IoT Security Using Machine Learning Methods

by

Seyedamiryousef Hosseini Goki

A Project Submitted in Partial Fulfillment of
the Requirements for the Degree of

Master of Science

in the Department of Computer Science

University of Victoria

IoT Security Using Machine Learning Methods

By

Seyedamiryousef Hosseini Goki

Supervisory Committee

Dr. Kui Wu, Supervisor

(Department of Computer Science)

Dr. Jianping Pan, Departmental Member

(Department of Computer Science)

ABSTRACT

The rapid growth of internet-connected devices has made robust cybersecurity measures essential to protect against cyber threats. IoT cybersecurity includes various methods and technologies to secure internet-connected devices and systems from cyber attacks. The unique nature of IoT devices and systems poses several challenges to cybersecurity, including limited processing power, minimal security features, and vulnerability to attacks like DoS and DDoS. Cybersecurity strategies for IoT include encryption, authentication, access control, and threat detection and response, which utilize machine learning and artificial intelligence technologies to identify and respond to potential cyber attacks in real-time. The report discusses two projects related to cybersecurity in IoT environments, one focused on developing an intrusion detection system (IDS) based on deep learning algorithms to detect DDoS attacks, and another focused on identifying potential abnormalities in IoT networks using a fingerprint. These projects highlight the importance of prioritizing cybersecurity measures to protect against the growing number of cyber threats facing IoT devices and systems.

Contents

List of Tables

List of Figures

ACKNOWLEDGMENT

I am incredibly grateful to Dr. Kui Wu, who invested an enormous amount of time and effort to provide guidance and improve the writing of this project. Their dedication and support were instrumental in helping me achieve my goals, and I cannot express my appreciation enough.

Also, I want appreciate my colleagues who helped me a lot in these research projects to publish our work.

Dedication

I dedicate this project to my wife and my parents who have always supported and encouraged me.

Chapter One

Introduction

As the number of internet-connected devices continues to grow, the need for robust cybersecurity measures to protect against cyber threats has become increasingly important. IoT cybersecurity refers to the methods and technologies used to secure internet-connected devices and systems from cyber attacks. The unique nature of IoT devices and systems presents several challenges to cybersecurity. IoT devices often have limited processing power and memory, making them more vulnerable to attacks such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Additionally, many IoT devices are designed with minimal security features, making them easy targets for hackers.

Cybersecurity for IoT involves a range of strategies, including encryption, authentication, access control, and threat detection and response. Encryption helps protect the privacy and integrity of data transmitted between IoT devices, while authentication and access control ensure that only authorized users can access and interact with IoT systems. Threat detection and response involve the use of technologies such as machine learning and artificial intelligence to identify and respond to potential cyber attacks in real-time. Ensuring strong cybersecurity for IoT is crucial for a range of industries, including healthcare, manufacturing, and transportation, as IoT devices are increasingly used to control critical systems and infrastructure. As the number of IoT devices continues to grow, it is essential to prioritize cybersecurity and implement robust measures to protect against cyber threats. In this report, we are going to discuss two projects that we have done in this domain.

For the first project, we understood that as the protected design of computer networks shifts towards unrestricted connection, the network gains increased flexibility, widespread coverage, and cognitive capabilities. These improvements have expedited the progress of advanced internet technologies, such as big data, cloud computing, the Internet of Things (IoT), and networks that can be programmed. However, the possibility of a DDoS attack caused by centralized control becomes more evident with software-defined network architecture [1]. There are two types of IDS, namely vulnerability assessment and anomaly detection. Vulnerability assessment identifies

attacks through recognized signatures, while anomaly detection detects unusual attacks based on normal usage patterns. Detecting unknown threats is challenging using abuse and anomaly detection. Although anomaly detection is helpful in identifying them, it has a high rate of false alerts because defining a range of typical usage patterns is complex [2].

Currently, identifying DDoS attacks is considered one of the most difficult network attack types [3]. These attacks aim to exhaust the target network or platforms, rendering the victim unable to carry out routine operations. DDoS attacks can be divided into two categories: resource bandwidth-consuming attacks and system resource-consuming attempts. Resource bandwidth attacks utilize many zombie hosts to rapidly generate a large amount of traffic, which is then directed towards the victim's server, completely consuming its network bandwidth resources.

One type of attack that can occur is flooding, which involves sending a large number of repeated packets such as UDP, TCP, and ICMP packets. This flooding attack can result in UDP flooding, TCP flooding, or ICMP flooding. Another type of attack is amplification, which can be accomplished through reflection, such as in DNS reflection amplification attacks. In system resource attacks, attackers can take advantage of protocol vulnerabilities to use the victim's host resources [4].

The traditional methods of network analysis and data processing face several challenges and difficulties, such as the reliability of the analysis and the real-time handling of vast amounts of data. In cellular networks, the behavior of network traffic can be extremely complex due to various factors, including device mobility and network heterogeneity. Deep learning has been effective in dealing with large-scale data analysis and discovering complex patterns. Networking researchers are utilizing deep learning techniques for traffic monitoring and analysis applications, such as traffic prediction and categorization, due to their success [5]. Traditional machine learning methods based on expert-generated features are outdated and unable to keep up with the increasing number of applications and the ever-changing nature of mobile traffic [6].

As cyberattacks become more advanced, it is getting harder to identify them in various sectors such as industry, national defense, and healthcare. Traditional intrusion detection systems are not able to recognize complex attacks with unconventional patterns. Attackers are able to avoid detection by pretending to be normal users. Deep Learning (DL) has the potential to address these challenges [2]. DL-based intrusion detection does not rely on a significant amount of malicious

activity or a predefined set of typical activities to establish detection rules. Instead, DL autonomously identifies intrusion patterns through empirical data learning.

The main objective of our first project is to examine innovative techniques in the field of metainnovation by utilizing an IDS (Intrusion Detection System) based on deep learning. The primary focus of the project is to detect DDoS (Distributed Denial of Service) attacks in IoT (Internet of Things) environments using various machine learning algorithms such as MLP (Multi-Layer Perceptron), LSTM (Long Short-Term Memory), BiLSTM (Bidirectional LSTM), KNN (K-Nearest Neighbors), SVM (Support Vector Machine), LDA (Linear Discriminant Analysis), DT (Decision Tree), and RF (Random Forest). The NSL-KDD (Network Security Laboratory-Knowledge Discovery and Data Mining) dataset is used in this project, and it consists of two labels, 0 and 1, representing abnormal and normal behavior, respectively. The findings of the classification process are presented using a confusion matrix.

In the second project we realized that anomalies in an internet of things (IoT) network provide important information about network traffic and patterns. The presence of anomalies does not necessarily suggest a destruction of the network, but they do offer valuable insight into the nature of the issues relating to anomalies in the network. Thus, using a fingerprint is one method of detecting irregularities in IoT-connected devices. The fingerprint is one of the most important components of the network for identifying IoT devices attached to it. Researchers face a number of challenges in identifying potential abnormalities in networked systems. Active fingerprinting provides additional information regarding connected devices, but it limits its use since it must be able to identify the device and apply security regulations when a network abnormality occurs. It may therefore be more appropriate to use the passive fingerprinting technique on any network-connected device instead of using the active fingerprinting technique. As there is no additional monitoring traffic sent to the network with the passive fingerprint approach, the network capacity is also utilized far less. A passive fingerprinting approach uses properties of USB hardware, features from protocol headers, and unique deviations from device clocks to create unique fingerprints for a device.

Identifying abnormalities in IoT devices on a network can help manage network resources and security rules effectively. If a collection of characteristics can be utilized to describe the device's typical behavior, the model may be the main foundation for identifying aberrant device behavior

of the same kind. Anomaly diagnosis can reveal consequences of device errors/faults other than assaults, which are often hidden from security technologies. The selection of a security strategy in this situation is dependent on an accurate identification of the type of equipment. A bad forecast not only contributes to the slowdown of the device but also compromises the security of the network. Our second project aims to identify devices in a network in order to facilitate the identification of unusual behavior in IoT devices. Using machine learning, we propose a feature-based approach to introduce a fingerprint technique and identify unusual device behaviors.

1.1 Structure of the Report

The rest of the report is organized as follows:

Chapter two of the report provides a condensed overview of the previous research that has been conducted in the area being studied.

Chapter three of the report is dedicated to introducing the first project and outlining the research methodology employed to carry out the investigation as well as results obtained.

Chapter four of the report is focused on presenting the second project, including the methodology employed to conduct the research and the outcomes of the investigation.

Chapter five represents the concluding section of the report, which summarizes the key findings and presents the implications of the study. Additionally, this chapter outlines the limitations of the research, highlights the potential areas for improvement, and recommends directions for future research.

Chapter Two

Related Work

This chapter provides an overview of the related work in the specific area being studied. This includes a summary of existing ideas and approaches that have been proposed and implemented by previous researchers in this field for each project. The purpose of this chapter is to provide a comprehensive understanding of the current state of the research, highlight the gaps that need to be addressed, and identify opportunities for further exploration. By analyzing the existing literature, the projects aim to build upon the knowledge that has already been established and contribute to the development of new and innovative ideas.

2.1 Literature Review for the first Project

Currently, Distributed Denial of Service (DDoS) attacks pose the most prevalent and potent threat to businesses, and their attractiveness as a tool for hackers is on the rise [7]. In 2018, GitHub experienced one of the most massive DDoS attacks in history, which received significant media attention. This attack severely impacted the security of one of the three pillars of the CIA security triad, namely "presence." [8]

Attackers utilize numerous dump terminals, computers, and botnets to carry out DDoS attacks simultaneously, causing a depletion of the targeted system's resources and making all services inaccessible. There are various legal and efficient technologies available that can be employed for performing DDoS attacks on both small and large scales.

A recent DDoS attack [8] misused the legitimate Memcached utility, which is typically used to reduce the burden on supporting Internet services. The attacker exploited Memcached items and fabricated IP addresses, directing Memcached responses to target addresses at a rate of 126.9 million packets per second, overwhelming the target system's capacity. Moreover, using fake IP addresses makes it challenging to trace DDoS attacks [9].

There are several studies available on Intrusion Detection Systems (IDS). Manso et al. [10] suggested an IDS based on software-defined networks, which identifies DDoS attacks and sends alerts to sensor nodes. Karim et al. [11] evaluated the effectiveness of Snort-based IDS in a network environment. Xu et al. [12] proposed a deep forest-based model for detecting and defending against DDoS attacks on smart nodes, with a focus on significant data context. Additionally, researchers have explored machine learning-based anomaly detection techniques for commercial sensor networks [13].

Lv et al. [14] suggest that it is feasible to utilize deep learning (DL) to tackle security challenges in CITS Digital Twins (DTs). In Lv et al.'s proposed research [16], they investigate the use of Digital Twins in manufacturing smart devices and enhance their fault diagnosis performance. Liu et al. Sun et al. [18] explain a lightweight communication approach for remote control. The authors are of the opinion that evaluating the functionality of the system demonstrates its suitability and feasibility for situations that do not demand promptness but necessitate a high degree of anonymity.

Mehbodniya et al. [19] proposed the use of Naive Bayes, random forests, and logistic regression as machine learning techniques to identify fraudulent identity attacks. Cao et al. [20] formulated an optimization model for SAGIN-IoV service needs and proposed an improved algorithm. Sun et al. [21] investigated a lifelong learning framework named Generalized Lifelong Spectral Clustering (GL22SC). Ahmadi et al. [22] put forward that deep-Q-reinforcement learning ensembles can employ a combined deep-Q-reinforcement learning ensemble based on spectral clustering (DQRE-SCnet) to select a subset of devices in each communication round. Sun et al. [23] described Flexible Clustered Lifelong Learning (FCL3), which comprises two knowledge libraries: a feature learning library and a model knowledge library.

Liu et al. [24] optimized the SFERNN by minimizing the cross-entropy loss on the source branches and the distributional discrepancy between the source and target branches. Mehbodniya et al. [25] developed a digital signature framework using the modified Lamport Merkle Digital Signature method for generating and verifying digital signatures. Zhang et al. [26] utilized an improved gray wolf optimization (IGWO) algorithm to construct a safety early-warning model for electric vehicle (EV) charging. Dong et al. [27] developed the Knowledge Aggregation-induced Transferability Perception (KATP) technique, which is an innovative effort to differentiate between transferable

and untransferable knowledge across domains. According to Yang et al. [28], a negative survey approach can be employed to safeguard aggregated vehicle fuel consumption data from time series-based differential attacks. Wu et al. [29] proposed an algorithm that combines interactive machine learning and active learning to predict HBR.

