps taken to prepare the data before analysis. This chapter also explains the methods used to create the proposed system, including how data was collected, the analysis of the current system, and the analysis of the new system.

Method of Data Collection

In this section, the approach for collecting data will use secondary methods. Because I will use literature reviews from other authors to address an identified gap. Studies show that there is a big need to develop good Deep Learning Models that can detect attacks in datasets. The NSL-KDD dataset will be studied and used to train four different deep learning methods. The overall structure of the methodology is shown below.

NSL-KDD is a simplified version of the original KDD dataset, which was obtained from the Canadian Institute for Cybersecurity. It has the same features as KDD. Each record includes 41 features and one class attribute. Each link is either an attack or a normal link.

NSL-KDD includes 39 different types of attacks, and each attack is grouped into one of four categories.
DOS, R2L, U2R, and Probing. We used 25,192 examples to train our models.

After that, these trained models will be checked and tested with 11,851 examples. Finally, the remaining part of the dataset will be used to check how well the model works.

DOS stands for denial of service, which is when someone stops authorized users from accessing a service, like with a syn flood attack.

R2L means attacking a distant computer to gain access to the victim's machine, like trying to figure out the password.

Performance Metrics in Intrusion Detection

Accuracy

Accuracy is the percentage of cases that were correctly identified, including both the correct positive and correct negative predictions, compared

to all the cases that were checked. Accuracy gives a general idea of how well an IDS works, but it might not be enough when the data is imbalanced, meaning there are way more normal instances than intrusion instances.

$$\text{Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{Total Instances}} \quad (1)$$

One big benefit of being accurate is that it's easy to understand.

It's simple to compute and understand, which is why it works well as a starting point for someone wanting to quickly assess how well an IDS is performing. This metric is easy to use, which makes it simple to evaluate things and compare them quickly. Furthermore, accuracy gives a general idea of how well or poorly an IDS is working. One of the most interesting aspects of accuracy in this case is that it does a great job of comparing different IDS solutions available. This makes it easier to compare different systems or setups, helping you pick the best intrusion detection system for your particular situation. In the case of an Intrusion Detection System, accuracy shows how well the system can tell apart different types of activities, especially the good ones from the bad ones. High accuracy would mean that it was good at recognizing both intrusions and normal activities, making it dependable for network security. Accuracy is often the first thing checked when evaluating how well an IDS is working because it gives a quick idea of how effective the system is.

Precision

Precision, which is also called positive predictive value, shows the percentage of real positive alerts among all the alerts that the intrusion detection system sends. It shows how good the IDS is at finding real attacks without giving too many false warnings.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \quad (2)$$

This accuracy is really suitable when the cost of getting false alarms is very high. For example, running real-time monitoring systems can lead to too many false alarms, which makes it hard for security staff to focus and might cause them to miss actual dangers. High precision means the IDS is expected to be very good at blocking false alarms, so most of the alerts it sends are likely to be real intrusions. This means that precision is a pretty good way to show how good an IDS is at making correct positive predictions.

In real situations, being precise helps ensure that an IDS works well at finding threats without too many false alarms. It will help security analysts decide how much they can trust the alerts sent by the IDS. Organizations focus on accuracy and pay more attention to implementing IDS solutions that provide more useful and trustworthy alerts, helping them improve their security systems. This will also make it easier to compare different IDS models or setups, helping to find out which one works best by catching real threats without too many false alarms.

Recall (Sensitivity)

Recall measures how many of the real intrusion events an IDS correctly detects, compared to all the actual intrusions that happen. It shows that the IDS can find every intrusion and doesn't miss any of them.

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \quad (3)$$

It is especially helpful when security teams need to identify all possible breaches. A high recall value means the IDS can detect most, if not all, of these intrusions and is also effective at stopping threats that are hard to detect. The metric is primarily intended to meet security coverage needs, and failure to obtain intrusion would result in significant vulnerabilities or even larger breaches.

Recall can help in adjusting and improving IDS systems by making it possible to measure the balance between how well the system detects threats and how often it raises false alarms.

