electronics

MDPI

Article

Deep Learning-Based Intrusion Detection Methods in Cyber-Physical Systems: Challenges and Future Trends

Muhammad Umer [1], Saima Sadiq [2], Hanen Karamti [3], Reemah M. Alhebshi [4], Khaled Alnowaiser [5], Ala' Abdulmajid Eshmawi [6], Houbing Song [7,*] and Imran Ashraf [8,*]

1 Department of Computer Science & Information Technology, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
2 Department of Computer Science, Khwaja Fareed University of Engineering and Information Technology, Rahim Yar Khan 64200, Pakistan
3 Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
4 Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 22254, Saudi Arabia
5 Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
6 Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 22254, Saudia Arabia
7 Department of Electrical Engineering and Computer Science, Embry Riddle Aeronautical University, Daytona Beach, FL 32114-3900, USA
8 Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38544, Korea
* Correspondence: h.song@ieee.org (H.S.); imranashraf@ynu.ac.kr (I.A.)

Citation: Umer, M.; Sadiq, S.; Karamti, M.; Alhebshi, R.M.; Alnowaiser, K.; Eshmawi, A.A.; Song, H.; Ashraf, I. Deep Learning-Based Intrusion Detection Methods in Cyber-Physical Systems: Challenges and Future Trends. *Electronics* **2022**, *11*, 3326. https://doi.org/10.3390/electronics11203326

Academic Editors: Piyush Kumar Shukla, Manoj Kumar, Xiaochun Cheng and Prashant Kumar Shukla

Received: 13 September 2022
Accepted: 30 September 2022
Published: 15 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: A cyber-physical system (CPS) integrates various interconnected physical processes, computing resources, and networking units, as well as monitors the process and applications of the computing systems. Interconnection of the physical and cyber world initiates threatening security challenges, especially with the increasing complexity of communication networks. Despite efforts to combat these challenges, it is difficult to detect and analyze cyber-physical attacks in a complex CPS. Machine learning-based models have been adopted by researchers to analyze cyber-physical security systems. This paper discusses the security threats, vulnerabilities, challenges, and attacks of CPS. Initially, the CPS architecture is presented as a layered approach including the physical layer, network layer, and application layer in terms of functionality. Then, different cyber-physical attacks regarding each layer are elaborated, in addition to challenges and key issues associated with each layer. Afterward, deep learning models are analyzed for malicious URLs and intrusion detection in cyber-physical systems. A multilayer perceptron architecture is utilized for experiments using the malicious URL detection dataset and KDD Cup99 dataset, and its performance is compared with existing works. Lastly, we provide a roadmap of future research directions for cyber-physical security to investigate attacks concerning their source, complexity, and impact.

Keywords: cyber-physical security; network security; deep learning; Internet of Things

1. Introduction

A cyber-physical system (CPS) is the interconnection of a cyber and physical system, where the exchange of data and information takes place in real time [1]. CPS is playing a significant role in the Internet of Things (IoT) based industry and offers substantial economic potential [2]. CPS considers the interaction of physical, network, and computing systems and is based on the Internet of Things (IoT). It has evolved as the Internet of cyber-physical Things which offers a wide range of services such as smart homes, smart cities, e-health, e-commerce, etc. A large number of industrial equipment can be controlled wirelessly

by adopting CPS which helps in managing complex and mega industrial systems [3]. Interconnected components of CPS have the ability to sense the surroundings and process the IoT-based objects remotely. It has the resilience to change the processes in runtime with real-time computing [4]. Moreover, CPS is embedded in various systems and is being utilized in diverse fields like communication, transport, health care, military, and various autonomous systems, as shown in Figure 1.