Khaliq et al. [30] propose parking recommender systems using local differential privacy (LDP) and elliptic curve cryptography (ECC), but there are still some research gaps in this area. Wu et al. [31] found that recent SBR prediction models have not performed well due to mislabeled instances in five publicly available datasets. Kim et al. conducted several KDD computer vision experiments to divide the dataset into four groups based on two or more independent variables, namely, attack and benign. Instead of focusing on primary groups, they concentrated on specific attacks within the same area and created a DL model for detecting DoS in both databases. [2]

Wang et al. proposed a real-time DDoS attack detection system for the software-defined Internet of Things. They utilized an updated firefly algorithm to improve the performance of the convolutional neural network (CNN) in detecting DDoS attacks. The system was able to accurately detect both normal and malicious traffic with over 99% accuracy [4]. Liu et al. proposed a two-level DDoS attack detection approach based on information entropy and deep learning. The first level identified suspicious elements and ports with coarse granularity, while the second level used a CNN model to distinguish regular traffic from suspicious traffic at the packet level. The proposed method achieved a detection accuracy of 98.98% in an SDN context [1]. Additionally, Zheng et al. [32] discovered that class imbalance negatively affected the accuracy of SBR prediction.

Zhang et al. [33] employed a random forest classifier to create a Just-in-Time defect prediction model based on data from six open source projects. Liu et al. [34] developed a DeepBAN communication framework that was found to improve the energy efficiency of dynamic WBANs by 15% compared to stochastic scheduling schemes. Gera et al. [35] used a novel dominant feature selection algorithm to extract the dominant feature set. Liu et al. [36] explored smart contract vulnerability detection using graph neural networks and expert knowledge. Zhang et al. [37] proposed a solution for rapid video prefetching and traffic reduction. Zong et al. [38] applied a multiscale grouping (MSG) structure and a 3D-BoNet instance segmentation model to a 3D point cloud tunnel dataset, using their new detection method.

Varmaghani et al. [39] proposed a technique to optimize energy consumption in dynamic wireless sensor networks using fog computing and fuzzy multiattribute decision-making. Singh et al. [41] developed algorithms for mobility and traffic management that are both flexible and high-performing through the use of sophisticated fuzzy logic. Xie et al. [42] have suggested various heuristic or metaheuristic algorithms/methods for solving the NP-hard problem. Li et al. [43] have summarized constructive interference (CI) and explained how it can benefit 1-bit signal design by considering traditional undesired multiuser interference and interference caused by imperfect hardware components.

Ghanbari et al. [45] improved VFD detection by developing feature extraction methods using a mother wavelet. Ramtin et al. [48] investigated the maximum damage a DDoS attacker can cause without being detected by a detection system at the network edge. They examined two classical classifiers based on hypothesis testing, considering whether the detector knows the distribution of attack traffic or not. The authors mathematically showed that the maximum damage follows a square root law and provided empirical data to illustrate their findings. Zheng et al. [49] proposed a detailed visual reasoning model that introduces different levels of knowledge representation into deep learning. They developed a multilayer semantic representation network for sentence representation [50]. Yu et al. [51] demonstrated the feasibility of inferring keystrokes on touch screens using a side-channel attack with an off-the-shelf smartphone. Kong et al. [52] proposed user authentication to protect user privacy and offer personalized services. The Breast Cancer Ultrasound Dataset was used as input for a two-dimensional contourlet by Hajipour et al. [53]. Zhao et al. [54] presented a fog-based smart grid scheme with sensible pricing and packing. Finally, Meng et al. [55] proposed a method for adaptive neural tracking control of an uncertain two-link rigid-flexible manipulator under vibration amplitude constraints.

Mishra et al. [67] conducted a comparison of intrusion detection and prevention methods for minimizing DDoS attacks and placed emphasis on detection techniques. Ghayvat et al. [79] proposed a strategy that incorporates a blockchain-based nondisclosure method with a two-step authentication architecture and an elliptic curve cryptography-based cryptographic signature framework to safeguard the ecosystem against DoS and DDoS attacks. In another study, Mirsky et al. [80] demonstrated a plug-and-play network intrusion detection system that can autonomously

and efficiently learn to detect attacks on the local network using Kitsune, a collaborative algorithm that utilizes autoencoders to differentiate between normal and anomalous traffic patterns.

In this section, we tried to provide a comprehensive summary of the latest research in the field of IoT intrusion detection. With the widespread adoption of IoT devices, the security of these devices has become a major concern. As a result, researchers have been working tirelessly to come up with innovative solutions to detect and prevent intrusion into IoT systems.

2.2 Literature Review for the second Project

Detecting anomalies in an Internet of Things (IoT) network is crucial in understanding network traffic and patterns. While the presence of anomalies does not necessarily imply that the network is being compromised, it provides valuable insights into the nature of the issues related to anomalies in the network. To identify irregularities in IoT-connected devices, one of the effective methods is to use a fingerprint, which is an essential component of the network for identifying IoT devices attached to it. However, identifying potential abnormalities in networked systems presents several challenges for researchers.

IoT anomaly detection studies did not focus on Euclidean distance involved in high-dimension information without upper limit. Aljawarneh et al. [96] for instance, provided a gaussian-based technique for feature extraction of an anomaly in the Internet of Things. In order to identify intrusions, IoT nodes with Euclidean distance were used. To train their classification technique, they used the K-nearest Neighbor algorithm.

Cheng et al. [97] introduced the HS-TCN method for anomaly detection as a semi-supervised technique. Using convolutional neural networks, it performs the task. A feature in their model was labeled to train on unlabeled data. In their discussion of fingerprinting techniques, Kim et al. [98] presented a fingerprinting method based on the edge of IoT in a cloud environment. They used packet analysis and packet placement history to identify anomalies. Additionally, Blaise et al. [99] proposed a fingerprinting technique for identifying Bot anomalies. This technique involves the discovery of the host distribution frequency, the detection of anomalies based on machine learning, and the categorization of Bots based on behavior.

For identifying illicit activity in IoT services, Fang et al. [110] introduced the DIB technique in medical services. It is responsible for managing personnel states and anomaly operations. Using fuzzy machine learning, they trained and classified their material.

In this section, we present a comprehensive overview of the literature that has been conducted for our second project. By presenting this literature review, we hope to provide a solid foundation for our second project and to build on the existing body of knowledge in the field. Our review serves as a starting point for our research, allowing us to better understand the current state of research, identify research gaps, and develop appropriate research questions and methodologies.

Chapter Three

Project One

ML-DDoSnet: IoT Intrusion Detection Based on Denial-of-Service Attacks Using Machine Learning Methods and NSL-KDD

The security of the Internet of Things (IoT) is a complex issue that involves protecting datagrams with integrity, confidentiality, and authentication services, as well as safeguarding the network from external threats. Given the heterogeneous technologies and data processing methods used by IoT devices, standard security solutions may not be sufficient, and intelligent procedures that can handle various levels of data flow are necessary. To address this issue, a project called "ML-DDoSnet: IoT Intrusion Detection Based on Denial-of-Service Attacks Using Machine Learning Methods and NSL-KDD" was developed, which focuses on using deep learning-based intrusion detection systems (IDS) to identify DDoS attacks. According to tests, BiLSTMs are better for binary classification (normal/attacker), while sequential models like LSTM or BiLSTM are more effective at detecting complex attacks in multiclass classifiers. However, further research is needed to address specific challenges, such as the impact of different data processing techniques on IDS. Among the different models tested, the BiLSTM approach was found to be the most reliable and suitable solution for detecting DDoS attacks in IoT.

3.1 Methods and Material

3.1.1 Distributed Denial-of-Service (DDoS) Attack

DDoS attacks refer to distributed denial-of-service attacks. These attacks exploit the limitations of network resources, such as the infrastructure that underpins a company's website. A DDoS attack involves flooding the targeted online resource with many requests to overload its capacity to handle multiple demands, thus causing it to malfunction. The traffic that floods the target comes from different sources, making it challenging to stop the attack by blocking a single source [86]. A DoS or DDoS attack can be likened to a large crowd of people surrounding a shop's entrance,

making it difficult for genuine customers to visit and disrupting business operations. Multiple attack machines can generate more attack traffic than a single attack machine, and shutting down multiple attack machines is more difficult than shutting down a single attack machine. The activity of each attack machine can be stealthy, making it harder to detect and shut down. As the overwhelming signal comes from various sources, relying solely on ingress filtering may not be sufficient to stop the attack. Additionally, it can be hard to distinguish between regular user traffic and DoS attacks when originating from various locations [87].

The utilization of computer networks that are connected to the Internet is common in conducting DDoS attacks. These networks are composed of malware-infected PCs and other devices, such as Internet of Things (IoT) equipment, and are controlled remotely by an intruder. A botnet refers to a group of bots, which are standalone devices. The attacker can send remote commands to each bot to launch an attack using the botnet. Each bot queries the IP address of the victim's server or network, and overwhelming it could result in a denial-of-service attack against normal traffic. Since each bot operates as an Internet node, distinguishing between attack traffic and normal traffic can be challenging [88].

DDoS attacks focus on different layers of a network connection. To comprehend other DDoS attacks, it's crucial to comprehend how a network connection is formed. A network connection on the internet comprises multiple layers or components. Each layer in the model has a specific purpose, similar to how each layer in a house has a particular function. The OSI model, a theoretical framework consisting of seven layers, is used to explain network connections as depicted in Figure 3-1.

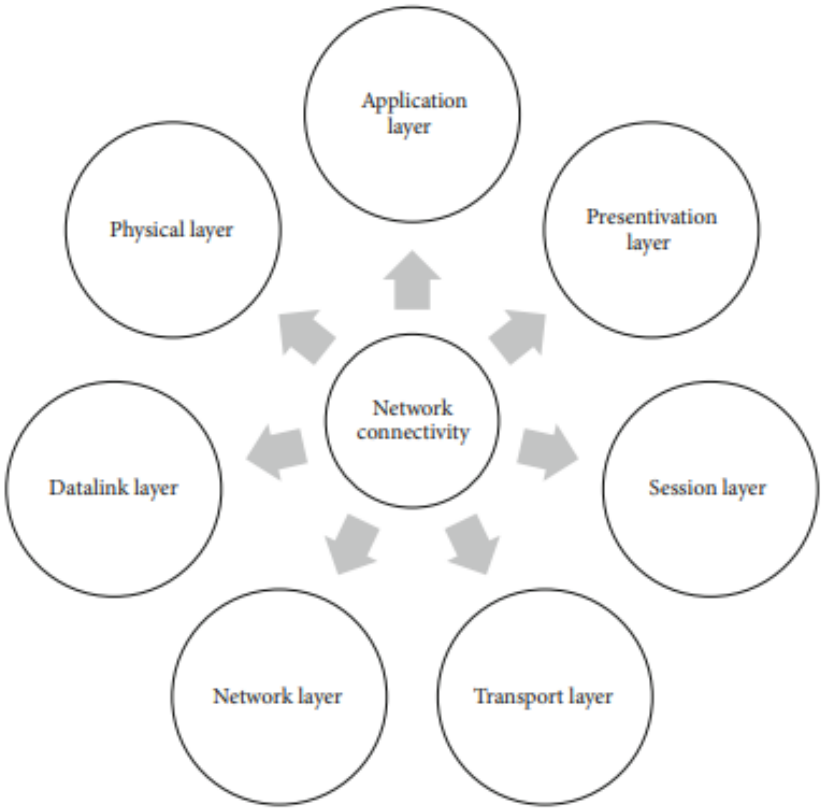

Figure 3-1: The 7-layer conceptual framework for describing network connectivity.

Although flooding a target device or network with traffic is a common characteristic of DDoS attacks, attackers may employ different attack methods depending on the target's defenses. There are three types of DDoS attacks, and intruders may use multiple attack vectors or switch between different types of attacks in response to the target's countermeasures. This information comes from sources [86-88].

3.1.2 Feature Extraction

The process of preparing data for network traffic classification involves three main stages: data preprocessing, training, and validation. During the data preparation stage, raw data is collected from various sources such as recorded network traffic, checked network information, and sampled packet data, and transformed into a properly formatted dataset with appropriate labels [89]. Once

the preprocessing is complete, the specific machine learning technique and problem domain will dictate the primary method used for training. Feature extraction, which is a crucial step in building a classification model, is then carried out on the processed data. The feature extraction process aims to improve the classification model's performance by removing irrelevant features and reducing the number of attributes in the dataset to speed up the training process. After the feature extraction, the resulting dataset, which has a suitable collection of features, is separated into two sets for training and testing. The machine learning technique chosen automatically learns the model parameters and produces a classifier during the training phase.

