



Article

Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network

Hani Alshahrani ¹, Attiya Khan ², Muhammad Rizwan ³, Mana Saleh Al Reshan ^{4,*}, Adel Sulaiman ¹ and Asadullah Shaikh ⁴

¹ Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia; hmalsahrani@nu.edu.sa (H.A.); aaalsulaiman@nu.edu.sa (A.S.)

² Department of Computer Science, Kinnaird College for Women, Lahore 54890, Pakistan; attiya.niazi001@gmail.com

³ College of Engineering and Technology, University of Derby, Derby DE22 3AW, UK; m.rizwan@derby.ac.uk

⁴ Department of Information Systems, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia; asshaikh@nu.edu.sa

* Correspondence: msalreshan@nu.edu.sa

Abstract: The Industrial Internet of Things (IIoT) refers to the employment of the Internet of Things in industrial management, where a substantial number of machines and devices are linked and synchronized with the help of software programs and third platforms to improve the overall productivity. The acquisition of the industrial IoT provides benefits that range from automation and optimization to eliminating manual processes and improving overall efficiencies, but security remains to be forethought. The absence of reliable security mechanisms and the magnitude of security features are significant obstacles to enhancing IIoT security. Over the last few years, alarming attacks have been witnessed utilizing the vulnerabilities of the IIoT network devices. Moreover, the attackers can also sink deep into the network by using the relationships amidst the vulnerabilities. Such network security threats cause industries and businesses to suffer financial losses, reputational damage, and theft of important information. This paper proposes an SDN-based framework using machine learning techniques for intrusion detection in an industrial IoT environment. SDN is an approach that enables the network to be centrally and intelligently controlled through software applications. In our framework, the SDN controller employs a machine-learning algorithm to monitor the behavior of industrial IoT devices and networks by analyzing traffic flow data and ultimately determining the flow rules for SDN switches. We use SVM and Decision Tree classification models to analyze our framework's network intrusion and attack detection performance. The results indicate that the proposed framework can detect attacks in industrial IoT networks and devices with an accuracy of 99.7%.



Citation: Alshahrani, H.; Khan, A.; Rizwan, M.; Reshan, M.S.A.; Sulaiman, A.; Shaikh, A. Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network. *Sustainability* **2023**, *15*, 9001. <https://doi.org/10.3390/su15119001>

Academic Editors: Yan Yan and Shanwu Tian

Received: 30 April 2023

Revised: 27 May 2023

Accepted: 31 May 2023

Published: 2 June 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

For a long time, precarious infrastructures, such as communication networks, electric systems, and industrial systems, have customarily worked in segregation from extrinsic networks, such as the Internet. However, advanced technologies, such as artificial intelligence and software-defined networking, are progressively being combined in such rigid environments to provide further benefits, such as increased flexibility and improved quality. The definition of the SDN is as follows: “In the SDN architecture, the control plane and data plane are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications” [1]. The SDN centralizes the switch control functions into an SDN controller. The switches then function as packet-processing devices and carry out the commands from the SDN controller [2].

The SDN controllers can use machine learning and deep learning techniques to improve network security and monitoring [3]. The Industrial Internet of Things (IIoT) is another such technology. The typical Internet of Things consists of devices from simple sensors to smartphones and wearable ones that are connected. Combining these interconnected devices with automated systems makes it possible to collect information, analyze it, and create an action to assist someone with a specific task or learn from the process. In reality, it ranges from smart mirrors to beacons in stores and beyond. The Industrial Internet of Things is an innovative attempt to set up a smart manufacturing environment by employing the benefits of the Internet of Things in industrial process management. Industrial IoT focuses on machine-to-machine (M2M) communications, machine learning, and big data to enable enterprises and industries to have better reliability and efficiency in their operations. Leveraging the industrial IoT is revolutionizing factory and industrial segmentation by presenting its eminence. The Industrial Internet of Things is swiftly progressing and comprises several services and industries, as shown in Figure 1. In the hospitality industry, the IoT can be helpful in understanding guests' context and predicting their needs through intelligence and embedded sensors. There are endless possibilities with the IoT in the healthcare sector. The telemedicine system is based on the IoT. It is a practice of providing medical care by using data communications and interactive audiovisuals. Educational institutions are also taking advantage of various IoT applications. For instance, the IoT is being used in e-learning, m-learning, and u-learning.



Figure 1. IoT in different sectors.

The financial services sector also seems to be taking up the IoT. Insurance companies use telematics applications to foretell and assess the possible risks that might result in a claim from the client. Energy companies use smart grids to capture analytics, improve security, and allow for rapid restoration when power failures occur. The IoT is changing how the retail market works. Automated checkouts are installed on the front side of the stores. This solution allows workers to focus on business opportunities and needs instead of spending time as a cashier. One of the finest examples of industries that are adopting IoT applications is the manufacturing industry. The manufacturers are using the IoT to keep track of production flow during the production process. Through the data gathered from IoT devices, manufacturers can measure the quality of items.

The automated industry relies on the Industrial Control System (ICS). The ICS consists of various types of controllers that are used to control the industrial plants and monitor

their performance to guarantee their accurate operations [4,5]. There are various types of ICSs, such as distributed control systems (DCS), programmable logic controllers (PLC), supervisory control, and data acquisition systems (SCADA). Since the introduction of the IoT in industrial systems, they have changed into open architecture environments. As a result, industrial control systems have become vulnerable to security threats and attacks. A survey conducted by the UK Government has estimated that the average cost of a cyber-security breach ranges from £75,000 to £311,000 for small and medium-sized enterprises (SMEs) and from £1.46m to £3.14m for larger organizations. The Stuxnet attack against a nuclear power plant in Iran in 2010 is one of the most prominent cyber attacks. An SQL injection attack through a Trojan called the Night Dragon was conducted in 2010 to target oil companies globally. In 2013, the energy companies of North America were targeted by a Trojan called Dragonfly, and, in 2014, by Havex [6]. Some of the significant cyber incidents in ICSs are mentioned in Table 1.

Table 1. Major ICS cyber-incidents [7].

Year	Name	Type
1903	Marchone Wireless Hack	Attack
2000	Maroochy Water	Attack
2010	Stuxnet	Malware
2010	Night Dragon	Malware
2011	Flame	Malware
2012	Shamoon	Malware
2013	New York Dam	Attack
2013	Havex	Malware
2014	German Steel Mill	Attack
2014	Dragonfly	Campaign
2014	Black Energy	Malware
2016	“Kemuri” Water Company	Attack
2017	CRASHOVERRIDE	Malware
2017	NotPetya	Attack
2017	TRITON	Malware

The Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are the most prominent attacks that prevent legitimate users from accessing services for which they have paid. These types of attacks have become serious security risks for computer networks, causing a drop in network performance by consuming resources and deactivating services [8]. The DoS/DDoS also affects industrial IoT networks and devices [9–11]. Jamming attacks are also carried out against industrial IoT devices and networks. In this attack, fake signals are sent to interrupt proceeding radio transmissions of the IoT devices, and it further depletes the energy, bandwidth, CPUs, and sensors or memory resources of the IoT devices during failed communication attempts [12–14]. Thus, the security of industrial IoT devices and networks is one of the most critical concerns for researchers nowadays. There are various challenges with the implementation of security within industrial IoT networks and devices. Industrial IoT systems are heterogeneous systems containing several types of devices, types of data being shared and transferred, methods of communication, different resource levels of the devices, and system configurations. Each of these elements adds up to the challenges of IoT security. Secondly, billions of devices are connected and provide a vast area of research to focus on when considering resiliency, nominal function, and security.