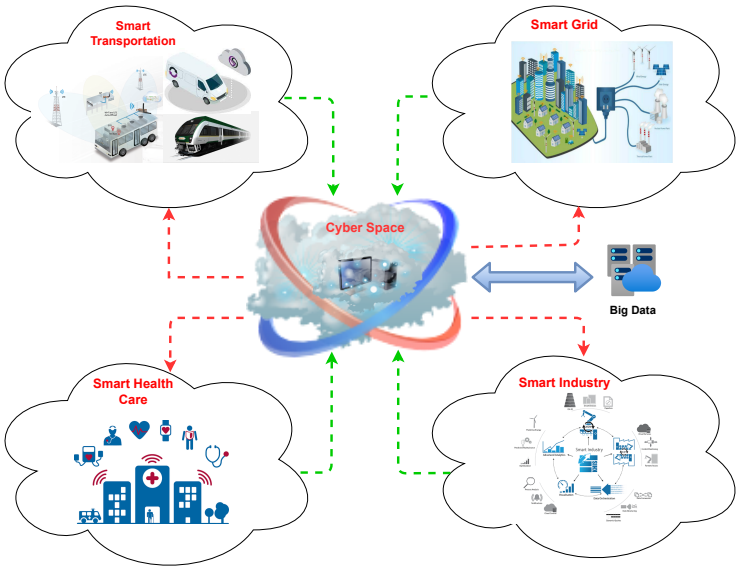

Figure 1. Applications of CPS.

CPS-based train control systems exchange control signals between the ground stations and trains wirelessly in real-time and provide more safety than traditional systems against accidents [5]. An increase of connectivity in the complex networks also gives rise to the invading paths of the attackers in CPS [6]. Controlling networks and software are vulnerable to attackers that try to infiltrate and malfunction CPS-based systems [7]. When a network is accessed by an attacker, it disturbs the execution of control software in the cyber system and gets hold of the physical system to cause power failure or other manipulation on the attacker's detection system [8]. These attacks on cyber and physical systems can cause substantial economic loss by launching havoc on industrial processes and equipment. For example, in 2014, blast furnaces were damaged in a German steel mill by a cyber-attack and in 2015 a huge outage of power was caused by malware in Ukraine due to the malfunctioning of the plant [7]. Therefore, the security of the cyber-physical system against adversarial attacks is an emerging research area. In CPS security, physical processes are considered an addition and come up as an extended form of cybersecurity. For instance, cracking a password due to personal information leakage is a main security issue of cybersecurity. However, in CPS security, there is no adverse effect of such information leakage on the system. However, if unauthorized access affects the system process, it may damage the physical dynamics of the system. Therefore, researchers emphasize controlling the physical dynamic of the CPS. Various factors that affect CPS are unpredicted events and quick environmental changes. In addition, one of the major problems with CPS security is the false alarms on the detection of cyber-physical attacks. Due to the exceedingly large CPS and complexity among its components, accuracy degrades in real CPS [9].

From a theoretical point of view, complex and huge systems can be represented with differential equations of a high order. In a high-order mathematical model, it is not possible to obtain an exact complex model, so unconsidered variables become vulnerable to attackers and lead to inaccurate detection. In CPS security modeling, data used in training for anomaly detection are acquired in a controlled environment set up or experiment [10]. For obtaining a reliable and safe CPS security model, machine learning models are deployed

that work by finding correlations between input and output on large amounts of data. Machine learning algorithms help in generating a model that can explore the complex relationship in CPS components, handle different network protocols and complex cyber software, and enhance the security level. In this paper, the attacks that damage the CPS and manipulate the processes are discussed. We mainly focus on different security designs of CPSs. The main contributions of the article are:

- CPS architecture is presented into three layers, namely the physical layer, network layer, and application layer. The layered architecture is used to provide more clarity in terms of functionality. Then, CPS attacks on each layer are discussed, mainly from the perspective of the physical system.
- Key features, challenges, and attack handling methods using machine learning-based models are highlighted regarding different layers.
- Keeping in view the nature of different attacks, a simple deep learning model is deployed for attack detection, especially the detection of malicious URLs and CPS attacks. For this purpose, multilayer perceptron (MLP) is adopted as it is not used in the existing literature. Despite existing hybrid and sophisticated models, the proposed MLP provides better and more robust results.
- Finally, future research directions are outlined for CPS security research to handle CPS attacks in real-time networks.