Most learning algorithms require the human selection of hyperparameters. The appropriate values of hyperparameters for a particular situation must be determined. Past experience, values from other successful applications, validation techniques, and rules of thumb are all used to select appropriate hyperparameters. Using the specified learning method, separate classifiers targeting different groups of hyperparameters can be trained using the training set. The performance of the classifiers developed is then evaluated using a validation set that does not overlap with the training set. The best-performing hyperparameters are used to construct the final classifier. In the testing phase, the performance of the final classifier is evaluated based on the predictions it makes using the defined activity [90].

3.1.3 Multilayer Perceptron

An artificial neural network (ANN) imitates the structure and operation of biological neural networks. The system is composed of artificial neurons arranged in layers and connected by weighted edges, as shown in Figure 3-2. Each neuron processes and aggregates the input signals using an activation function to generate an output signal. The output signals are then passed on to the next layer, until the final output layer is reached [91]. Hidden layers between the input and output layers perform calculations and processing. During the training phase, the weights of connected neurons are randomly assigned and then refined using a learning algorithm. Backpropagation with gradient descent is the most commonly used approach for adjusting the edge weights. ANN can vary in size and shape, but a simple ANN typically consists of a feedforward network with no loops [91].

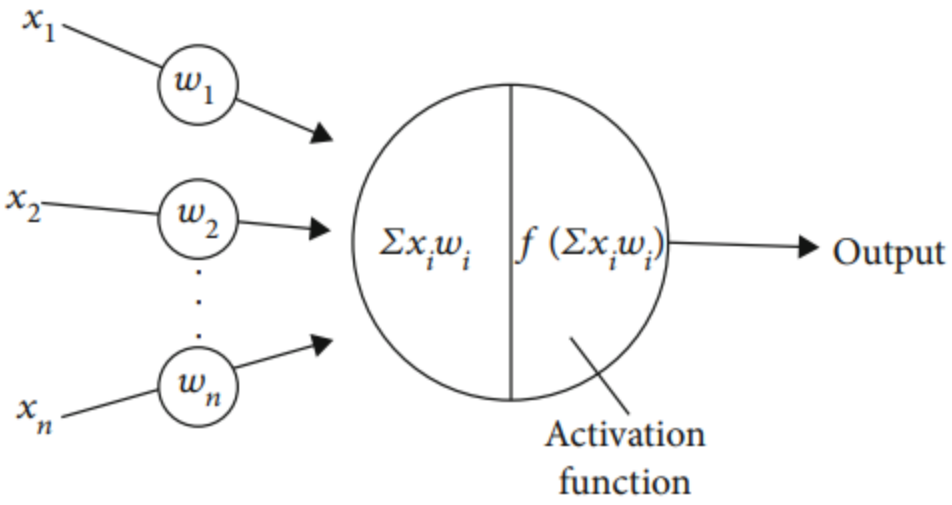

Figure 3-2: The leading architecture of the MLP method.

3.1.4 Long Short-Term Memory (LSTM)

In 1997, a new model called Long short-term memory (LSTM) was proposed, which is a type of gated recurrent neural network. Bidirectional LSTM is an extension of the LSTM model. The key feature of these networks is their ability to retain data for future cell processing.

LSTM can be thought of as an RNN with two essential vectors and a memory pool [92]:

- The first vector represents the output at the current step, which is in a short-term state.
- The second vector represents the long-term state, which is capable of storing, retrieving, and discarding information for long-term use as it passes through the network.

Figure 3 illustrates that a perceptron determines the decision to read, store, or write. The activation functions produce a value between 0 and 1. The forget and output gates determine if new information should be retained or discarded. The selection of the model is made using the LSTM block's memory and the output gate's state. The output is then fed back into the network as input, creating a recurring sequence. The LSTM model can address the difficulties that traditional machine learning methods face in extracting the meaning at a higher level while categorizing texts [93]. The model utilizes a content matrix consisting of pretrained distributed word vectors as input and then utilizes its unique memory structure to extract feature expressions that create context

information (as seen in Figure 3-3). The LSTM approach is depicted in Figure 3-3(a), which utilizes only historical context, resulting in a limited understanding of complex words due to the lack of future context. The BiLSTM combines a forward LSTM layer and a backward LSTM layer to address this issue. The correlation technique can be used by summing the information from both directions before and after the word. Figure 3-3(b) shows the architecture of the model [93].

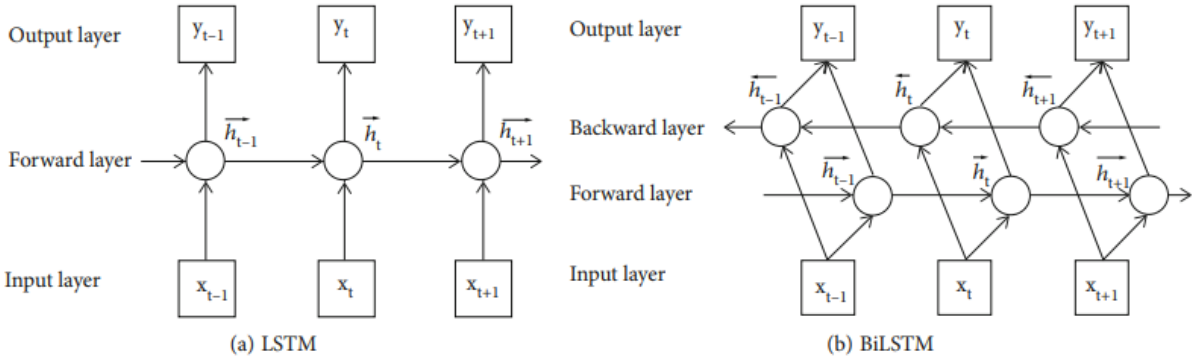

Figure 3-3: The architecture of the LSTM and BiLSTM methods.

3.2 Results and Discussion

3.2.1 Data Collection

The NSL-KDD database was proposed to address some of the significant inconsistencies in the KDD dataset [94]. It includes a comprehensive dataset that simulates a variety of intrusions in a military network environment. However, some of the problems highlighted by McHugh in the KDD dataset still persist in the current version. While the natural network structure may not be entirely represented, it can still be used as a resource because of the lack of public datasets for network-based systems. Researchers may utilize this dataset to compare various intrusion detection technologies by incorporating user data. Moreover, the NSL-KDD training and testing sets contain a substantial number of records, which offers the advantage of conducting tests on the entire dataset instead of randomly selecting a small portion. This approach can save costs and ensure that the evaluation results of different research projects are consistent and comparable [94].

The NSL-KDD dataset provides advantages compared to the original KDD dataset as it has less information in the learning suite, which avoids classifier bias towards certain records. In addition, testing sets do not have duplicate history, which prevents any influence on training performance due to higher detection capability of repeating data [95].

The primary KDD dataset has an inverse relationship between the number of records picked from each category and its proportion, leading to varying recognition accuracy for different machine learning methods. This makes it more efficient to accurately assess different learning strategies over a wider range. The training and test sets contain a large number of records, making it economical to conduct tests on the entire dataset rather than selecting a small portion randomly. This ensures that the results of different research paper assessments are consistent and similar. One significant disadvantage of KDD datasets is the excessive number of redundant records, which can negatively affect pattern recognition, particularly for networks vulnerable to attacks such as U2R and R2L. Additionally, these duplicate records in the test set can distort assessment results since approaches with better detection rates for repeated records can influence the outcome [94].

3.2.2 Results of Feature Extraction

DDoS detection techniques commonly use passive network monitoring to collect network traffic. The obtained data is then analyzed to identify any attack traffic. There are two primary methods of scanning a passive network, which include packet capture that intercepts and records network data packets, and network flow monitoring that provides aggregated traffic data for a flow between two endpoints. The effectiveness of DDoS detection systems is evaluated using two sets of features, including packet-level and flow-level characteristics. Table 3-1 summarizes these characteristics.

In this study, a flow is defined as a one-way series of packages with the same 5-tuple values, which consist of the source IP address, source port number, destination IP address, port number, and protocol ID. The research investigates the detection performance of machine learning-based algorithms on these specified characteristics.

Table 3-1: The correlation coefficient for IoT intrusion detection.

Correlation value	Qualitative value
(-0.1, 0.1)	Very weak
(-0.3, -0.1) or (0.1, 0.3)	Weak
(-0.5, -0.3) or (0.3, 0.5)	Moderate
(-1, -0.5) or (0.5, 1)	Strong

3.2.3 Classification Results

Numerous techniques for detecting Distributed Denial of Service (DDoS) attacks have been introduced, with many of them relying on a straightforward Artificial Neural Network (ANN) implemented using the backpropagation algorithm. The main difference between these techniques lies in the design of the ANN in terms of the number of neurons in each layer and the number of hidden layers. Most ANNs that have been evaluated have a single hidden layer, where the input layer neurons reflect the extracted features from network traffic, while the output layer neurons display the required labels. Typically, the number of neurons in the hidden layer ranges from 3 to 50. ANNs have broad applicability in various detection tasks.

In this project, an Artificial Neural Network (ANN) is utilized to determine the quantity of compromised devices involved in a DDoS attack. The system creates a regular profile beforehand and continuously monitors network traffic to detect any attack. A DDoS attack is documented when the entropy of flow size differs from a standard preset threshold. The difference value is entered into the ANN model to compute the number of compromised devices. To detect DDoS attacks, an ensemble detection approach is developed that integrates multiple ANN classifiers. In the proposed method the training dataset is initially divided into two categories, namely attack and regular traffic.

The dataset for each category was split into n subgroups, with the data being separated into k distinct groups within each subset. By leaving out one of the disjoint sets, k training sets were

generated using these non-overlapping sets. This resulted in k and n ANN classifiers being formed for each category. Then, a new instance is evaluated by all classifiers. A weighted majority voting approach is used to make decisions on the n subsets within each class, while a weighted product rule is used to make decisions across different categories.

In this project, eight machine learning algorithms are utilized for diagnosing DDoS attacks in IoT. The NSL-KDD dataset is used, with labels of 1 and 0 representing normal and anomalous behaviors, respectively. The first diagnostic approach employed is the MLP network. The ANN network is constructed with two hidden layers, consisting of 19 and 10 neurons each. 70% of the dataset is used for training, while the remaining 30% is reserved for validation and testing. The iteration process continues until the numerical label's Mean Squared Error (MSE) is fixed. The results of the MLP network are depicted in Figure 3-4.

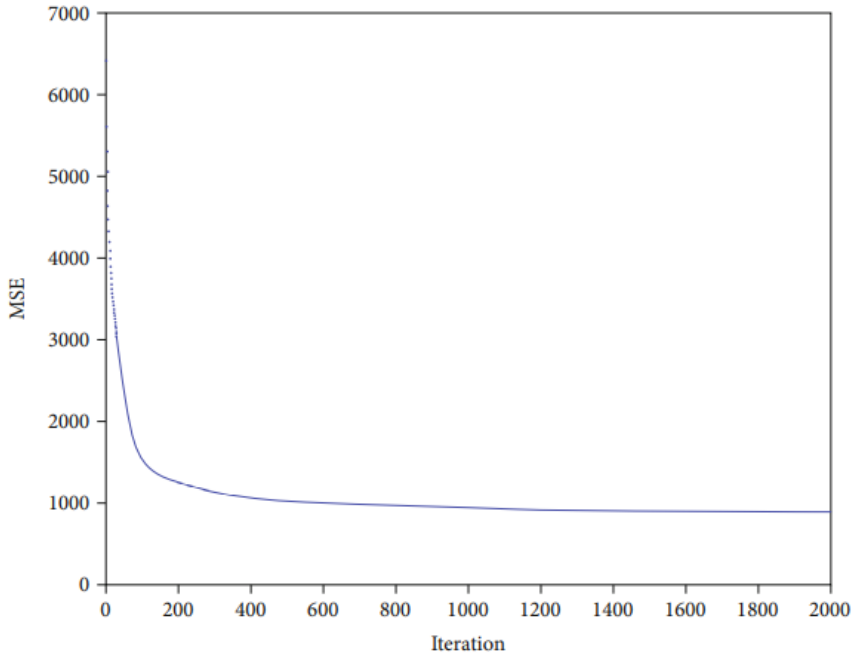

Figure 3-4: The MLP method training process.