Previously, the ICSs were autonomous systems, and they were isolated from the world. Thus, they were not open to attacks. However, the increase in connectivity of ICSs with the Internet for industrial management and communication for information transmission has made these systems more vulnerable to cyberattacks and anomalies. Thus, security has become a significant concern in industrial IoT systems because of their sensitive nature. The reliability, safety, and availability of industrial IoT systems are compromised by the lack of security parameters in the communication protocols.

1.1. Problem Statement

The IIoT makes use of the IoT technology in ICSs, i.e., industrial control systems. Since ICSs perform operations continuously, they also produce a large amount of data. These systems have become vulnerable to network attacks and other malicious attacks due to internet connectivity. Therefore, it is not possible to ensure the authenticity of the data. Thus, ensuring the security of IIoT devices and the IIoT network is a significant problem that needs to be solved.

1.2. Limitations of Existing Work

Various intrusion detection and classification schemes employing artificial intelligence have been studied in the literature [15]. Most of the security frameworks developed to secure industrial IoT networks had a high false alarm rate. Furthermore, they were unable to detect unknown attacks on the network. Hence, they were not very effective in securing industrial IoT networks against network attacks, resulting in costly damages to industrial IoT networks, data losses, and loss of revenue. Thus, we used machine learning algorithms and SDN technology in our framework for the effective detection of malicious attacks, network intrusion, and the identification of abnormal behavior in industrial IoT networks and devices.

1.3. Contributions of this Paper

The major contributions of our paper are manifold:

1. In this paper, a discussion on cyber attacks and security threats to the industrial IoT environment is given.
2. We propose an SDN-based security framework to detect industrial IoT network intrusion by analyzing traffic flow data.
3. The main objective of our work is to protect industrial IoT devices and networks against malicious attacks and security threats. For that purpose, we consider different attacks on industrial IoT environments, such as DoS/DDoS attacks, jamming attacks, and man-in-the-middle attacks.
4. We use machine learning algorithms, i.e., SVM and Decision Tree on an SDN controller, for early intrusion detection within a network or device of the industrial IoT and determine the flow rules for the SDN switches based on analyzed data.
5. We evaluate the proposed SDN-based security framework using the NSL-KDD intrusion detection dataset.
6. The evaluation results show that the proposed framework provides high efficiency of security and can detect intrusion and malicious attacks in industrial IoT networks.

2. Literature Review

Several studies have been conducted to analyze the security vulnerabilities in IIoT systems. Various challenges prevent securing the IIoT and ensuring end-to-end security in the IIoT environment. In this section, we present brief descriptions of the various types of research conducted for the IIoT environment. These types of research mainly focus on the attacks on the IIoT environment and several other threats to the IIoT systems. George et al. [16] proposed a graph-based framework to represent the vulnerability relationship in the IIoT network. It also helps in the risk assessment of the IIoT network. They also proposed various risk mitigation strategies for improving IIoT network security.

Furthermore, they discussed methods to identify hot spots in the IIoT networks. The proposed system performance is evaluated by simulating with graphs of varying sizes and structures. Rubio et al. [17] presented the analysis of applying Opinion Dynamics in the IIoT environment. They addressed how the Opinion Dynamics algorithm can improve attack traceability in the IIoT environment. The proposed system is evaluated through a case study, and the results demonstrate the feasibility of the approach in IIoT infrastructures. AL-Hawawreh et al. [18] proposed a deep learning-based model that can learn using the information gathered from TCP/IP packets for anomaly detection in IICSs. The authors developed the model by a continuous training process that is carried out using a deep auto-encoder and a deep feed-forward neural network framework evaluated using NSL-KDD and UNSW-NB15.

Samsonov et al. [19] presented various approaches to provide security in IIoT environments. They employed edge and fog computing technologies, various data transmission technologies, cryptographic techniques, IIoT device protection, and blockchain technology to secure IIoT systems. However, they have not discussed the system reconfiguration for new tasks, the motive for choosing security mechanisms, and shared IIoT devices management. Teochew [20] addressed various security problems in the IIoT. The author also discussed various attacks on different IIoT architecture layers, attacks based on application scenarios, and third-party hardware/software-based attacks. Furthermore, the recommendations for approaching these security challenges are discussed.

Esfahani et al. [21] proposed a hash and OR operation-based lightweight authentication mechanism for M2M communication in an IIoT environment. The authors claim that the proposed system has a low computational cost, storage, and communication overhead while confidentiality, authentication, and session key agreement are achieved. Moreover, the proposed system also resists specific security attacks, i.e., man-in-the-middle attacks, modification attacks, replay attacks, and impersonation attacks. Wing et al. [22] proposed a blockchain-based solution to secure the IIoT through its security technology and tools. They further gave recommendations to guide future blockchain developers and researchers. Chen et al. [23] analyzed the security threats in IIoT systems and designed a protection framework for securing IIoT systems. The author analyzed the security threats to the IIoT through the communication protocols used and the main functionalities for each level of typical IIoT architecture. They identified the concealed dangers in the data processing layer, data transmission layer, and data acquisition layer. The proposed security framework provides protection measures against security threats in these layers. Choo et al. [24] presented various performances, privacy, and security-related issues of the IIoT. They addressed existing cryptographic solutions presented in 21 papers. Lastly, they presented various potential research agendas. Sinai et al. [25] presented the concept of the IoT, IIoT, and Industry 4.0. They addressed various opportunities and challenges associated with these systems. The work also focuses on the security challenges of IIoT systems that originate from the high sensitivity of managed information. Bakhshi et al. [26] addressed various security issues and threats in the IIoT. They focused mainly on the security threats on a cloud-side layer, consisting of abstraction levels and data accumulation, of the IoT. The authors referred to the Cisco and Microsoft Azure IoT architectures as the reference models. Further, they subdivided the threats based on security attacks and vulnerabilities. Kwon et al. [27] analyzed the security issues of the provisioning process in the IWSN by investigating the necessary ISN standards, i.e., WirelessHART, ISA 100.11.A, and Zigbee, an ISA 100.11a-certified device, and various provisioning process-related research works. They tested and analyzed the provisioning process using ISA 100.11a to verify its security issues. Lastly, they discussed the future research direction on providing security for the IWSN in the IIoT age. The summary of the techniques presented above is listed in Table 2.