For example, increasing the sensitivity of the IDS to improve its ability to detect threats might also lead to

more false alarms, which can make it harder for security teams to focus on real issues. Security professionals can work to find a good balance that improves their ability to detect threats while also keeping their efforts efficient, when looking at both recall and precision to measure how well they find true positives.

Remember, recall is very important when looking at different IDS models or setups and comparing them to each other. An organization can find out which of its systems is better at detecting intrusions in different situations by comparing their recall values. This really helps in choosing and setting up IDS solutions to get the best possible security based on their own unique requirements.

Specificity

Specificity looks at how many real negative alerts are correctly identified compared to all the cases that are actually not intrusions. It shows how well the IDS can recognize normal activities and not raise unnecessary alerts.

$$\text{Specificity} = \frac{\text{True negatives}}{\text{True negatives} + \text{False Positives}} \quad (4)$$

One big benefit of the F1 score is that it gives just one number, which shows how well the system can both catch real problems and not miss too many false alarms. This will be really helpful, especially when there's a disagreement between precision and recall, because the F1 score will balance both and give a full picture of how well the IDS is performing. A high F1 score shows the system is good at balancing accuracy and catching real intrusions, so it identifies threats correctly without making too many false alerts. For practical purposes, the F1 score is seen as a method to compare and evaluate how well different IDS models or setups perform. This helps security experts understand clearly how an IDS is performing in both finding intrusions and reducing false alarms. This shows how important it is in a place where both wrong alarms and missed attacks can have big costs. The F1 score will help make sure that, from the organization's perspective, the security provided by the intrusion detection system is both reliable and thorough.

F1 Score

The F1 score is a balanced measure that takes into account both recall and precision, and it is calculated by finding the harmonic mean of these two values. It's especially helpful when the data set has a mix of classes that aren't balanced.

$$\text{F1 score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

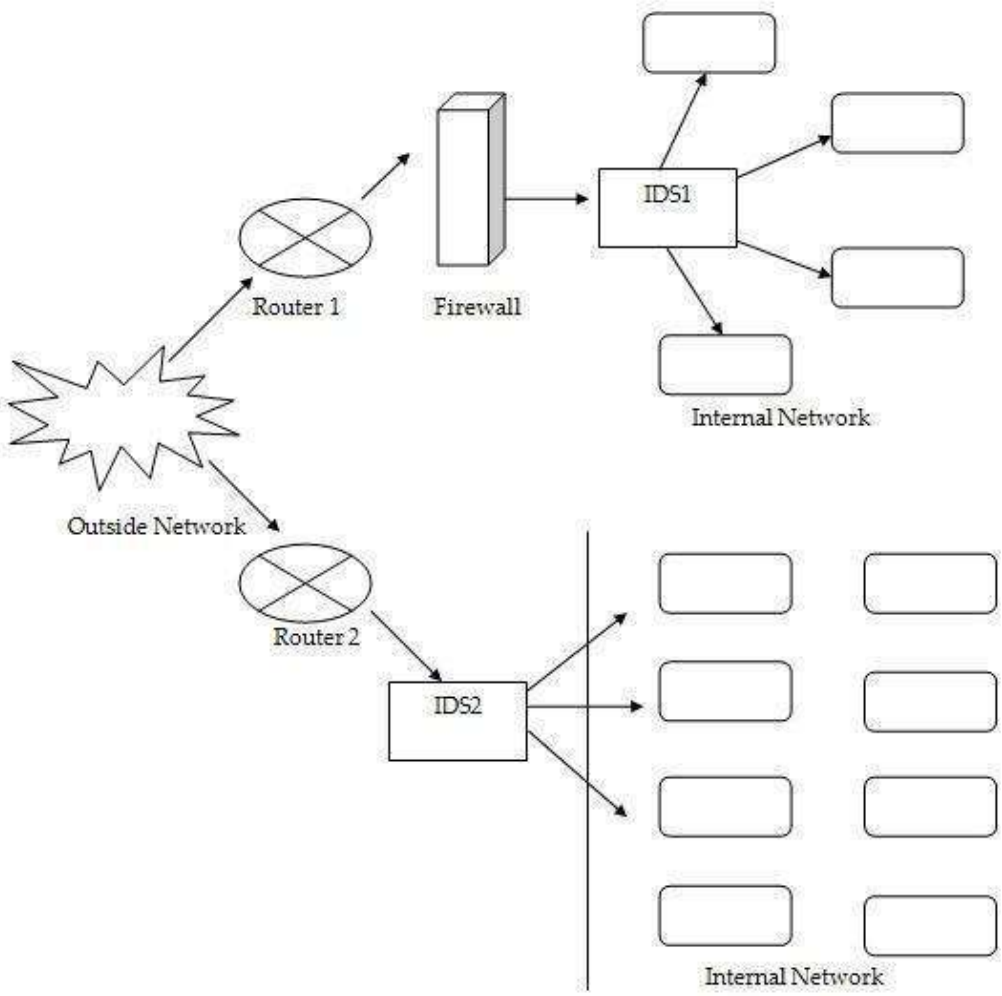
Another big benefit of the F1 score is that it provides a single measure, which helps people understand how the system handles false positives and how well it finds real threats. This will be important when you need to decide between being very accurate or catching more things, because the F1 score finds a balance between the two; that's why it gives a better overall picture of how well the IDS is working. A high F1 score shows the system has a good balance between precision and recall, which means it can accurately detect intrusions without too many false alarms. The F1 score is really helpful for assessing and comparing how well different IDS models or setups perform. It helps security experts see how good an Intrusion Detection System is at finding intrusions or at keeping false alarms to a low level. It's important to have a fair look at performance because false alarms and missed threats can both be costly in the workplace. By focusing more on the F1 score, an organization can ensure that its IDS offers dependable and thorough security protection.