The outcomes of the categorization process are displayed through a confusion matrix, which is illustrated in Figure 3-5.

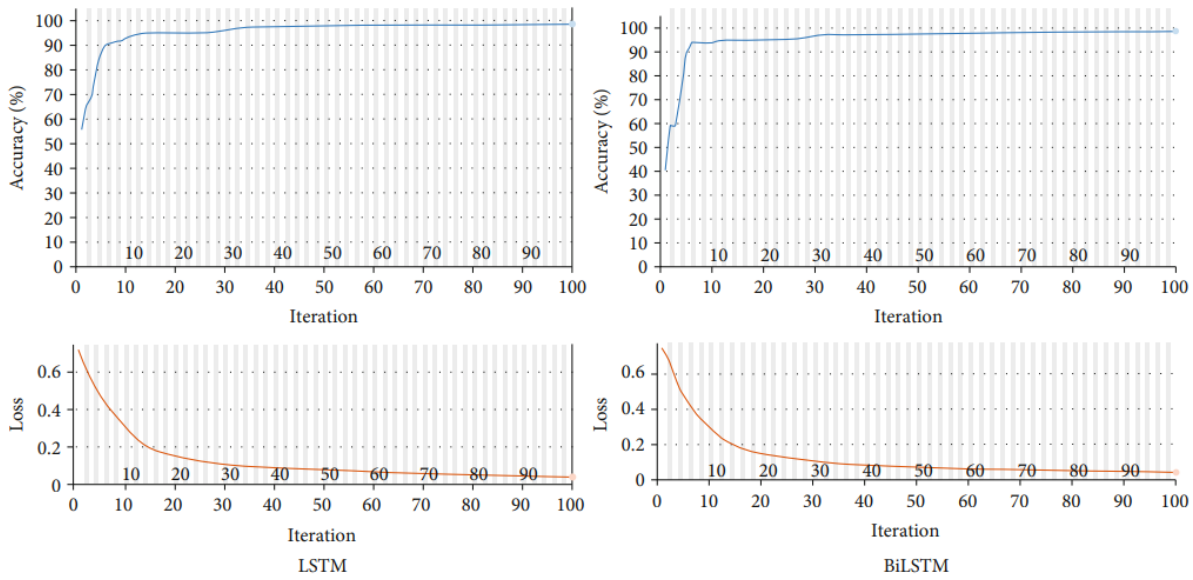

Figure 3-5: The training process of the LSTM and BiLSTM networks.

The results of the training process are illustrated in Figure 3-6, which displays the confusion matrix. The confusion matrix reveals that the model successfully detects 99.9% of the attacks, as it correctly identified 12098 out of 12109 anomaly nodes. However, the model misclassified 11 nodes. Thus, the sensitivity of the training process is 99.9%. On the other hand, specificity is a measure that indicates the frequency of false positives. The analysis of the results reveals that 97.6% of the normal nodes are accurately classified, while 2.4% are misclassified.

The accuracy metrics of the model are determined by the true-positive rate, which represents the percentage of all diagnostic positives. The results show that 98.4% of the 12297 nodes used in DDoS attacks were correctly classified as positive nodes. In conclusion, the training procedure achieved 99% accuracy, indicating that it is highly effective in identifying DDoS attacks.

The results obtained from testing the dataset validate the effectiveness of the employed networks. The accuracy of the testing samples for 30% of the data is 79.5%. Additionally, the sensitivity, specificity, and accuracy scores are 97.9%, 67.3%, and 66.5%, respectively. By measuring the difference between the two accuracies using overfitting metrics (OF), the OF is found to be 19.5%, indicating good categorization findings.

The LSTM and BiLSTM algorithms demonstrated high accuracy values of 99.9% and 100%, respectively, in the training procedure. The OF values for LSTM and BiLSTM are 20.1% and 17.7%, respectively. The study employed eight machine learning algorithms, including MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF, to confirm the classification findings. The LSTM and BiLSTM methods outperformed other approaches in terms of test accuracy.

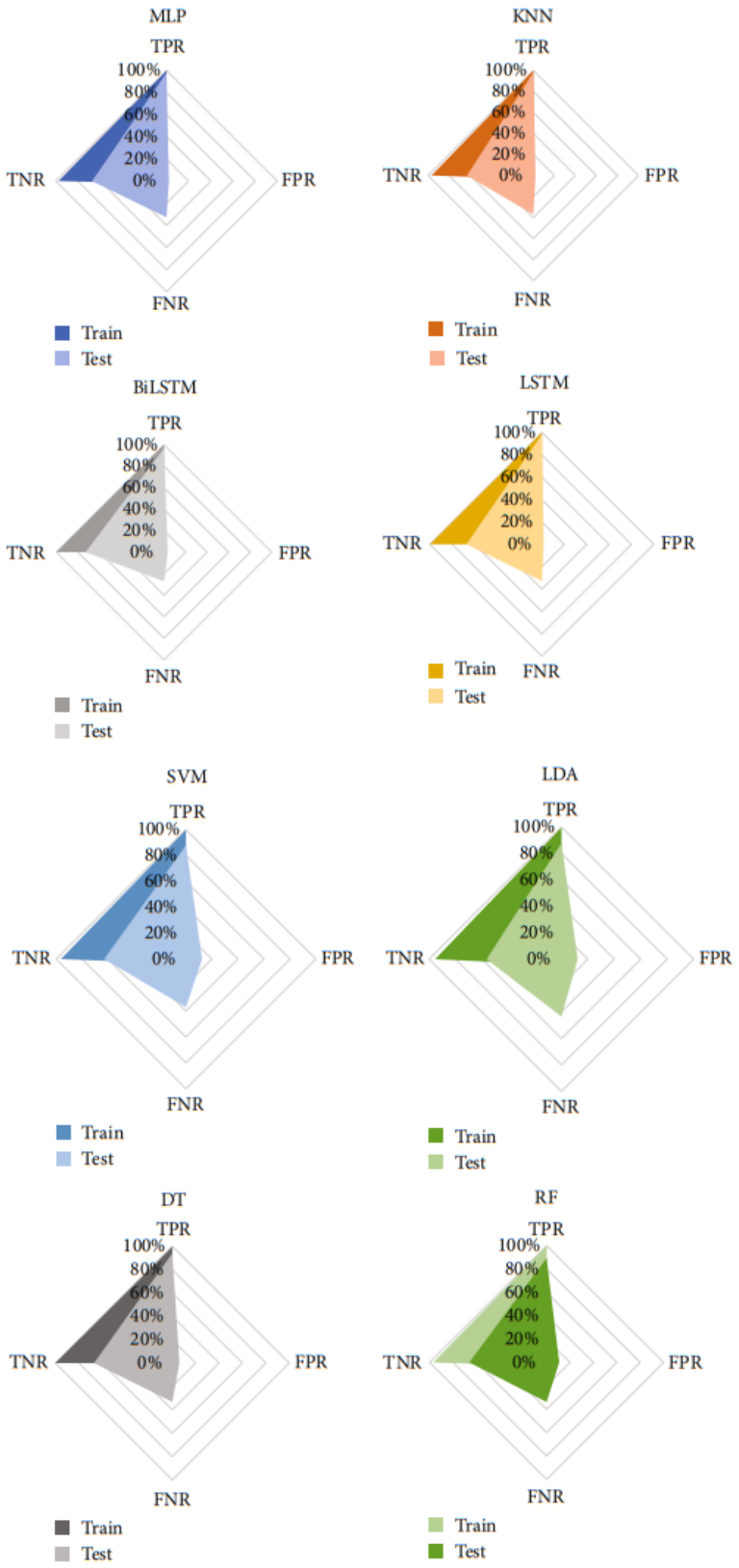

Figure 3-6: The confusion plots of the used ML methods.

In order to compare the effectiveness of various machine learning approaches for detecting DDoS attacks, the ROC (receiver operating characteristic) curve is presented in Figure 3-7. The ROC curve shows the false positive rate on the horizontal axis and the true positive rate on the vertical axis. The ideal classifier would have the highest true positive rate and the lowest false positive rate. Based on the results, the BiLSTM approach seems to be the best classifier for the given features.

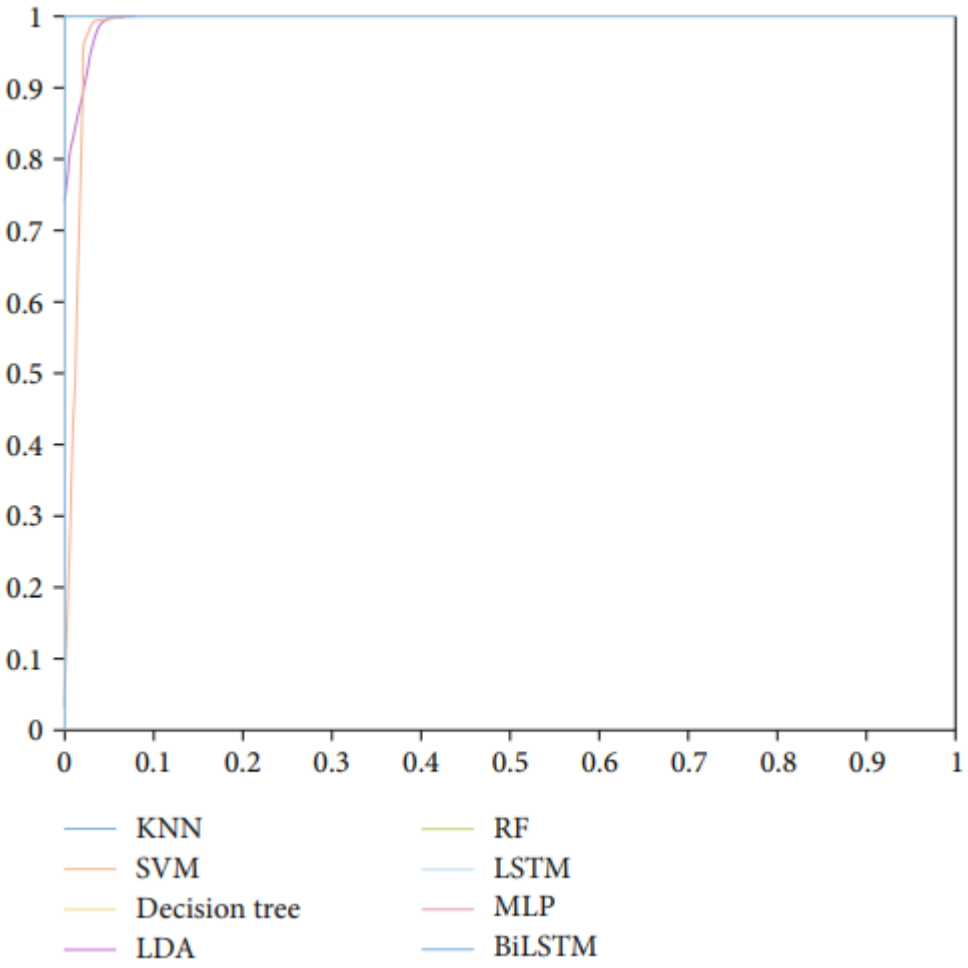

Figure 3-7: The ROC curve of the proposed methods.

The accuracy rates of various machine learning classifiers are depicted in Figure 3-8. According to the data, the accuracy values for MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF are 79.5 percent, 80 percent, 82.3 percent, 77 percent, 82.8 percent, 69 percent, 77.7 percent, and 75.4 percent, respectively. Among these classifiers, the BiLSTM architecture with the highest accuracy is considered the most accurate and appropriate approach for diagnosing DDoS attacks in IoT, using the given strategy.