Numerous studies have been proposed for the detection of malicious traffic and attacks in the industrial IoT. From the studies discussed above, it is noticed that machine learning algorithms could improve network security in the IIoT environment. Moreover, it is also observed that the models for securing IIoT networks are still under development. For this

purpose, we combined SDN technology and machine learning algorithms for intrusion detection in IIoT networks.

Table 2. Major works in IIoT.

Paper	Year	Main Idea
[16]	2018	Proposes a graph-based framework to represent the vulnerability relationship in IIoT networks.
[17]	2020	Presents the idea of applying Opinion Dynamics in the IIoT environment.
[18]	2018	Proposes a deep learning-based model that can learn using the information gathered from TCP/IP packets for anomaly detection in IICSSs.
[19]	2019	Presents various approaches to provide security in IIoT environments. The authors employed edge and fog computing technologies, various data transmission technologies, cryptographic techniques, IIoT device protection, and blockchain technology to secure IIoT systems.
[20]	2020	Discusses various attacks on different IIoT architecture layers, attacks based on application scenarios, and third-party hardware/software-based attacks.
[21]	2017	Proposes a hash and OR operation-based lightweight authentication mechanism for M2M communication in the IIoT environment.

3. IoT, Industrial IoT, and Industry 4.0

3.1. IoT

The IoT refers to a system of billions of interrelated physical devices, i.e., computing devices, digital and mechanical machines, animals, people, or objects connected to the Internet, and can transfer and share data over the Internet.

Layers of IoT

The essential IoT layers act as the backbone of IoT systems. These layers can form the basis of the development of effective IoT multilayered architecture. These layers are discussed below and summarized in Table 3.

Table 3. Representation of IoT by Seven Layer Architecture.

Layer	Services Provided
Perception Layer	Actuators, Sensors, Devices, Controllers, Machines
Transport Layer	Protocols, Communications, WiFi, Networks, Bluetooth
Processing Layer	Data Accumulation, Data Abstraction
Application Layer	Smart Applications, Decision-Making Software, Device Monitoring and Control Services, Artificial Intelligence and Machine Learning-Based Solutions
Edge Layer	Preprocessing on Local Servers, Gateways, and other Edge Nodes across the network
Business Layer	Business Models, CRM, Business Intelligence Programs
Security Layer	Device Security, Cloud Security, Connection Security

- Perception Layer: This is the physical layer that consists of sensors, actuators, devices, and machines. Sensors, i.e., gauges, meters, and probes, sense and gather information about the industrial IoT environment. The actuators used in lasers, motor controllers, and robotic arms translate electrical signals from IoT systems into physical actions.
- Transport Layer: This layer transports the sensor data between the perception layer and processing layer using technologies, such as WiFi, LPWAN, Ethernet, and ZigBee.

- Processing Layer: This layer is also called the middleware layer. The processing layer is responsible for collecting information from the transport layer and performing processing on it [28].
- Application Layer: The application layer is responsible for interacting with end-users directly. It consists of various applications, such as mobile apps, device monitoring software, business intelligence services, etc. All the applications have their application layer protocols.

There are some additional layers in IoT systems to cater to the business needs of IoT systems. These layers are described below:

- Edge Layer: This performs the preprocessing of data close to the edge. It occurs on local servers, gateways, and other edge nodes across the network.
- Business Layer: The business layer is the layer on which businesses, based on collected data, can make decisions.
- Security Layer: The security layer covers all the IoT layers mentioned above. It includes device security, connection security, and cloud security.

3.2. Industrial IoT

The industrial IoT refers to the utilization of the IoT in the industrial sector and business settings. The industrial IoT is the intersection of operational technology (OT) and information technology (IT). An advance notification is generated from a machine about an approaching breakdown; the cloud-based intelligent factory floors obtain the status of assembly-line production or the progress of raw materials in real time. These are examples of how future industries and factories will work. Industrial Control System: An industrial control system refers to hardware devices and software integration that support and monitor critical infrastructures. It includes a programmable logic controller (PLC), a remote terminal unit (RTU), an intelligent electronic device (IED), a control server, a distributed control system (DCS), supervisory control and data acquisition (SCADA), and sensors [29].

Components of Industrial IoT

The components of the industrial IoT can vary concerning the application. However, generally, they are categorized into three areas discussed below and shown in Figure 2.



Figure 2. Components of industrial IoT.

- Front-End Edge Devices: Front-end edge devices, i.e., sensors or control devices, are responsible for data collection and acting on the data. This data can be a temperature reading, accelerometer reading, or video feed. The sensors/devices can be used as individual units or multiple sensors bundled together, and the sensors can be embedded into devices that perform more tasks than just sensing things.
- Connectivity Technology: Once the data is collected, the next step is to send the data to the cloud. Similarly, the cloud sends back commands to the industrial IoT system. Industrial IoT systems rely majorly on wireless technology, including Bluetooth, Mesh Networks, WiFi, and LPWAN.

- Industrial IoT Platform Data Analysis: The industrial IoT system contains industrial IoT software for the analysis of acquired and transmitted data. The industrial IoT software can also make decisions and push commands back to the controls at the edge.

3.3. Industry 4.0

Industry 4.0 is the term often used for the fourth industrial revolution. Industry 4.0, which includes the industrial IoT and smart manufacturing, combines physical production and operations with smart digital technologies, big data, and machine learning to build a more complete and well-connected environment for organizations focused on supply chain management and manufacturing. It is defined as the current trend of data exchange and automation in manufacturing technologies, including the Internet of Things, cyber-physical systems, cognitive computing, cloud computing, and creating a smart industry or factory. Industry 4.0 is based on the cyber-physical system, i.e., intelligent machines. These systems use modern control systems with software systems embedded and connected to the IoT through Internet addresses. In this way, production and products get connected to the network and can communicate, enabling value creation, real-time optimization, and new ways of production. The objective is to monitor the processes and assets in real time, enabling processes to make autonomous decisions and fulfill customer needs. Industry 4.0 is characterized in the following way:

- Provides more automation compared to the third industrial revolution;
- Shifting from centralized industrial control systems to systems where intelligent products define the production steps;
- Bridging the gap between the digital and physical world using cyber-physical systems;
- Customization or personalization of products;
- Closed-loop control systems and data models.

4. Proposed Methodology

In this section, we propose an SDN-based model for attack detection in an industrial IoT environment. The proposed framework comprises three components, i.e., industrial IoT devices, a centralized SDN controller, and SDN-enabled switches, as shown in Figure 3:

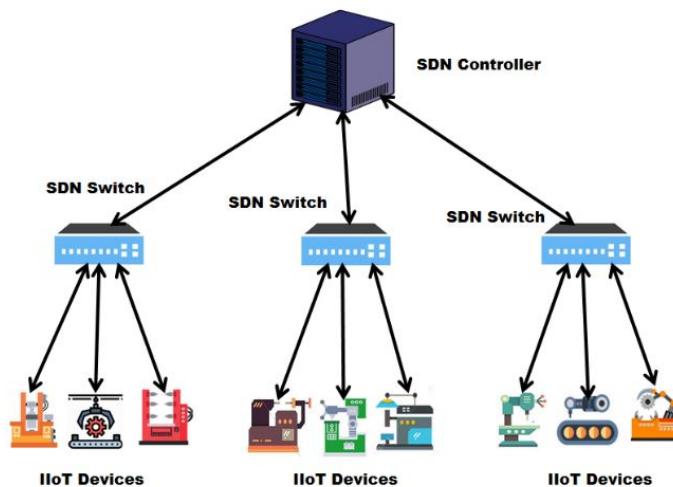


Figure 3. SDN-Based Model for Industrial IoT Anomaly Detection.