Analysis of Existing System

A network intrusion detection system is a tool used in a network to spot harmful activities. It uses the K-Nearest Neighbor algorithm to detect intrusions. The network traffic is being watched in the network that is part of the subnet. If an attack is noticed, it checks the traffic against a list of known attacks. Then a warning is sent to the administrator. Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS) are the two main types of systems used to detect intrusions. NIDS is placed in the router to detect the movement of network traffic. HIDS runs on an individual system. The two intrusion detection systems have the same job. HIDS also monitors the unauthorized activity. It involves a quick look at the files already in the

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720213

system. Then it checks it against the old system files. If the system detects any unauthorized access or unusual changes, it sends a warning to the administrator. If a file is changed or removed, it shows that something harmful is happening.



Existing Intrusion Detection System Design (Fichtenkamm, 2022)

This method doesn't handle big datasets well because when there are a lot of data points, the time needed to calculate the distance between the new point and every existing point becomes very large, which slows down the algorithm's performance.

The KNN algorithm has trouble working with data that has many dimensions. When there are a lot of dimensions, it's hard for the algorithm to properly calculate the distance between points in each dimension.

We need to scale the features by standardizing and normalizing them before using the KNN algorithm on any dataset. If we don't do that, KNN might make incorrect predictions.

KNN can be affected by noisy data, missing values, and outliers in the dataset. We have to handle the missing data by filling in the blanks ourselves and also get rid of any extreme values that don't fit the pattern.