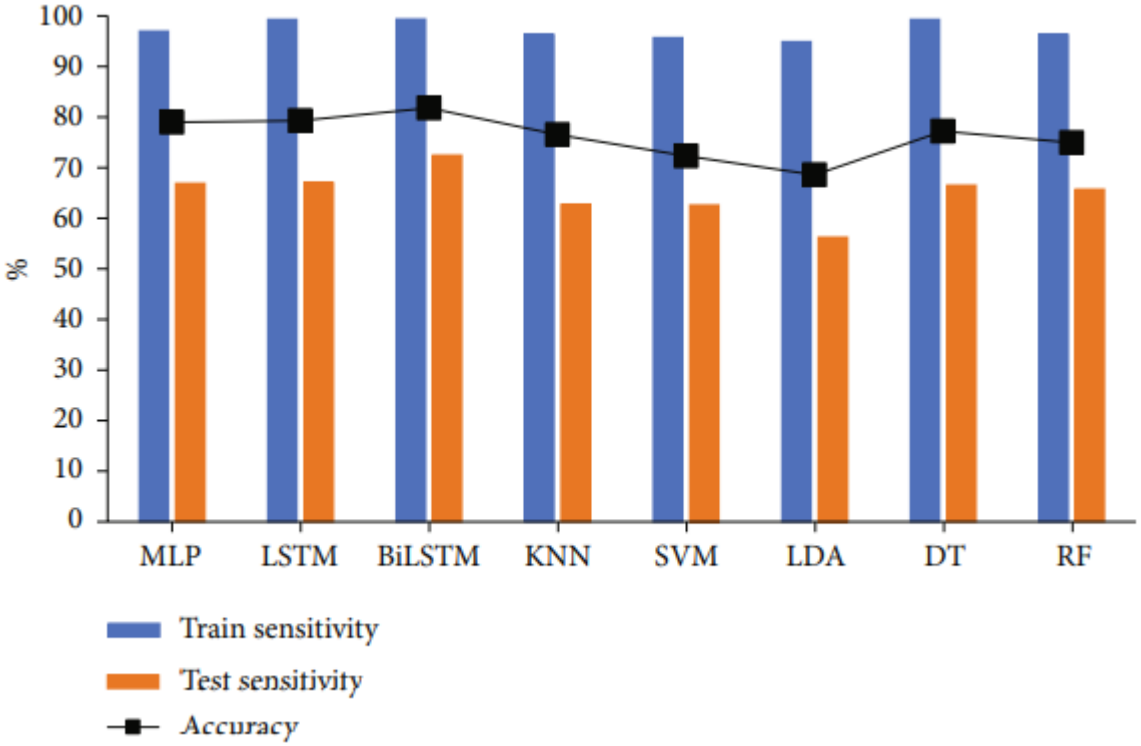

Figure 3-8: The accuracy, train sensitivity, and test sensitivity of the proposed approach.

3.4 Conclusion

In this project, a variety of machine learning algorithms including MLP, LSTM, BiLSTM, KNN, SVM, LDA, DT, and RF were employed to diagnose DDoS attacks in IoT using a dataset called NSL-KDD. The dataset had labels indicating normal and anomalous behaviors. The accuracy of each algorithm was evaluated using a confusion matrix. The MLP algorithm had the highest effectiveness in recognizing attacks, with a 99.9% success rate according to its training confusion matrix. Specificity, which measures the frequency of bad outcomes, was used to evaluate misdiagnoses. The accuracy of the LSTM and BiLSTM algorithms during the training phase was found to be 99.9% and 100%, respectively. The BiLSTM approach was found to be the best classifier for the dataset, with a test accuracy of 82.3%, followed by LSTM, SVM, and RF. KNN, LDA, and DT had lower test accuracy values. The ROC was used to compare the performance of the different algorithms in diagnosing DDoS attacks.

Chapter Four

Project Two

A Framework for Detecting Anomalies of Fingerprint in Parallel and Distributed Network Attack Systems Based on The Internet of Things: Applications Based on Convolutional Deep Learning Algorithms

The operation of an internet of things (IoT) network can potentially divulge significant information about network activity and traffic. While anomalies in the network may not always pose an immediate threat, they can provide valuable insight into potential network issues. Therefore, a fingerprinting approach can be employed to detect errors on IoT-connected devices.

By analyzing traffic patterns, it is possible to uncover the effects of device errors or faults beyond just attacks, which are typically disguised from standard security solutions. Consequently, it is imperative to identify the specific type of equipment in order to select the appropriate security measures. Failing to make accurate predictions can slow down device performance and compromise network security. Thus, we developed a second project called "A Framework for Detecting Anomalies of Fingerprint in Parallel and Distributed Network Attack Systems Based on The Internet of Things: Applications Based on Convolutional Deep Learning Algorithms." The primary goal of this project is to detect anomalous behavior in IoT devices by identifying them on a network. To achieve this, we propose a feature-based approach that uses machine learning to create a fingerprint method and identify unusual behavior patterns in devices.

Our approach outperforms existing methodologies, resulting in a 14% increase in the average forecast F1-score. By comparing packet header features with long-term device behavior, we aim to extend this technique to detect unusual device activity.

4.1 Methods and Materials

4.1.1 Machine learning

Often referred to as a model, a machine learning algorithm describes data in the context of a problem. The goal is to convert data into insight. A retailer may use a machine-learning algorithm to estimate sales for the next quarter based on previous sales and other relevant information. In a similar way, a manufacturer of wind turbines may visually inspect crucial machinery and pass the video data via algorithms designed to detect hazardous flaws.

Supervised machine learning techniques can be used to predict or justify the value of a category. For example, they can determine if a customer is likely to make an online purchase, with the potential outcomes being either a buyer or non-buyer. Additionally, there are more than two categories that can be classified, and a classification algorithm can be used to identify normal or anomalous data. The approach chosen depends on the problem at hand, and there are two types of learning: supervised and unsupervised. Figure 4-1 below provides a breakdown of machine learning techniques, which will be discussed in more detail individually.

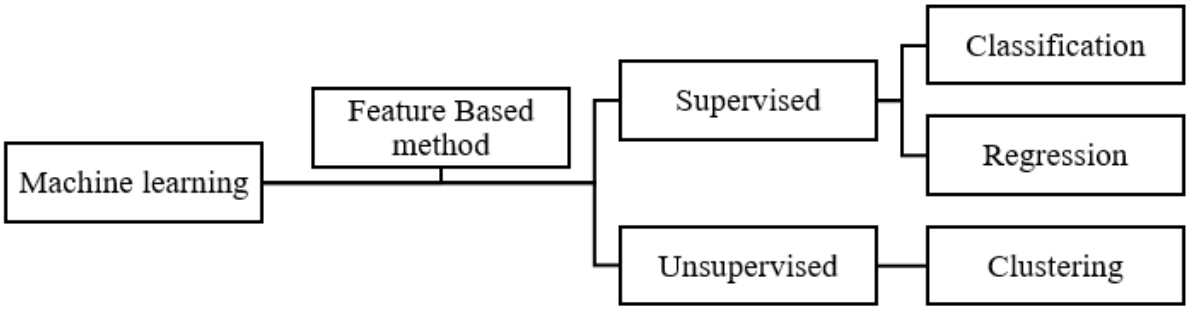

Figure 4-1: Flow chart of machine learning methods.

4.1.2 Convolutional Neural network

Convolutional neural networks consist of neurons that have adjustable weights and biases. Each neuron processes a set of inputs, calculates a dot product, and may also include a non-linear operation. The entire network can be represented as a single differentiable scoring function, which takes the raw image pixels as input and produces class scores as output [105]. Moreover, they still employ a loss function (such as SVM/Softmax) on the last fully connected layer, and all the learning strategies developed for traditional neural networks are still applicable [106].

A ConvNet is made up of multiple layers, each with its own unique function for transforming one set of activations into another [107]. The three primary types of layers used to build ConvNet topologies are the Convolutional Layer, Pooling Layer, and Fully-Connected Layer, which are the same types of layers used in traditional neural networks. These layers can be combined in different ways to create a complete ConvNet architecture.

4.1.3 Proposed Method

The proposed approach for fingerprinting involves extracting device characteristics from their fingerprints. Statistics such as packet arrival time, Ethernet packet size, IP header size, packet number, packet direction, and source/destination IP addresses (minimum, maximum, mean, variance, etc.) are among the attributes that can be provided. A multi-class machine learning classifier can be trained using the generated fingerprint to identify different Internet of Things devices. Furthermore, it is possible to extract characteristics from encrypted communication using existing information. Instead of extracting the characteristics of each individual packet during the initial device setup, feature extraction is performed on a series of packets. In the absence of data with the necessary features, systematic analysis is required to identify abnormalities. Therefore, machine learning techniques are utilized to analyze the data, discover correlations, or predict unknown events.

This approach utilizes a classification method based on machine learning. The goal is to identify traffic anomalies in an IoT system using a suggested fingerprint. The first step is to create a labeled data set, which serves as the suggested fingerprint for classifying and identifying the features of

networked devices. Once the labeled data set and device fingerprint have been generated, machine learning techniques are used to classify the packets, with a deep convolutional neural network being recommended for this purpose. In the third phase, the approach's performance is evaluated based on several criteria, including accuracy, sensitivity, precision, specificity, F1-score, and risk detection error. Figure 4-2 depicts the conceptual diagram of this approach.

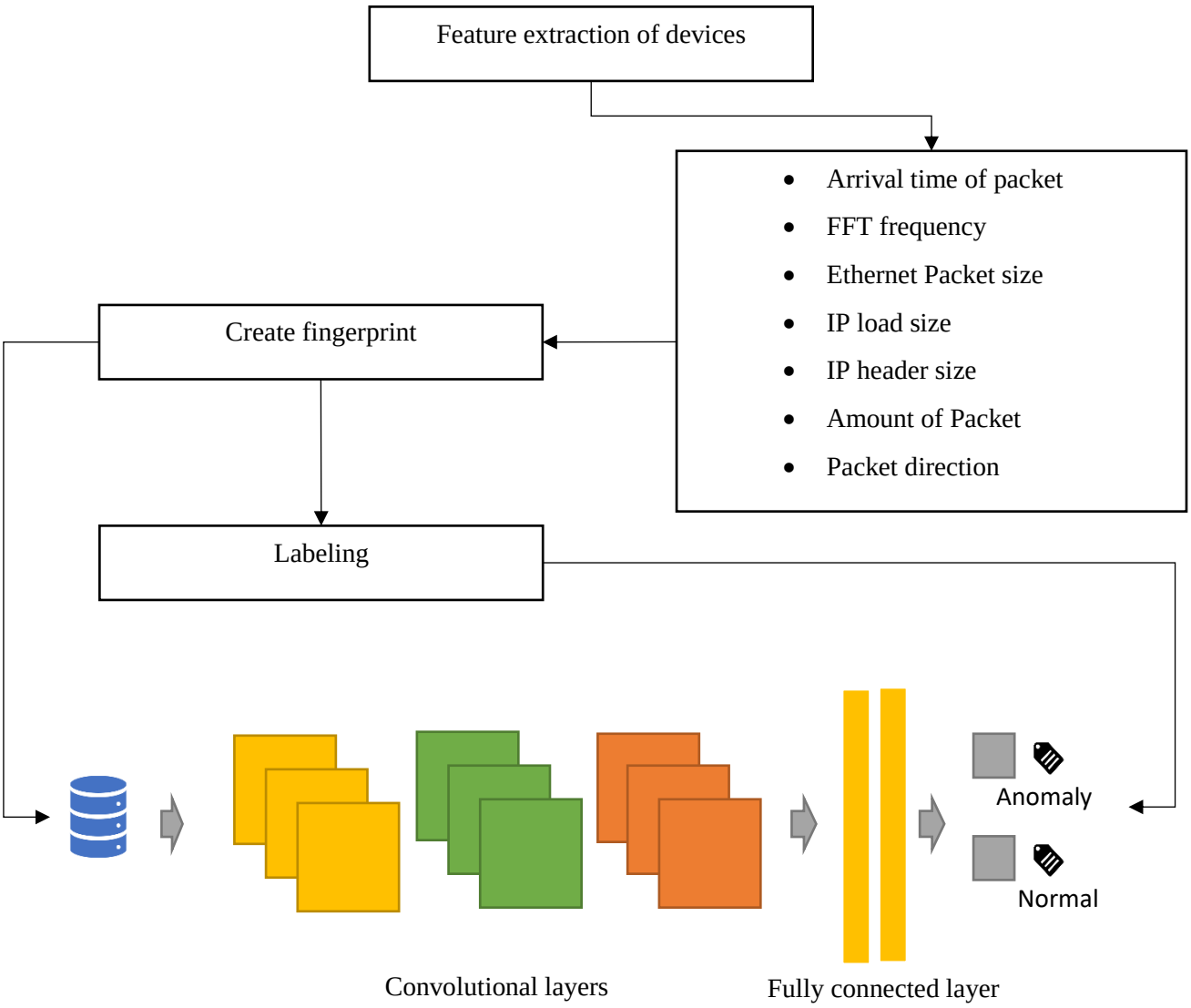

Figure 4-2: Conceptual diagram of the proposed model.