- The industrial IoT device is any IoT-enabled device operating in the industry. Industrial IoT devices may include drilling gears, green energy devices, smart meters, smart irrigation devices, smart frost systems, smart assembly lines, and various sensors. All of these devices are connected to the allocated SDN-enabled switch.
- Each industry is assigned an SDN switch to connect its devices. The switch is SDN-enabled and security policies are installed within it. The SDN-enabled switches

monitor the traffic flow in industrial IoT devices and provide traffic data to the SDN controller.

- The industrial IoT devices are connected to the SDN switches and these switches are connected to the SDN controller. The machine learning algorithm is applied to the SDN controller to detect anomalous traffic and the abnormal behavior of the traffic flow. As a result, the flow rules are defined for the switches.

The industrial IoT devices working in the same industry are connected to the SDN-enabled switch. The SDN-enabled switches provide the traffic flow data to the SDN controller, responsible for determining whether the traffic flow is normal or anomalous. Based on the analyzed data, it determines the flow rules for the SDN-enabled switches. Based on these rules, the SDN-enabled switches perform various operations on the traffic flow, such as complete flow blocking, partial flow blocking, and blacklisting the attack source. For anomaly detection, a machine learning algorithm is applied to an SDN controller. Machine learning techniques can aid in developing security policies for SDN controllers by accurately predicting potential susceptible hosts [30].

Dataset: We evaluate the performance of the framework using the NSL-KDD dataset, which is used for network intrusion detection. The reasonable number of test and train set records makes this dataset run experiments affordably on a complete set instead of selecting a small portion of the dataset randomly. Each record contains 41 attributes that describe various aspects of the flow and are labeled as either an attack type or normal. The 42nd attribute contains information on the various five kinds of network connection vectors, which are divided into one normal class and four attack classes. The NSL-KDD dataset has the following advantages:

- The train set contains no duplicated records, therefore, the classifier will not provide any biased outputs.
- There are no duplicate records in the test set, resulting in higher reduction rates.

In this dataset, there are 22 different types of attacks classified into four major types of attacks [31]. The four attack types are classified as DoS, R2L, Probe, and U2R. These attacks are shown in Table 4.

Table 4. Attacks in NSL-KDD [31].

Types of Attacks	Attacks in Training Set of NSL-KDD
DoS	Neptune, back, smurf, pod, land, teardrop
Probe	PortswEEP, satan, Nmap, ipsweep
R2L	Warezclient, ftpwrite, warezmaster, IMAP, guess password, spy, phf, multihop
U2R	Butteroverflow, rootkit, perl, loadmodule

Data Preprocessing: In data preprocessing, feature selection is done to select the subset of the most relevant features. For feature selection, we have used a correlation-based feature selection (CFS) algorithm. Correlation is a measurement of the linear relationship between two or more variables. The reason for using CFS for feature selection is that useful variables have a strong correlation with the target. The variables should also be uncorrelated with one another but correlated with the target. We can predict one variable based on the other if the two are correlated. As a result, if there is a correlation between two features, the model only requires one because the second does not provide any new information. Using the CFS algorithm, 23 uncorrelated features were selected for prediction.

Support Vector Machine(SVM): Support Vector Machine (SVM) is a supervised learning technique used for the regression and classification of problems. The kernels and algorithms in SVM are used to analyze the data for regression and classification. The SVM algorithm's goal is to create a decision boundary or best line that can segregate the n-dimensional space into the classes such that in the future new data points can be easily put into an incorrect category. The best

line is called the hyperlink. For creating a hyperlink, SVM chooses the extreme points. The extreme points are called support; hence, the algorithm is named Support Vector Machine.

Decision Tree: The Decision Tree is a supervised machine-learning technique where the data is split based on a certain parameter. The Decision Tree contains two types of entities, i.e., leaves and decision nodes. The leaves are outcomes, whereas; on the decision nodes, the data is split. There are two types of decision trees based on the target variable type:

- **Categorical Variable Decision Trees:** Categorical Variable Decision Trees are those which have categorical target variables.
- **Continuous Variable Decision Trees:** Continuous Variable Decision Trees are those which have continuous target variables.

The proposed SDN-based framework effectively overcomes the problem of network anomaly detection in the industrial IoT. The SDN controller has a global view and receives monitoring information from the SDN switches. The SDN switches are responsible for monitoring the industrial IoT devices' traffic flow and sending each packet of flow to the SDN controller. The SDN controller detects anomalous behavior through the data provided by the switches. The machine learning algorithm is applied to the SDN controller for detecting potentially dangerous network traffic. Based on the classified data, the SDN controller determines the traffic flow rules for the switches, which makes this framework effective in network anomaly detection.

5. Experimentation and Results

We used the NSL-KDD dataset in our analysis, which is used for network intrusion detection. The machine learning techniques, i.e., SVM and Decision Trees, are used to evaluate the effectiveness of the proposed model. We assessed the machine learning algorithms by using the following quality metrics [32]:

$$\text{Accuracy} = \frac{TN + TP}{FP + FN + TP + TN} \quad (1)$$

$$\text{Precision} = \frac{TP}{FP + TP} \quad (2)$$

$$\text{Recall} = \frac{TP}{FN + TP} \quad (3)$$

$$\text{F1-score} = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} \quad (4)$$

5.1. Classification Using SVM

The NSL-KDD dataset is classified using the linear SVM model and quadratic SVM model of classification. The benefit of using SVM is that, while it is a linear model, we can utilize the kernels to represent the linearly non-separable data. Moreover, SVM uses considerably less memory and is more efficient in large dimensional spaces. The dataset in the linear and quadratic SVM models is classified using 125,973 observations. The accuracy of the quadratic SVM classifier model is higher compared to the linear SVM model. The prediction speed of the linear SVM model is greater compared to the quadratic SVM model. The training time taken by the linear SVM model to classify the NSL-KDD dataset is 699.22 s; whereas; it is 465.28 s in the quadratic SVM model. The summary of the results of both of the SVM models is shown in Table 5.

Since the quadratic SVM model shows greater accuracy compared to the linear SVM model, the confusion matrix for the classified data in the quadratic SVM model is shown in Figure 4, which summarizes the performance of the quadratic SVM classification model. Figure 4a shows the number of observations against the predicted class and true class. Figure 4b shows the true positive rates and false negative rates. Figure 4c shows positive predictive values and false discovery rates.