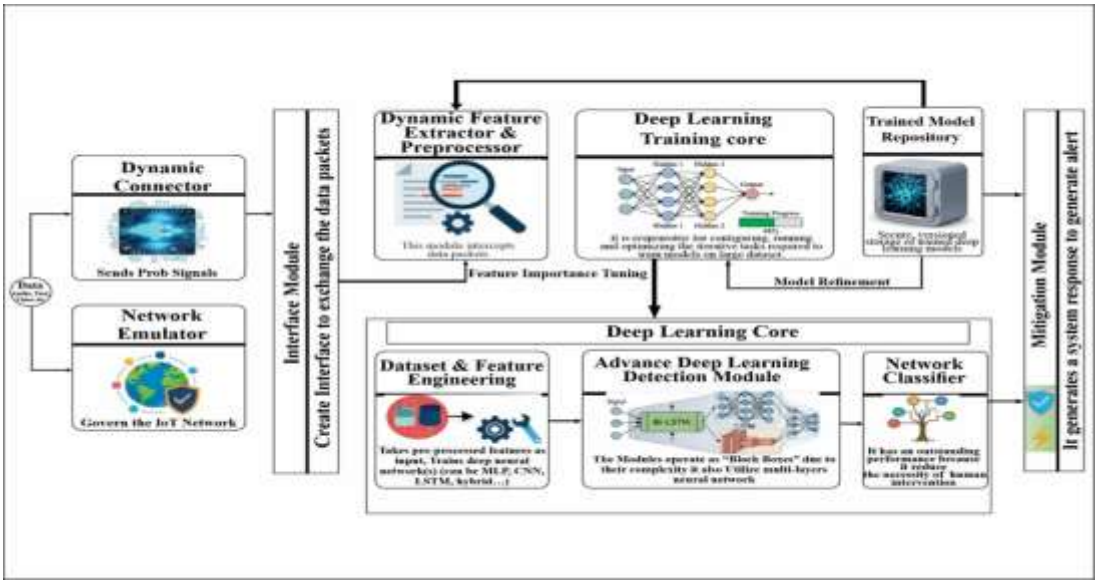
Proposed System

The suggested Deep Learning-based Intrusion Detection (DID) system, shown in Figure 1, is a new and automatic system that learns from data collected

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720213

from the host IoT network and can find intrusions once it has been properly trained.

The system's connector links the simulated network with the requests coming from the IoT network. The simulated network interacts with the feature extractor and the network classifier via an interface module. The feature extractor gets the features from the network packets, which serve as the data used by the deep neural network in the proposed method. The suggested intrusion detection system is constantly changing and gets updated with new features that are found by the classifier update module. Once the intrusion is found, the network classifier sends it to the mitigation step. This step helps lessen the effect of the intrusion.



The Overview of the Proposed System.

The system moves from using fixed rules to using a Deep Learning Core, which makes it smarter at detecting threats. By using BLSTM (Bidirectional Long Short-Term Memory), the system can understand the context of network traffic, which helps it find "Zero-Day" attacks and complex anomalies that a basic firewall might not catch. In Temporal and Sequential Intelligence, the proposed system includes an Advanced Deep Learning Detection Module that uses Bi-LSTM, which lets the system examine data sequences in both forward and backward directions over time. This is a big benefit for IoT security because an attack, such as a slow DDoS or a multi-step exploit, might only show up when you look at the order of events, not when you check each packet alone. In Automated Feature Engineering, it includes a Dynamic Feature Extractor and Preprocessor. This module automatically catches and gets ready data packets for the model. It decreases the need for people to step in and lets the system adjust to various kinds of IoT data like audio, text, and video on its own as it keeps learning and improving. This process includes a training center and a place where trained models are stored. This creates a feedback loop called Model Refinement and Feature Importance Tuning, where the system can be updated with new data, making sure the detection accuracy gets better over time as the network environment changes, and also supporting Proactive Mitigation. The system has a special module for handling issues, and it also keeps an eye on things without being active. This makes sure that once the Network Classifier spots a threat, the system quickly creates an alert and might stop the threat, shifting from just watching to taking action.

Components of the Detection System

The developed proposed intrusion detection system was designed with simplicity in mind, making it easy to set up and use. This is why the detection system

was built using a modular approach. The suggested Deep Intrusion Detection system has three main parts. These are the Communication Module, the Intrusion Detection Module, and the Mitigation Module. These three modules work together.

The communication module handles two-way communication between the sender and the receiver. Any type of communication goes through the IDM module. If any unauthorized access is found, this module sends the packets to the mitigation module.

Communication Module (CM)

The communication module works by using Dynamic Connection, Network Emulator, and Interface module. One of the main things this system offers is that it works without depending on any specific communication protocol. The basic set of rules that control how IoT devices talk to each other is not a problem for the DID system. It was achieved by using a creative design in the communication module. In this section, the way the communication module works has been explained.

Dynamic Connection

The dynamic connector sends probe signals. It also sends signals to all IoT devices in the set network. It also looks at the broadcast beacons, catches the handshake messages, and checks the session requests to find out what communication protocols are being used. It keeps a list of the communication protocols that are currently being used in the IoT environment. The dynamic connector keeps the network interfaces working properly and catches communication signals from various devices. The dynamic connector takes the packets it gets from various network connections and handles them. It uses secondary storage as cache memory to keep the translated packets. When it gets the bit stream from the IoT devices, it uses the right communication protocols from the protocol table to turn the bit stream into network packets with the correct protocol.