4.1.4 Performance Metrics

Precision, also called positive predictive value, is a metric that indicates the proportion of relevant results among the retrieved examples. It measures the probability that a retrieved instance is truly positive rather than false positive. It is an important measure for evaluating the accuracy of predictions and identifying the percentage of false positives for each device type. In other words, precision can help to assess the quality of the classification model and its ability to correctly identify the targeted devices [108]. The higher the precision, the fewer false positives and the more accurate the model is in predicting the device types. Therefore, precision is a crucial metric for machine learning models that aim to identify and classify networked devices in an IoT system. Here is a mathematical representation of precision.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{1}$$

In addition to recall rate, sensitivity rate and True Positive rate are also known as true positive rate. The tool displays the proportion of relevant examples found in the search as compared to all relevant instances in a test, as well as the probability of finding a relevant instance at random. We utilize Recall to assess the accuracy of each forecast for each device type. Here is a mathematical representation of recall [109].

$$\text{Recall} = \frac{TP}{TP + FN} \tag{2}$$

The F1-score is a measure that assigns the same importance to precision and recall. In addition to the F1-score, there are two other commonly used F-measures: the F2-score and the F0.5-score, which place more emphasis on recall and precision, respectively. The F1-score is used to evaluate the accuracy of predictions for each type of device. When the F1-score is at its highest value, it represents the harmonic mean of precision and recall. The F1-score can be mathematically represented as follows [18-19].

$$\mathrm{F}_1 = \frac{2 \times Percision \times Recall}{Percision + Recall} \tag{3}$$

4.2 Results and Discussion

4.2.1 Feature Selection

To create a unique identifier for each device, packet-based fingerprinting is used, which extracts 23 characteristics from every packet to create a feature vector. The first 12 feature vectors are utilized to generate a 176-dimensional fingerprint for the device. The fingerprint is constructed by creating two sequences of 21 packets each, which are filtered using the device's MAC address. Finally, Scapy1 is utilized to extract the necessary features for the fingerprint creation process.

4.2.2 Implementation Tools and Dataset

The Sentinel[100] dataset can be used by IoT devices for anomaly detection and fingerprinting. The dataset contains a total of 27 smart home devices that are connected via Ethernet or WiFi. MATLAB software is utilized to conduct feature extraction, fingerprinting, and deep learning network training.

The data is derived from the devices' traffic patterns during their setup, including powering on, establishing a direct wireless or Ethernet connection, and transmitting WiFi credentials. The average capture time was 68 seconds, and the average packet length was 350 bytes. A device can now be easily configured by following a series of instructions in a PC program or using a smartphone app. Whenever the device is captured, it is hard reset to return it to its original factory settings.

4.2.3 Classification results

The scikit-learn package is used to compare the average F1-scores of popular classification techniques, which is a useful way to assess the impact of the chosen algorithm. In Table 4-1, the minimum, maximum, and average F1-scores for each classification technique are presented (refer to Figure 4-3). To provide more extensive insights, a 10-fold cross-validation was employed across 10 rounds during the classification process. The Random Forest (RF) classifiers achieved the highest average prediction F1-scores with the least amount of variance. Even though decision tree

classifiers were outperformed in terms of prediction F1-score, RF classifiers categorized devices more rapidly. We utilized RF as the classification method to train our model and predict device types.

Figure 4-3: The results of classification (F1 score Metrics).

The Gini impurity measures the probability of incorrect classification of a randomly selected fingerprint, based on class distribution. In the RF algorithm, the significance of each feature in classification is determined by averaging it across all trees. The average significance values for each feature used in RF classification can be found in Figure 4-4. The top 10 characteristics of packet-based and sequence-based techniques are summarized in the table, with sequence-based fingerprinting relying on sequences generated from a known source. The majority of the top 10 attributes are related to packet size, with 80% pertaining to source-originating sequences and the remaining 20% for bidirectional sequences. Other than packet size, features such as source or destination port class and packet direction can affect prediction accuracy by approximately 0.18.

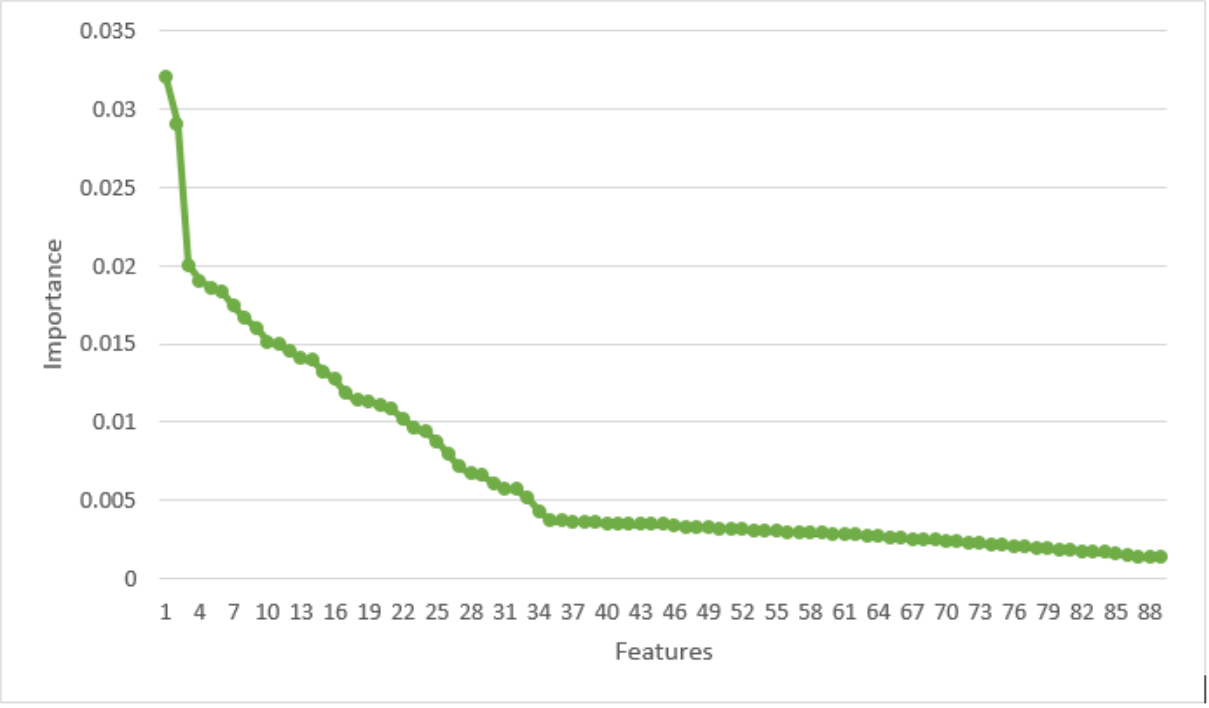

Figure 4-4: Importance of the feature based on RF.

Table 4-1: Selected features for classification based on RF method.

Feature name	Sequence
Size of Packet	IP payload size
IP counter of Destination	Ethernet frame size
HTTP feature	Ethernet frame size
Destination port	Ethernet frame size
UDP feature	Ethernet frame size
IP feature	IP payload size
Source port	IP payload size

The average prediction F1-score is impacted by the features used for classifier training. To investigate this, the number of features used to train the classifier was varied and the resulting average F1-score was measured. Figure 4-5 displays a plot of F1-scores against the number of features used by the classification algorithm to build the model. The F1-score values in the model have somewhat increased with the inclusion of additional features, particularly at feature numbers 2, 4, 7, and 25. A significant improvement in F1-score has been attributed to the inclusion of highly important characteristics. Beyond the first 40 attributes, the significance value drops below 0.1, which has a lesser impact on the ability to differentiate between different device types. Consequently, after the first 40 features, the F1-score surpasses 0.90, and as more features are added up to 90, the accuracy progressively increases from 0.90 to 0.92 without any sudden jumps.

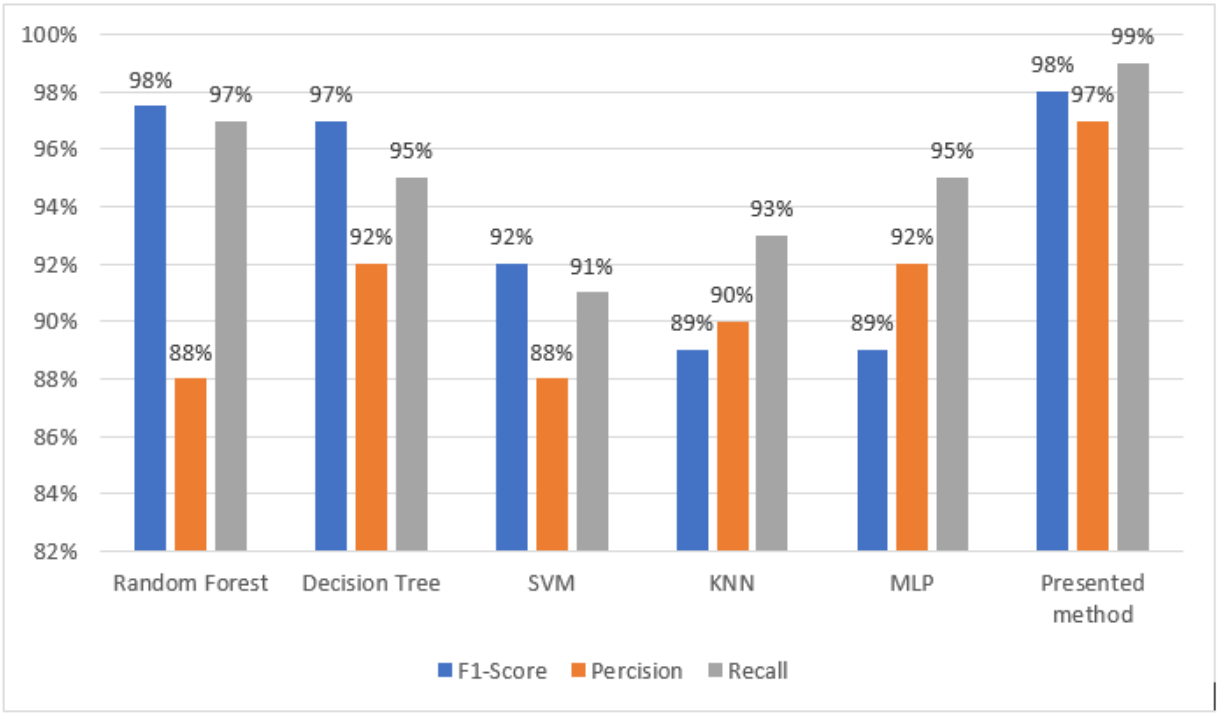

Figure 4-5: The performance of the presented CNN method through classification experiments.

4.3 Conclusion

Neural network-based techniques are commonly employed in IoT to classify or detect anomalies using various artificial intelligence algorithms. To develop a novel approach for device fingerprinting, in this project, we extract features from a sequence of packets, including packet sizes, interarrival times, Fast Fourier Transform of interarrival times, packet directions, and so on. Our method has improved the average prediction F1-score by 14% when compared to state-of-the-art techniques. Consequently, the average prediction F1-score for the 10 devices with the lowest F1-score increased from 0.45 to 0.78. We also examined the impact of the confidence threshold on the classifier's ability to detect unknown devices and suggested possible threshold ranges that could be used in different scenarios.

Chapter Five

Conclusion

The Internet of Things (IoT) has become a vital component of modern society, with the ability to connect and control various devices remotely. However, the security of these devices is of utmost concern due to their complexity and heterogeneity, which makes them vulnerable to attacks and breaches. Standard security solutions, such as firewalls and intrusion detection systems (IDS), may not be sufficient to protect IoT devices, and more intelligent procedures that can handle various levels of data flow are necessary.

Fortunately, machine learning-based IDS has emerged as a promising solution for detecting attacks and anomalies in IoT networks. These IDS can analyze traffic patterns and data flow in real-time to identify potential threats. However, there are specific challenges that need to be addressed, such as the impact of different data processing techniques on IDS accuracy.

To improve IoT security, fingerprint-based approaches and feature-based anomaly detection methods have been proposed. These approaches aim to identify and categorize IoT devices based on their unique characteristics, allowing for more accurate and efficient detection of abnormal behavior.

Ultimately, a comprehensive and proactive approach to IoT security is essential for protecting IoT devices and the data they generate. This approach should consider both hardware and software components, as well as the network infrastructure. By adopting such an approach, IoT devices can operate safely and securely in today's interconnected world.