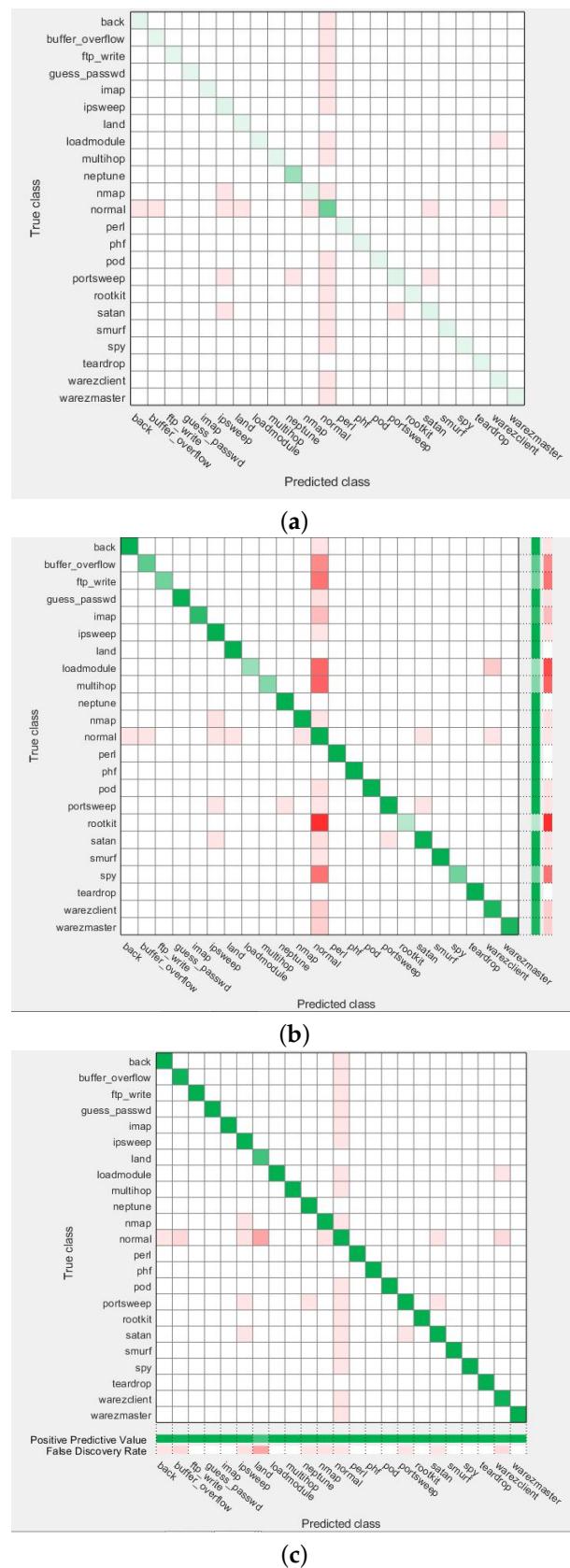


Figure 4. Confusion Matrix for data classification using Quadratic SVM model. **(a)** Number of Observations; **(b)** TP Rates/FN Rates; and **(c)** Positive Predictive Rates/False Discovery Rates.

The scatter plot, ROC curve, and parallel coordinates chart for the NSL-KDD dataset using the quadratic SVM model are given in Figure 5. The horizontal lines in the scatter plot in Figure 5a depict an excellent fit to the data. The ROC curve in Figure 5b shows the area under the curve (AUC) to be 1.00 or 100%, which denotes an ideal curve for data classification. Thus, the positive and negative results are distinguished 100% of the time using this classifier. The parallel coordinates plot for the dataset in the quadratic SVM is shown in Figure 5c.

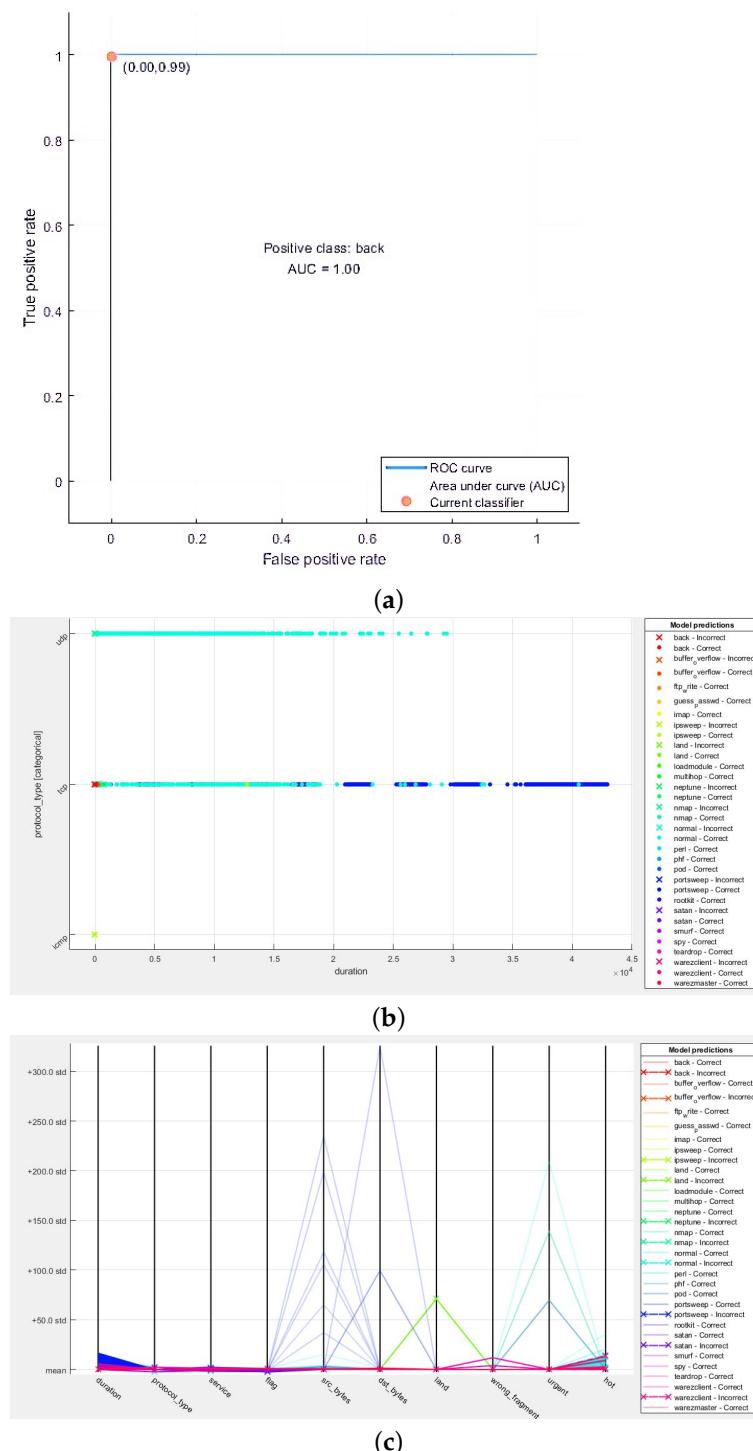


Figure 5. Classification using Quadratic SVM Model. (a) ROC Curve using Quadratic SVM Model; (b) Scatter Plot using Quadratic SVM Model; (c) Parallel Coordinates Plot using Quadratic SVM Model.