Network Emulator

The main network protocols that control how IoT networks work are shown in the protocol table. It includes all the important details about the network. Instead of linking directly to the network, the suggested method uses a new approach to keep communication going. That is done using a network emulator, as mentioned in Hou et al.(2022). It has a Virtual Network Client (VNC) module that gets the packets from the cache memory in the dynamic connector, picks the right network protocol from a list of protocols, handles the packets based on the chosen protocol, and then sends them to the correct IoT device.

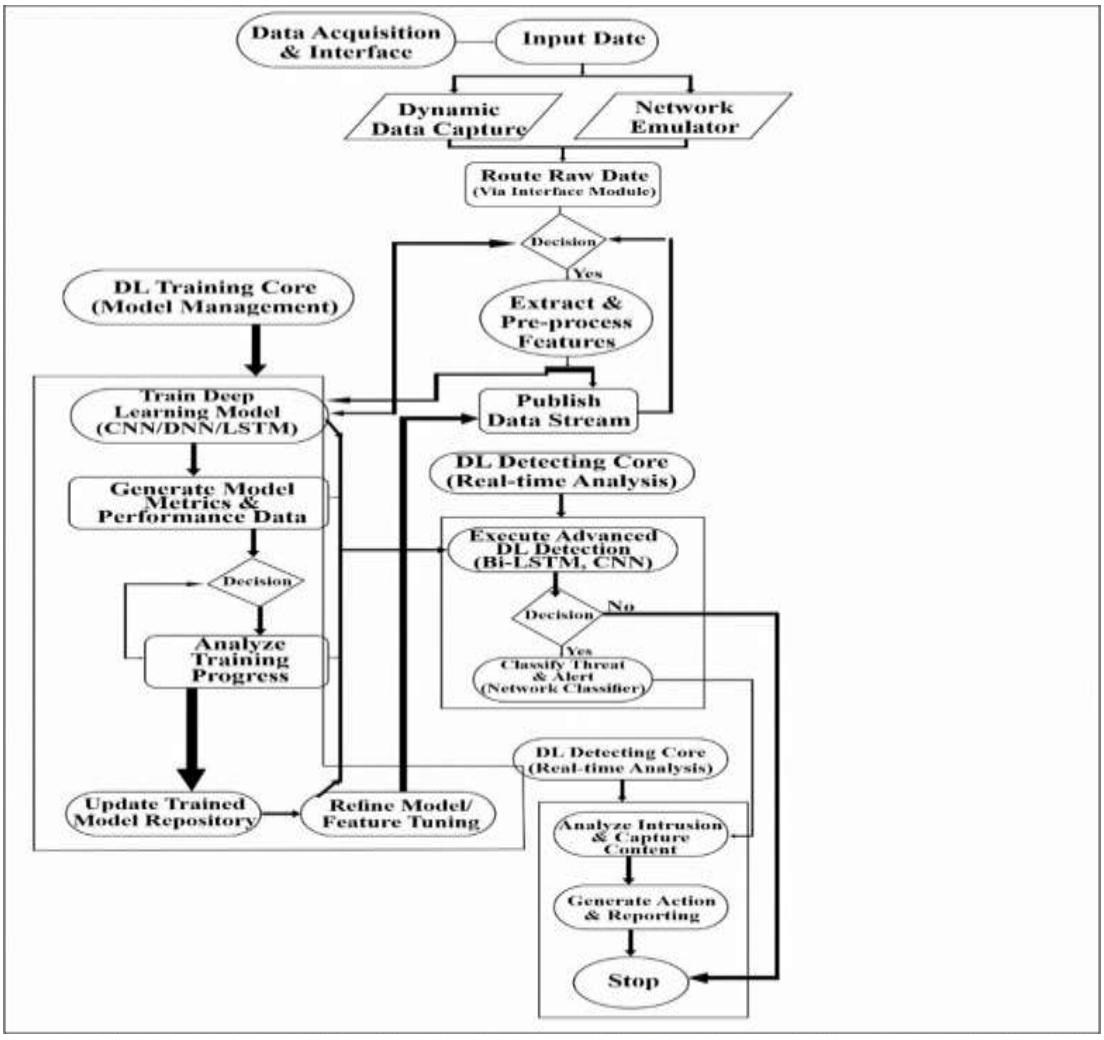
Interface Module

The interface module makes it possible to send and receive data packets. It manages how data is sent and received between the communication module and the intrusion detection module. The interface module manages the dynamic connector and the network emulator.

Activity Diagram

Activity diagrams are pictures that show how a process works by breaking it down into steps and actions. They also let you show decisions, repeated steps, and things happening at the same time. In the Unified Modeling Language, activity diagrams are used to show the step-by-step processes involved in the business and operations of different parts of a system. Here is the activity diagram for the system that has been suggested.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1720213



An activity diagram shows how decisions are made by checking different conditions.

IV. CONCLUSION

The fast-growing Internet of Things (IoT) has created a huge opportunity for cyber threats, making important systems and personal information more at risk from advanced attacks. Traditional network intrusion detection systems (NIDS) use fixed rules and manually created features, which means they can't find new attacks like zero-day exploits and changing malware that are common today. Moreover, the diverse and fast-moving data from IoT devices using different protocols like MQTT and CoAP creates complex patterns that regular systems struggle to handle properly. There is a strong need for a detection system that can: look at network traffic as a steady, two-way flow to get a complete picture. Lower the number of false alarms that cause "alert fatigue" for network administrators. Work well against the changing and urgent threats that