REFERENCES

[1] Y. Liu, T. Zhi, M. Shen, L. Wang, Y. Li, and M. Wan, “Software-defined DDoS detection with information entropy analysis and optimized deep learning,” Future Generation Computer Systems, vol. 129, pp. 99–114, 2022.

[2] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-based network intrusion detection against denial-of-service attacks,” Electronics, vol. 9, no. 6, pp. 916–921, 2020.

[3] F. O. Catak and A. F. Mustacoglu, “Distributed denial of service attack detection using autoencoder and deep neural networks,” Journal of Intelligent Fuzzy Systems, vol. 37, no. 3, pp. 3969–3979, 2019.

[4] J. Wang, Y. Liu, H. Feng, and National Engineering Laboratory on Interconnection Technology for Next Generation Internet, Beijing Jiaotong University, Beijing, China, “IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks,” Mathematical Biosciences and Engineering, vol. 19, no. 2, pp. 1280–1303, 2021.

[5] M. Abbasi, A. Shahraki, and A. Taherkordi, “Deep learning for network traffic monitoring and analysis (NTMA): a survey,” Computer Communications, vol. 170, pp. 19–41, 2021.

[6] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, “Mobile encrypted traffic classification using deep learning: experimental evaluation, lessons learned, and challenges,” IEEE Transactions on Network and Service Management, vol. 16, no. 2, pp. 445–458, 2019.

[7] K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, “Toward secure software-defined networks against distributed denial of service attack,” The Journal of Supercomputing, vol. 75, no. 8, pp. 4829–4874, 2019.

[8] S. Kottler, “February 28th DDoS incident report,” GitHub, pp. 1–3, 2018, http://githubengineering.com/ddos-incidentreport/.

[9] S. Haider, A. Akhunzada, I. Mustafa et al., “A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks,” IEEE Access, vol. 8, pp. 53972– 53983, 2020.

[10] P. Manso, J. Moura, and C. Serrão, “SDN-based intrusion detection system for early detection and mitigation of DDoS attacks,” Information, vol. 10, no. 3, p. 106, 2019.

[11] I. Karim, Q. T. Vien, T. A. Le, and G. Mapp, “A comparative experimental design and performance analysis of Snort-based intrusion detection system in practical computer networks,” Computers, vol. 6, no. 1, p. 6, 2017.

[12] R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu, “A DRDoS detection and defense method based on deep forest in the big data environment,” Symmetry (Basel), vol. 11, no. 1, p. 78, 2019.

[13] D. Ramotsoela, A. Abu-Mahfouz, and G. Hancke, “A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study,” Sensors (Switzerland), vol. 18, no. 8, p. 2491, 2018.

[14] Z. Lv, Y. Li, H. Feng, and H. Lv, “Deep learning for security in digital twins of cooperative intelligent transportation systems,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2021.

[15] J. Chen, Q. Wang, J. Huang, and X. Chen, “Motorcycle ban and traffic safety: evidence from a quasi-experiment at Zhejiang, China,” Journal of advanced transportation, vol. 2021, Article ID 7552180, 13 pages, 2021.

[16] Z. Lv, J. Guo, and H. Lv, “Safety Poka yoke in zero-defect manufacturing based on digital twins,” IEEE transactions on industrial informatics, p. 1, 2022.

[17] X. Liu, J. Zhao, J. Li, B. Cao, and Z. Lv,“Federated neural architecture search for medical data security,” IEEE transactions on industrial informatics, vol. 18, no. 8, pp. 5628–5636, 2022.

[18] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, “A secure and anonymous communicate scheme over the Internet of Things,” ACM Transactions on Sensor Networks, vol. 18, no. 3, pp. 1–21, 2022.

[19] A. Mehbodniya, J. L. Webber, M. Shabaz, H. Mohafez, and K. Yadav, “Machine learning technique to detect Sybil attack on IoT based sensor network,” IETE Journal of Research, pp. 1–9, 2021.

[20] B. Cao, J. Zhang, X. Liu et al., “Edge-cloud resource scheduling in space-air-ground integrated networks for Internet of Vehicles,” IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5765– 5772, 2021.

[21] G. Sun, Y. Cong, J. Dong, Y. Liu, Z. Ding, and H. Yu, “What and how: generalized lifelong spectral clustering via dual memory,” IEEE transactions on pattern analysis and machine intelligence, vol. 44, no. 7, pp. 3895–3908, 2021.

[22] M. Ahmadi, A. Taghavirashidizadeh, D. Javaheri, A. Masoumian, S. J. Ghoushchi, and Y. Pourasad, “DQRESCnet: a novel hybrid approach for selecting users in federated learning with deep-Q-reinforcement learning based on spectral clustering,” Journal of King Saud University-Computer and Information Sciences, 2021.

[23] G. Sun, Y. Cong, Q. Wang, B. Zhong, and Y. Fu, “Representative task self-selection for flexible clustered lifelong learning,” IEEE transaction on neural networks and learning systems, vol. 33, no. 4, pp. 1467–1481, 2020.

[24] F. Liu, G. Zhang, and J. Lu,“Multi-source heterogeneous unsupervised domain adaptation via fuzzy-relation neural networks,” IEEE Transactions on Fuzzy Systems, vol. 29, no. 11, pp. 3308–3322, 2020.

[25] A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, “Modified Lamport Merkle Digital Signature blockchain framework for authentication of Internet of Things healthcare data,” Expert Systems, p. e12978, 2022.

[26] L. Zhang, T. Gao, G. Cai, and K. L. Hai, “Research on electric vehicle charging safety warning model based on back propagation neural network optimized by improved gray wolf algorithm,” Journal of Energy Storage, vol. 49, p. 104092, 2022.

[27] J. Dong, Y. Cong, G. Sun, Z. Fang, and Z. Ding, “Where and how to transfer: knowledge aggregation-induced transferability perception for unsupervised domain adaptation,” IEEE Transactions on Pattern Analysis and Machine Intelligence, p. 1, 2021.

[28] W. Yang, X. Chen, Z. Xiong, Z. Xu, G. Liu, and X. Zhang, “A privacy-preserving aggregation scheme based on negative survey for vehicle fuel consumption data,” Information Sciences, vol. 570, pp. 526–544, 2021.

[29] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, “Improving high-impact bug report prediction with combination of interactive machine learning and active learning,” Information and Software Technology, vol. 133, p. 106530, 2021.

[30] A. Khaliq, A. Anjum, A. Ajmal, J. Webber, A. Mehbodniya, and S. Khan, “A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy,” IEEE Access, vol. 10, 2022.

[31] X. Wu, W. Zheng, X. Xia, and D. Lo, “Data quality matters: a case study on data label correctness for security bug report prediction,” IEEE Transactions on Software Engineering, vol. 48, no. 7, pp. 2541–2556, 2021.

[32] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, “A comparative study of class rebalancing methods for security bug report classification,” IEEE Transactions on Reliability, vol. 70, no. 4, pp. 1658–1670, 2021.

[33] W. Zheng, T. Shen, X. Chen, and P. Deng, “Interpretability application of the Just-in-Time software defect prediction model,” Journal of Systems and Software, vol. 188, article 111245, 2022.

[34] K. Liu, F. Ke, X. Huang et al., “DeepBAN: a temporal convolution-based communication framework for dynamic WBANs,” IEEE Transactions on Communications, vol. 69, no. 10, pp. 6675–6690, 2021.

[35] T. Gera, J. Singh, A. Mehbodniya, J. L. Webber, M. Shabaz, and D. Thakur, “Dominant feature selection and machine learning-based hybrid approach to analyze android ransomware,” Security and Communication Networks, vol. 2021, Article ID 7035233, 22 pages, 2021.

[36] Z. Liu, P. Qian, X. Wang, Y. Zhuang, L. Qiu, and X. Wang, “Combining graph neural networks with expert knowledge for smart contract vulnerability detection,” IEEE Transactions on Knowledge and Data Engineering, p. 1, 2021.

[37] X. Zhang, Y. Wang, M. Yang, and G. Geng, “Toward concurrent video multicast orchestration for caching-assisted mobile networks,” IEEE Transactions on Vehicular Technology, vol. 70, no. 12, pp. 13205–13220, 2021.

[38] C. Zong, H. Wang, and Z. Wan, “An improved 3D point cloud instance segmentation method for overhead catenary height detection,” Computers & electrical engineering, vol. 98, article 107685, 2022.

[39] A. Varmaghani, A. Matin Nazar, M. Ahmadi, A. Sharifi, S. Jafarzadeh Ghoushchi, and Y. Pourasad, “DMTC: optimize energy consumption in dynamic wireless sensor network based on fog computing and fuzzy multiple attribute decision-making,” Wireless Communications and Mobile Computing, vol. 2021, Article ID 9953416, 14 pages, 2021.

[40] C. Zong and Z. Wan, “Container ship cell guide accuracy check technology based on improved 3D point cloud instance segmentation,” Brodogradnja, vol. 73, no. 1, pp. 23–35, 2022.

[41] R. Singh, A. Mehbodniya, J. L. Webber et al., “Analysis of network slicing for management of 5G networks using machine learning techniques,” Wireless Communications and Mobile Computing, vol. 2022, Article ID 9169568, 10 pages, 2022.

[42] Y. Xie, Y. Sheng, M. Qiu, and F. Gui, “An adaptive decoding biased random key genetic algorithm for cloud workflow scheduling,” Engineering applications of artificial intelligence, vol. 112, article 104879, 2022.

[43] A. Li, C. Masouros, A. L. Swindlehurst, and W. Yu, “1-bit massive MIMO transmission: embracing interference with symbol-level precoding,” IEEE Communications Magazine, vol. 59, no. 5, pp. 121–127, 2021.

[44] Y. Feng, B. Zhang, Y. Liu et al., “A 200-225-GHz manifoldcoupled multiplexer utilizing metal wave guides,” IEEE Transactions on Microwave Theory and Techniques, vol. 69, no. 12, pp. 5327–5333, 2021.

[45] M. Ghanbari, “Adaptive machine learning and signal processing detection schemes for DDoS attacks,” 2022.

[46] Z. Niu, B. Zhang, B. Dai et al., “220 GHz multi circuit integrated front end based on solid-state circuits for high speed communication system,” Chinese Journal of Electronics, vol. 31, no. 3, pp. 569–580, 2022.

[47] W. Zheng, L. Yin, X. Chen, Z. Ma, S. Liu, and B. Yang,“Knowledge base graph embedding module design for visual question answering model,” Pattern Recognition, vol. 120, p. 108153, 2021.

[48] A. R. Ramtin, P. Nain, D. S. Menasche, D. Towsley, and E. D. S. E Silva, “Fundamental scaling laws of covert DDoS attacks,” Performance Evaluation, vol. 151, p. 102236, 2021.

[49] W. Zheng, X. Liu, X. Ni, L. Yin, and B. Yang, “Improving visual reasoning through semantic representation,” IEEE Access, vol. 9, pp. 91476–91486, 2021.

[50] W. Zheng, X. Liu, and L. Yin, “Sentence representation method based on multi-layer semantic network,” Applied Sciences, vol. 11, no. 3, p. 1316, 2021.

[51] J. Yu, L. Lu, Y. Chen, Y. Zhu, and L. Kong, “An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing,” IEEE Transactions on Mobile Computing, vol. 20, no. 2, pp. 337–351, 2021.

[52] H. Kong, L. Lu, J. Yu, Y. Chen, and F. Tang, “Continuous authentication through finger gesture interaction for smart homes using WiFi,” IEEE Transactions on Mobile Computing, vol. 20, no. 11, pp. 3148–3162, 2021.

[53] B. Hajipour Khire Masjidi, S. Bahmani, F. Sharifi, M. Peivandi, M. Khosravani, and A. Hussein Mohammed, “CT-ML: diagnosis of breast cancer based on ultrasound images and timedependent feature extraction methods using contourlet transformation and machine learning,” Computational Intelligence and Neuroscience, vol. 2022, Article ID 1493847, 15 pages, 2022.

[54] S. Zhao, F. Li, H. Li et al., “Smart and practical privacy preserving data aggregation for fog-based smart grids,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 521–536, 2021.

[55] Q. Meng, X. Lai, Z. Yan, C. Su, and M. Wu, “Motion planning and adaptive neural tracking control of an uncertain two-link rigid-flexible manipulator with vibration amplitude constraint,” IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 8, pp. 3814–3828, 2021.

[56] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “A hybrid machine learning approach for detecting unprecedented DDoS attacks,” The Journal of Supercomputing, vol. 78, no. 6, pp. 8106–8136, 2022.