Table 5. Summary Linear SVM and Quadratic SVM Classification Results.

Model	Accuracy	Prediction Speed	Training Time
Linear SVM	99.3%	1300 obs/s	699.22 s
Quadratic SVM	99.7%	1100 obs/s	465.28 s

5.2. Classification Using Decision Tree

The NSL-KDD dataset is classified using a Decision Tree classifier model, i.e., Fine Tree and Medium Tree. A Decision Tree is a quick technique to find the most important variables and relationships between two or more variables. In comparison to other classification algorithms, they are extremely quick and efficient. Moreover, there is no outsider influence or missing data in the Decision Tree; the Decision Tree requires less data. The dataset is classified using 125,973 observations. The accuracy of the Acceptable Tree classifier model is much higher than the Medium Tree classifier model. The prediction speed of a Fine Tree classifier is also much higher than a Medium Tree classifier. The training time of the Fine Tree classifier model is 11.029 s; whereas, it is 35.687 s for the Medium Tree classifier model. The summary of the results of both of the Decision Tree classifier models is shown in Table 6.

Table 6. Summary of Fine Tree and Medium Tree Classification Results.

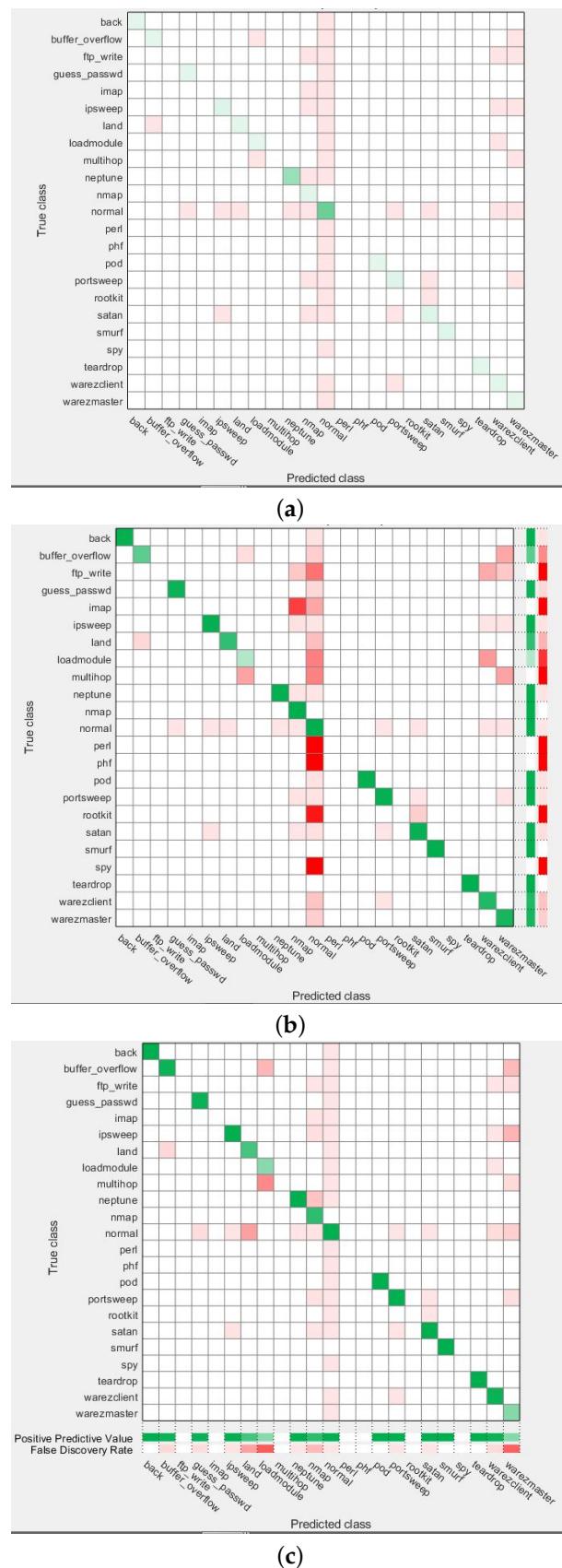
Name of Model	Accuracy	Prediction Speed	Training Time
Fine Tree	99.4%	570,000 obs/s	11.029 s
Medium Tree	95.9%	190,000 obs/s	35.687 s

Since the Fine Tree classifier model shows greater accuracy compared to the Medium Tree classifier model, the confusion matrix for the classified data using the Fine Tree model is shown in Figure 6, which summarizes the performance of the Fine Tree classification model. Figure 6a shows the number of observations against the predicted class and true class. Figure 6b shows the true positive rates and false negative rates. Figure 6c shows the positive predictive values and false discovery rates.

The scatter plot, ROC curve, and parallel coordinates chart for the NSL-KDD dataset using the Fine Tree model are given in Figure 7. The ROC curve in Figure 7a shows the area under the curve (AUC) to be 1.00 or 100%, which denotes an ideal curve for data classification. Thus, the positive and negative results are distinguished 100% of the time using the Fine Tree classifier model. The horizontal lines in the scatter plot in Figure 7b depict an excellent fit to the data. The parallel coordinates plot for the dataset in the Fine Tree model is shown in Figure 7c.

5.3. Performance Analysis

We classified our data using the SVM models and Decision Trees as shown in Figure 8. In the SVM model, we used the linear SVM model and Quadratic SVM model; whereas, in the Decision Trees, the Fine Tree model and Medium Tree model were used. The comparison of the accuracy of the classifier models is shown in Figure 8a. The bar chart shows the accuracy of the Quadratic SVM model to be 99.7%, which is the highest compared to the other three models. Thus, the Quadratic SVM model is the most accurate data classification model used in our experimentation. The comparison of the prediction speed of the classifier models is shown in Figure 8b. The bar chart shows the prediction speed of the Fine Tree classifier model to be 570,000 obs/s, which is the highest compared to the other three models. Thus, the Fine Tree model is the highest prediction speed model used in our experimentation.