are specific to IoT systems. The method that will be used to collect data is through secondary sources. Because I will use literature reviews from other authors to address an identified gap. Studies show that there is a strong need to develop good Deep Learning Models that can detect attacks in datasets. The NSL-KDD dataset will be studied and used to train four different Deep Learning methods. In the future, more methods using deep learning will be introduced to help society safely guide information and develop new ideas.

REFERENCES

[1] E. A. Aleng, S. Omega, and A. M. Michael, "Analysis of Vulnerability Factors and Severity Levels of Ransomware Strike on Organizational Data," *IRE Journals*, vol. 8, no. 9, pp. 1360–1367, Mar. 2025. ISSN: 2456-8880. doi: https://doi.org/10.64388/IREV8I9-1707466-7744.

[2] O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9463–9472, 2020.

[3] B. Roy, *A Deep Learning Approach for Intrusion Detection in Internet of Things Using Bi-Directional Long Short-Term Memory Recurrent Neural Network*. School of Computing, Engineering and Mathematics, Dec. 2018.

[4] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 45–59, Mar. 2020.

[5] N. Islam, F. Farhin, I. Sultana, M. S. Kaiser, M. S. Rahman, M. Mahmud, A. S. Hosen, and G. H. Cho, "Towards Machine Learning Based Intrusion Detection in IoT Networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801–1821, 2021.

[6] J. L. Leevy and T. M. Khoshgoftaar, "A Survey and Analysis of Intrusion Detection Models Based on CSE-CIC-IDS2018 Big Data," *Journal of Big Data*, vol. 7, no. 1, pp. 1–19, 2020.

[7] J. R. Vacca, *Network and System Security*. Elsevier, 2013.

[8] J. Yin, M. Tang, J. Cao, H. Wang, M. You, and Y. Lin, "Vulnerability Exploitation Time Prediction: An Integrated Framework for Dynamic Imbalanced Learning," *World Wide Web*, pp. 1–23, 2021.

[9] J. Yin, M. Tang, J. Cao, M. You, H. Wang, and M. Alazab, "Knowledge-Driven Cybersecurity Intelligence: Software Vulnerability Co-Exploitation Behaviour Discovery," *IEEE Transactions on Industrial Informatics*, pp. 1–9, 2022. doi:10.1109/TII.2022.3192027.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.

[11] M. A. Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of Malicious Activities in Industrial Internet of Things Based on Deep Learning Models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, Aug. 2018.