[57] A. Prasad and S. Chandra, “VMFCVD: an optimized framework to combat volumetric DDoS attacks using machine learning,” Arabian Journal for Science and Engineering, vol. 47, pp. 1–19, 2022.

[58] X. Xu, J. Sun, C. Wang, and B. Zou, “A novel hybrid CNNLSTM compensation model against DoS attacks in power system state estimation,” Neural Processing Letters, vol. 54, no. 3, pp. 1597–1621, 2022.

[59] E. Tsogbaatar, M. H. Bhuyan, D. Fall et al., “A 1D-CNN based deep learning for detecting VSI-DDoS attacks in IoT applications,” in International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, vol. 12798 of Advances and Trends in Artificial Intelligence. Artificial Intelligence Practices, pp. 530–543, Springer, Cham, 2021.

[60] D. Tang, L. Tang, W. Shi, S. Zhan, and Q. Yang, “MF-CNN: a new approach for LDoS attack detection based on multifeature fusion and CNN,” Mobile Networks and Applications, vol. 26, no. 4, pp. 1705–1722, 2021.

[61] H. Alkahtani and T. H. H. Aldhyani, “Botnet attack detection by using CNN-LSTM model for Internet of Things applications,” Security and Communication Networks, vol. 2021, 23 pages, 2021.

[62] R. V. Mendonca, A. A. M. Teodoro, R. L. Rosa et al., “Intrusion detection system based on fast hierarchical deep convolutional neural network,” IEEE Access, vol. 9, pp. 61024–61034, 2021.

[63] M. Ghanbari and W. Kinsner, “Detecting DDoS attacks using an adaptive-wavelet convolutional neural network,” Canadian Conference on Electrical and Computer Engineering, 2021, pp. 1–7, ON, Canada, September 2021.

[64] X. Liu, Z. Tang, and B. Yang, “Predicting network attacks with CNN by constructing images from NetFlow data,” in 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and

IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 61–66, Washington, DC, USA, May 2019.

[65] J. Cheng, Y. Liu, X. Tang, V. S. Sheng, M. Li, and J. Li, "DDoS attack detection via multi-scale convolutional neural network," Computers, Materials & Continua, vol. 62, no. 3, pp. 1317–1333, 2020.

[66] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," Expert Systems with Applications, vol. 169, p. 114520, 2021.

[67] N. Mishra and S. Pandya, "Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review," IEEE Access, vol. 9, pp. 59353–59377, 2021.

[68] M. Ahmadi and M. Q. H. Abadi, "A review of using object orientation properties of C++ for designing expert system in strategic planning," Computer Science Review, vol. 37, p. 100282, 2020.

[69] G. Zhou, X. Bao, S. Ye, H. Wang, and H. Yan, "Selection of optimal building facade texture images from UAV-based multiple oblique image flows," IEEE Transactions on Geoscience and Remote Sensing, vol. 59, no. 2, pp. 1534–1552, 2021.

[70] M. Ahmadi, M. Soofiabadi, M. Nikpour, H. Naderi, L. Abdullah, and B. Arandian, "Developing a deep neural network with fuzzy wavelets and integrating an inline PSO to predict energy consumption patterns in urban buildings," Mathematics, vol. 10, no. 8, p. 1270, 2022.

[71] G. Zhou, X. Zhou, Y. Song et al., "Design of supercontinuum laser hyperspectral light detection and ranging (LiDAR) (SCLaHS LiDAR)," International journal of remote sensing, vol. 42, no. 10, pp. 3731–3755, 2021.

[72] M. Tondro, M. Jahanbakht, S. B. Rabbani, and M. Zaber, "Does immergence of ICT focused institutions increase the pace of urban development? A provincial case study in Iran using data from the ground and above," in I2022 IEEE Conference on Technologies for Sustainability (SusTech), pp. 219–223, Corona, CA, USA, April 2022.

[73] G. Zhou, R. Zhang, and S. Huang, "Generalized buffering algorithm," IEEE Access, vol. 9, pp. 27140–27157, 2021.

[74] X. Liang, L. Luo, S. Hu, and Y. Li, “Mapping the knowledge frontiers and evolution of decision making based on agent based modeling,” Knowledge-Based Systems, vol. 250, p. 108982, 2022.

[75] L. Zhao and L. Wang, “A new lightweight network based on MobileNetV3,” KSII Transactions on Internet and Information Systems (TIIS), vol. 16, no. 1, pp. 1–15, 2022.

[76] H. Zhu, M. Xue, Y. Wang, G. Yuan, and X. Li, “Fast visual tracking with Siamese oriented region proposal network,” IEEE Signal Processing Letters, vol. 29, p. 1437, 2022.

[77] J. Li, K. Xu, S. Chaudhuri, E. Yumer, H. Zhang, and L. Guibas, “GRASS: generative recursive autoencoders for shape structures,” ACM Transactions on Graphics (TOG), vol. 36, no. 4, pp. 1–14, 2017.

[78] P. P. F. Rajeena, R. Orban, K. S. Vadivel et al., “A novel method for the classification of butterfly species using pre-trained CNN models,” Electronics, vol. 11, no. 13, p. 2016, 2022.

[79] H. Ghayvat, S. Pandya, P. Bhattacharya et al., “CP-BDHCA: blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications,” IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1937–1948, 2021.

[80] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: an ensemble of autoencoders for online network intrusion detection,” 2018, http://arxiv.org/abs/1802.09089.

[81] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, “A hierarchical hybrid intrusion detection approach in IoT scenarios,” in 2020 IEEE Global Communications Conference, GLOBECOM 2020- Proceedings, pp. 1–7, Taipei, Taiwan, December 2020.

[82] M. Ghanbari and W. Kinsner, “Detecting DDoS attacks using polyscale analysis and deep learning,” International Journal of Cognitive Informatics and Natural Intelligence, vol. 14, no. 1, pp. 17–34, 2020.

[83] J. Zhang, C. Zhu, L. Zheng, and K. Xu, “ROSEFusion: random optimization for online dense reconstruction under fast Wireless Communications and Mobile Computing 15 camera motion,” ACM transactions on graphics, vol. 40, no. 4, pp. 1–17, 2021.

[84] F. Zhang, J. Zhai, X. Shen, O. Mutlu, and X. Du, “POCLib: a high-performance framework for enabling near orthogonal processing on compression,” IEEE transactions on Parallel and Distributed Systems, vol. 33, no. 2, pp. 459–475, 2022.

[85] R. F. Fouladi, O. Ermiş, and E. Anarim, “A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software defined network,” Computers & Security, vol. 112, p. 102524, 2022.

[86] Y. Cui, Q. Qian, C. Guo et al., “Towards DDoS detection mechanisms in software-defined networking,” Journal of Network and Computer Applications, vol. 190, p. 103156, 2021.

[87] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer Internet of Things devices,” in Proceedings -2018 IEEE Symposium on Security and Privacy Workshops, SPW, pp. 29–35, San Francisco, CA, USA, May 2018.

[88] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, “Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN,” Future Generation Computer Systems, vol. 111, pp. 763–779, 2020.

[89] Z. Liu, X. Yin, and Y. Hu, “CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning,” IEEE Access, vol. 8, pp. 42120–42130, 2020.

[90] J. Hou, P. Fu, Z. Cao, and A. Xu, “Machine learning based DDoS detection through NetFlow analysis,” in Proceedings IEEE Military Communications Conference MILCOM, pp. 565–570, Los Angeles, CA, USA, October 2018.

[91] Y. N. Soe, P. I. Santosa, and R. Hartanto, “DDoS attack detection based on simple ANN with SMOTE for IoT environment,” in Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC, pp. 1–5, Semarang, Indonesia, October 2019.

[92] Y. Li and Y. Lu, “LSTM-BA: DDoS detection approach combining LSTM and Bayes,” in Proceedings -2019 7th International Conference on Advanced Cloud and Big Data, CBD, pp. 180–185, Suzhou, China, September 2019.

[93] W. Huang, X. Peng, Z. Shi, and Y. Ma, “Adversarial attack against LSTM-based DDoS intrusion detection system,” in Proceedings-International Conference on Tools with Artificial Intelligence, ICTAI, pp. 686–693, Baltimore, MD, USA, November 2020.

[94] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA, pp. 1–6, Ottawa, ON, Canada, July 2009.

[95] R. Rama Devi and M. Abualkibash, “Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets - a review paper,”International Journal of Computer Science & Information Technology (IJCSIT), vol. 11, no. 3, pp. 65–80, 2019.

[96] Aljawarneh, S. A., & Vangipuram, R. (2020). GARUDA: Gaussian dissimilarity measure for feature representation and anomaly detection in the Internet of things. The Journal of Supercomputing, 76(6), 4376-4413.

[97] Cheng, Y., Xu, Y., Zhong, H., & Liu, Y. (2020). Leveraging Semi-supervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. IEEE Internet of Things Journal.

[98] Kim, D., Andalibi, V., & Camp, L. J. (2020, May). Fingerprinting Edge and Cloud Services in IoT. In 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE) (pp. 13-21). IEEE.

[99] Blaise, A., Bouet, M., Conan, V., & Secci, S. (2020). Botnet Fingerprinting: a Frequency Distributions Scheme for Lightweight Bot Detection. IEEE Transactions on Network and Service Management.

[100] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, and S. Tarkoma, “IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT,” in 37th IEEE International Conference on Distributed Computing Systems, ICDCS 2017, Atlanta, GA, USA, June 5-8, 2017, pp. 2177–2184, 2017

[101] Fatemifar, S., Awais, M., Arashloo, S. R., & Kittler, J. (2019, June). Combining multiple one-class classifiers for anomaly based face spoofing attack detection. In 2019 International Conference on Biometrics (ICB) (pp. 1-7). IEEE.

[102] Krawczyk, B., Triguero, I., García, S., Woźniak, M., & Herrera, F. (2019). Instance reduction for one-class classification. Knowledge and Information Systems, 59(3), 601-628.

[103] Ahmed, C. M., MR, G. R., & Mathur, A. P. (2020, October). Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In Proceedings of the 6th ACM on cyber-physical system security workshop (pp. 23-29).

[104] Selvathi, D., & Chandralekha, R. (2022). Fetal biometric based abnormality detection during prenatal development using deep learning techniques. Multidimensional Systems and Signal Processing, 33(1), 1-15.

[105] Ackerson, J. M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. Information, 12(7), 272.

[106] He, Z., Zhang, T., & Lee, R. (2019). Sensitive-sample fingerprinting of deep neural networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4729-4737).

[107] Fatemifar, S., Arashloo, S. R., Awais, M., & Kittler, J. (2021). Client-specific anomaly detection for face presentation attack detection. Pattern Recognition, 112, 107696.

[108] Botchkarev, A. (2018). Performance metrics (error measures) in machine learning regression, forecasting and prognostics: Properties and typology. arXiv preprint arXiv:1809.03006.

[109] Rácz, A., Bajusz, D., & Héberger, K. (2019). Multi-level comparison of machine learning classifiers and their performance metrics. Molecules, 24(15), 2811.

[110] Fang, L., Li, Y., Liu, Z., Yin, C., Li, M., & Cao, Z. J. (2020). A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks. IEEE Transactions on Industrial Informatics.

[111] Gautam, C., Balaji, R., Sudharsan, K., Tiwari, A., & Ahuja, K. (2019). Localized multiple kernel learning for anomaly detection: One-class classification. Knowledge-Based Systems, 165, 241-252.

[112] Villa-Pérez, M. E., & Trejo, L. A. (2020). m-OCKRA: an efficient one-class classifier for personal risk detection, based on weighted selection of attributes. IEEE Access, 8, 41749-41763.

[113] Wang, Q., Chen, H., Li, Y., & Vucetic, B. (2019, July). Recent advances in machine learning-based anomaly detection for industrial control networks. In 2019 1st International Conference on Industrial Artificial Intelligence (IAI) (pp. 1-6). IEEE.

[114] Seliya, N., Khoshgoftaar, T. M., & Van Hulse, J. (2009, November). A study on the relationships of classifier performance metrics. In 2009 21st IEEE international conference on tools with artificial intelligence (pp. 59-66). IEEE.

[115] Esmaeili M, Goki SH, Masjidi BH, Sameh M, Gharagozlou H, Mohammed AS. ML-DDoSnet: IoT Intrusion Detection Based on Denial-of-Service Attacks Using Machine Learning Methods and NSL-KDD. Wireless Communications and Mobile Computing. 2022 Aug 21;2022.