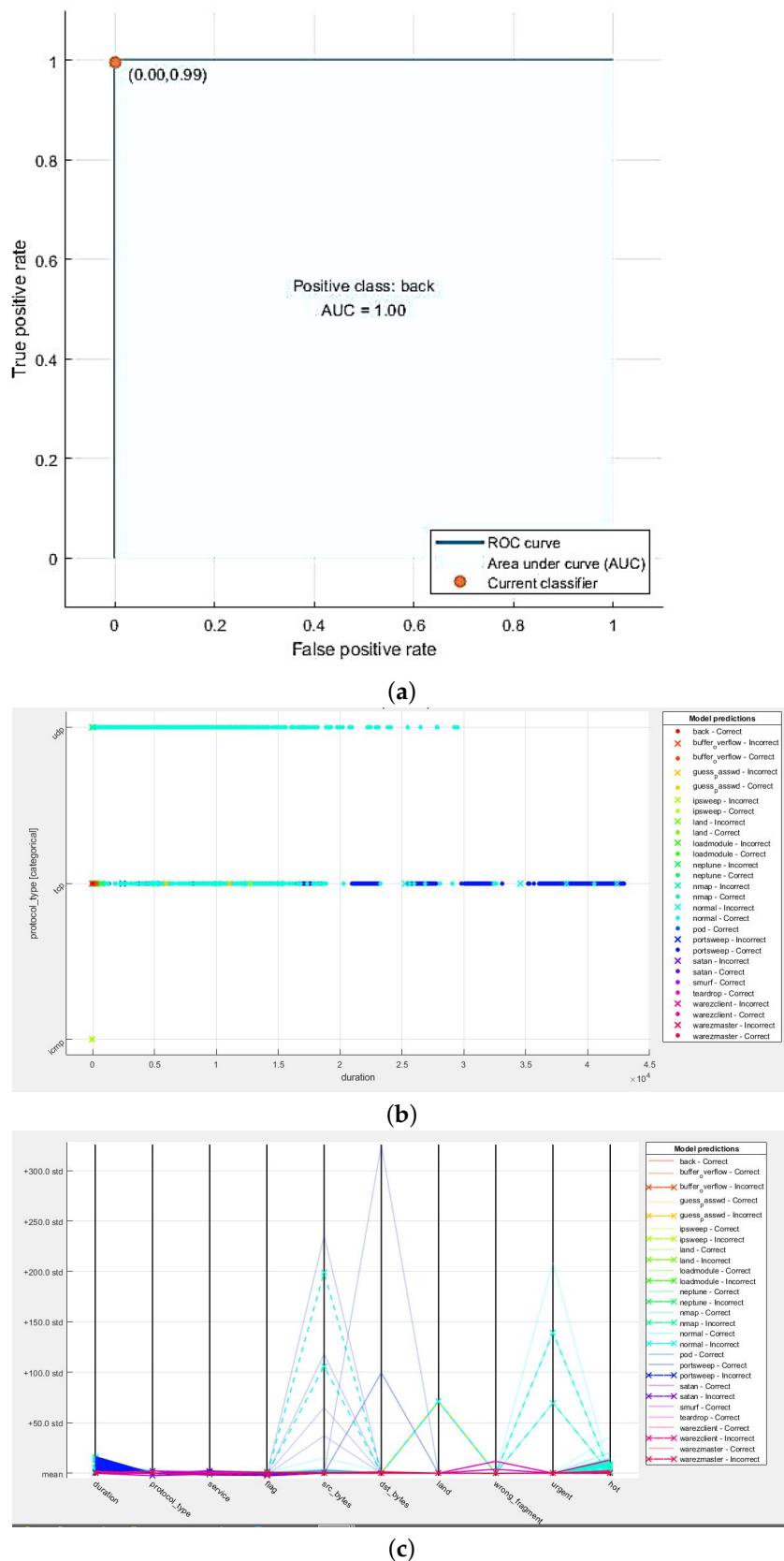


Figure 7. Classification using Fine Tree Model. (a) ROC Curve classification using Fine Tree model; (b) Scatter Plot classification using Fine Tree model; (c) Parallel Coordinates Plot for classification using Fine Tree model.

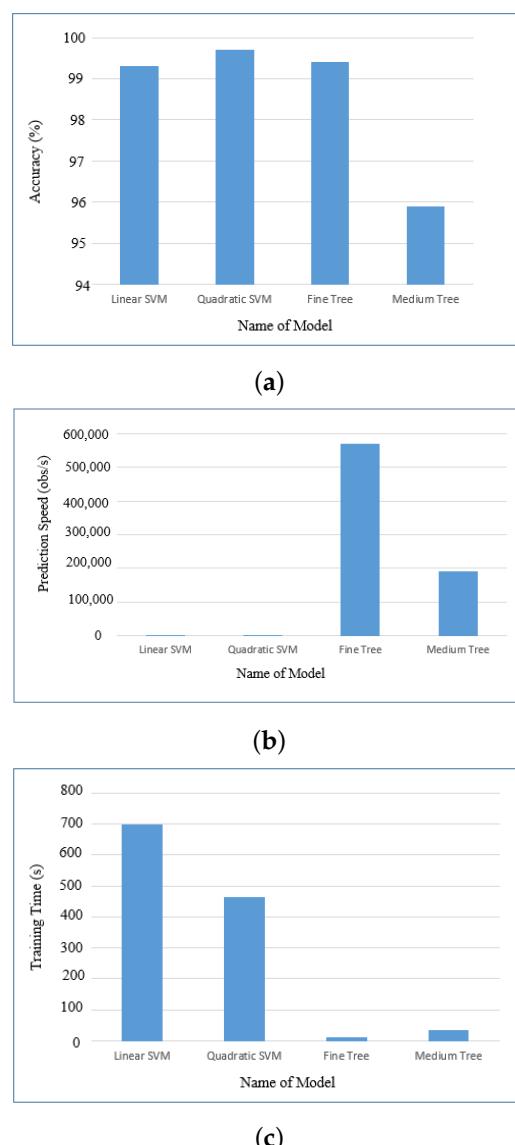


Figure 8. Comparison of various functions. (a) Accuracy of Classification Models; (b) Prediction Speed of Classifier Models; (c) Training Time of Classifier Models.

The comparison of the training time of the classifier models is shown in Figure 8c. The bar chart shows the training time of the Fine Tree classifier model to be 11.029 s, which is the least compared to the other three models. Thus, the Fine Tree model is the least used training time model in our experimentation. The summary of the accuracy, prediction speed, and training time of the classifier models are shown in Table 7.

Table 7. Summary of Linear SVM and Quadratic SVM Classification Results.

Name of Model	Accuracy	Prediction Speed	Training Time
Linear SVM	99.3%	1300 obs/s	699.22 s
Quadratic SVM	99.7%	1100 obs/s	465.28 s
Fine Tree	99.4%	570,000 obs/s	11.029 s
Medium Tree	95.9%	190,000 obs/s	35.687 s

6. Conclusions and Future Work

IoT deployment in the industrial sector has several benefits, such as optimization, automation, the elimination of manual processes, and increased efficiency. However, security remains a challenge in industrial IoT devices and networks. The security threats and cyber-attacks on industrial IoT networks and devices cause industries and businesses to suffer financial losses, reputational damage, and the theft of important information. Many approaches and frameworks have been applied for intrusion detection in industrial IoT devices and networks. Machine learning techniques play a vital role in these approaches. In this work, we proposed an SDN-based framework using machine learning techniques to detect threats and cyber-attacks in industrial IoT networks and devices. We used the NSL-KDD dataset in our experimentation for classification. SVM and Decision Tree classification models are used for the evaluation of our framework. The performance of the SVM and Decision Tree is evaluated, and the quadratic SVM showed 99.7% accuracy. In the future, we will employ newer data sources to enhance the adaptability and efficacy of this study.