[12] M. Fichtenkamm, G. F. Burch, and J. Burch, "Cybersecurity in a COVID-19 World: Insights on How Decisions Are Made," *ISACA Journal*, 2022.

[13] M. J. Page *et al*., "Updating Guidance for Reporting Systematic Reviews: Development of the PRISMA 2020 Statement," *Journal of Clinical Epidemiology*, vol. 134, pp. 103–112, Feb. 2021. doi:10.1016/j.jclinepi.2021.02.003.

[14] M. S. Kumar, J. Ben-Othman, and K. Srinivasagan, "An Investigation on WannaCry Ransomware and Its Detection," in *Proc. IEEE Symposium on Computers and Communications (ISCC)*, 2018, pp. 1–6.

[15] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, 2009, pp. 1–6.

[16] M. Rahman Shahid, *Deep Learning for Internet of Things (IoT) Network Security*. Institut Polytechnique de Paris, 2021. NNT: 2021IPPAS003. tel-03193266.

[17] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An Optimized LSTM-Based Deep Learning Model for Anomaly Network Intrusion Detection," *Scientific Reports*, vol. 15, p. 1554, 2025. doi: https://doi.org/10.1038/s41598-025-85248-z.

[18] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A Deep Learning-Based Intrusion Detection Framework for Securing IoT," *Transactions on*

Emerging Telecommunications Technologies, vol. 33, no. 3, p. e3803, 2022.

[19] P. Vimalachandran, H. Liu, Y. Lin, K. Ji, H. Wang, and Y. Zhang, "Improving Accessibility of the Australian My Health Records While Preserving Privacy and Security of the System," *Health Information Science and Systems*, vol. 8, no. 1, pp. 1–9, 2020.

[20] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial Attacks Against Network Intrusion Detection in IoT Systems," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10327–10335, 2020.

[21] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed, and F. Anwar, "Effective Combining of Feature Selection Techniques for Machine Learning-Enabled IoT Intrusion Detection," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 31381–31399, 2021.

[22] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," *IEEE Access*, vol. 7, pp. 38597–38607, 2019.

[23] S. T. Brugger and J. Chow, "An Assessment of the DARPA IDS Evaluation Dataset Using Snort," *UCDAVIS Department of Computer Science*, vol. 1, p. 22, 2007.

[24] O. Sarjiyus, M. B. El-yakub, and E. A. Aleng, "Interlayered Security Model for Cloud Computing in Internet of Things (IoT) Domain," *Journal of American Science*, vol. 21, no. 8, pp. 30–41, 2025. ISSN: 1545-1003 (Print), ISSN: 2375-7264 (Online). doi:10.7537/marsjas210825.02.

[25] J. Shareena, A. Ramdas, and H. AP, "Intrusion Detection System for IoT Botnet Attacks Using Deep Learning," *SN Computer Science*, vol. 2, no. 3, pp. 1–8, 2021.

[26] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[27] T. Huang, Y. J. Gong, W. N. Chen, H. Wang, J. Zhang, "A Probabilistic Niching Evolutionary Computation Framework Based on Binary Space Partitioning," *IEEE Transactions on Cybernetics*, vol. 52, no. 1, pp. 51–64, 2022. doi:10.1109/TCYB.2020.2972907.

[28] G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," *Sensors*, vol. 19, no. 9, p. 1977, 2019.

[29] Y. Zhang, Y. Shen, H. Wang, Y. Zhang, and X. Jiang, "On Secure Wireless Communications for Service-Oriented Computing," *IEEE Transactions on Services Computing*, vol. 11, no. 2, pp. 318–328, 2015.

[30] Y. S. Almutairi, B. Alhazmi, and A. A. Munshi, "Network Intrusion Detection Using Machine Learning Techniques," *Advances in Science and Technology Research Journal*, vol. 16, no. 3, pp. 193–206, 2022. doi: https://doi.org/10.12913/22998624/149934.

[31] M. Zeeshan, Q. Riaz, M. A. Bilal, M. K. Shahzad, H. Jabeen, S. A. Haider, and A. Rahim, "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," *IEEE Access*, vol. 10, pp. 2269–2283, 2021.

[32] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019.