Author Contributions: Conceptualization, H.A., A.K. and M.R.; methodology, M.S.A.R., A.S. (Adel Sulaiman) and A.S. (Asadullah Shaikh); software, H.A., A.K. and M.R.; validation, M.S.A.R., A.S. (Adel Sulaiman) and A.S. (Asadullah Shaikh); formal analysis, H.A., A.K. and M.R.; investigation, M.S.A.R., A.S. (Adel Sulaiman) and A.S. (Asadullah Shaikh); resources, M.R. and A.K.; data curation, M.S.A.R. and H.A.; writing—original draft preparation, H.A., A.K. and M.R.; writing—review and editing, M.S.A.R., A.S. (Adel Sulaiman) and A.S. (Asadullah Shaikh); visualization, A.S. (Adel Sulaiman); supervision, A.S. (Asadullah Shaikh); project administration, M.S.A.R. and M.R.; funding acquisition, H.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the General Research Funding Program, grant code NU/DRP/SERC/12/32.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The authors accessed the data on 8 May 2021 from Kaggle: Machine Learning and Data Science Community, and data is available at <https://www.kaggle.com/datasets/hassan06/nslkdd> (accessed on 8 May 2021).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Wang, C.; Liu, Y. A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 393–430. [[CrossRef](#)]
2. Yang, G.; Shin, C.; Yoo, Y.; Yoo, C. A case for SDN-based network virtualization. In Proceedings of the 2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Houston, TX, USA, 3–5 November 2021; pp. 1–8.
3. Sultana, N.; Chilamkurti, N.; Peng, W.; Alhadad, R. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer Peer Netw. Appl.* **2019**, *12*, 493–501. [[CrossRef](#)]
4. Asghar, M.R.; Hu, Q.; Zeadally, S. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Comput. Netw.* **2019**, *165*, 106946. [[CrossRef](#)]
5. Azzam, M.; Pasquale, L.; Provan, G.; Nuseibeh, B. Forensic readiness of industrial control systems under stealthy attacks. *Comput. Secur.* **2023**, *125*, 103010. [[CrossRef](#)]
6. Venkatachary, S.K.; Prasad, J.; Samikannu, R. Cybersecurity and cyber terrorism—In energy sector—A review. *J. Cyber Secur. Technol.* **2018**, *2*, 111–130. [[CrossRef](#)]
7. Hemsley, K.E.; Fisher, R.E. *History of Industrial Control System Cyber Incidents*. No. INL/CON-18-44411-Rev002; Idaho National Lab. (INL): Idaho Falls, ID, USA, 2018. . [[CrossRef](#)]
8. Ali, T.E.; Chong, Y.W.; Manickam, S. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Appl. Sci.* **2023**, *13*, 3183. [[CrossRef](#)]
9. Verma, A.; Ranga, V. Machine learning based intrusion detection systems for IoT applications. *Wirel. Pers. Commun.* **2020**, *111*, 2287–2310. [[CrossRef](#)]
10. Marinov, M.B.; Nikolov, N.; Dimitrov, S.; Todorov, T.; Stoyanova, Y.; Nikolov, G.T. Linear interval approximation for smart sensors and IoT Devices. *Sensors* **2022**, *22*, 949. [[CrossRef](#)]

11. Debauche, O.; Mahmoudi, S.; Guttaduria, A. A new edge computing architecture for IoT and multimedia data management. *Information* **2022**, *13*, 89. [[CrossRef](#)]
12. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [[CrossRef](#)]
13. Uyanik, H.; Ovatman, T. An investigation of the transmission success in Lorawan enabled IoT-HAPS communication. *Internet Things* **2022**, *20*, 100611. [[CrossRef](#)]
14. Morais, R.; Mendes, J.; Silva, R.; Silva, N.; Sousa, J.J.; Peres, E. A versatile, low-power and low-cost IoT device for field data gathering in precision agriculture practices. *Agriculture* **2021**, *11*, 619. [[CrossRef](#)]
15. Javed, A.R.; Usman, M.; Rehman, S.U.; Khan, M.U.; Haghghi, M.S. Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4291–4300. [[CrossRef](#)]
16. George, G.; Thampi, S.M. A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitations. *IEEE Access* **2018**, *6*, 43586–43601. [[CrossRef](#)]
17. Rubio, J.E.; Roman, R.; Lopez, J. Integration of a Threat Traceability Solution in the Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6575–6583. [[CrossRef](#)]
18. AL-Hawawreh, M.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* **2018**, *41*, 1–11. [[CrossRef](#)]
19. Saksonov, E.A.; Leokhin, Y.L.; Azarov, V.N. Organization of Information Security in Industrial Internet of Things Systems. In Proceedings of the 2019 International Conference “Quality Management, Transport and Information Security, Information Technologies” (IT QM IS), Sochi, Russia, 23–27 September 2019; pp. 3–7. [[CrossRef](#)]
20. Tsochev, G. Some Security Problems and Aspects of the Industrial Internet of Things. In Proceedings of the 2020 International Conference on Information Technologies (InfoTech), Varna, Bulgaria, 17–18 September 2020; pp. 1–5. [[CrossRef](#)]
21. Esfahani, A.; Mantas, G.; Maticsek, R.; Saghezchi, F.B.; Rodriguez, J.; Bicaku, A.; Maksuti, S.; Tauber, M.G.; Schmittner, C.; Bastos, J. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment. *IEEE Internet Things J.* **2019**, *6*, 288–296. [[CrossRef](#)]
22. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2020**, *10*, 100081. [[CrossRef](#)]
23. Chen, H.; Hu, M.; Yan, H.; Yu, P. Research on Industrial Internet of Things Security Architecture and Protection Strategy. In Proceedings of the 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Jishou, China, 14–15 September 2019; pp. 365–368. [[CrossRef](#)]
24. Choo, K.R.; Gritzalis, S.; Park, J.H. Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3567–3569. [[CrossRef](#)]
25. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [[CrossRef](#)]
26. Bakhshi, Z.; Balador, A.; Mustafa, J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Barcelona, Spain, 15–18 April 2018; pp. 173–178. [[CrossRef](#)]
27. Kwon, S.; Jeong, J.; Shon, T. Toward Security Enhanced Provisioning in Industrial IoT Systems. *Sensors* **2018**, *18*, 4372. [[CrossRef](#)] [[PubMed](#)]
28. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796. [[CrossRef](#)] [[PubMed](#)]
29. Karmakar, A.; Dey, N.; Baral, T.; Chowdhury, M.; Rehan, M. Industrial Internet of Things: A Review. In Proceedings of the 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 18–20 March 2019; pp. 1–6. [[CrossRef](#)]
30. Nanda, S.; Zafari, F.; DeCusatis, C.; Wedaa, E.; Yang, B. Predicting network attack patterns in SDN using machine learning approach. In Proceedings of the 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, USA, 7–10 November 2016; pp. 167–172.
31. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [[CrossRef](#)]
32. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e3997. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.