The rest of the paper is organized as follows: Section 2 provides the most recent related work of CPS. Section 3 provides the CPS architecture as a layered approach. Section 4 introduces different types of CPS attacks at each layer. Section 5 discusses securing methods for CPS. Section 6 presents the potential research directions for CPS security. Finally, we conclude the article and provide future directions in Section 7.

2. Related Work

Recent research on intrusion detection frameworks in the literature demonstrates the enhanced performance of machine learning models. The intrusion detection method uses hardware and software to identify intrusions in networks [11]. The deployment of an embedded system enables the network-level implementation of security regulations. An intrusion detection strategy is divided into network-based and host-based. The online data are used to extract features for classification-based intrusion detection models. Machine learning methods, including supervised and unsupervised models as well as deep learning models, are frequently utilized in intrusion detection systems.

Unsupervised learning techniques automatically cluster a huge amount of data without the use of labels. However, little amounts of tagged data can aid in enhancing network security or cybersecurity performance. This method cannot produce high accuracy due to the unique characteristics of unknown assaults. In order to locate clusters based on similarity, an unsupervised learning approach for intrusion detection has been developed [12]. Models of supervised learning that produce positive outcomes require labels for training. Machine learning models have been widely used in conventional intrusion detection techniques. However, due to classifiers' poor generalization capabilities, these models were unable to effectively anticipate various invasion attacks. The hybrid technique developed by the researchers enhanced the intrusion detection system while enhancing the capabilities of machine learning models. A combination of SVM, particle swarm optimization (PSO), and k nearest neighbor algorithms were used by Aburomman et al. [13]. The effectiveness of the categorization was greatly increased by combining these methods. Marteau [14] discovered symbolic sequences and independent attacks from standard system call sequences have significant resemblance. He demonstrated the importance of covering similarity as a measure of an anomaly in host-based detection by comparing and analyzing three similarity metrics.

The intrusion detection frameworks face a significant challenge from high-dimensional data in an increasing number of incursions and attacks. An essential data feature has to be studied to reduce dimensions in order to decrease time complexity and resource use.

Hussian et al. designed anomaly detection using SVM and artificial neural networks (ANN) for fraud detection in the second stage [15]. Similar to this, the authors decreased the dimensionality of the data by using the PCA-LDA ensemble method [16]. One of the efficient techniques for detecting intrusions is clustering. The authors applied an improved density peak algorithm for intrusion detection in [17].

Vehicles' security concerns have been the subject of multiple publications over the past few years. The public key infrastructure built on blockchain is a noteworthy trend in this regard. In order to handle the distribution and maintenance of the Certificate Revocation List (CRL) in vehicle public key infrastructure, the authors employed blockchain technology in [18]. An accountable credential management framework for vehicular communication is presented in another research as a potential solution to these issues [19]. This system takes advantage of transparency log techniques while addressing issues unique to vehicular communication. The authors proposed a framework that checks the authenticity of the IDs and keys on the blockchain, which promises a simple authentication process and lessens computational and communication load to access the network's safety messages [20]. A reputation evaluation method was proposed in [21] that used both direct past encounters, and indirect judgments about automobiles were provided in order to stop the dissemination of fake messages.

To identify malicious attacks, deep learning models and hierarchical methods have been developed. By removing dimensions from correlation and information gain [22], ANN is applied to the KDD99 dataset for intrusion detection and produced better results in terms of accuracy. The authors used PCA and multivariate CA to detect DDoS attacks in real-time. Musafer et al. [23] designed an approach using an autoencoder for intrusion detection on a current dataset CICIDS2017. The scientists developed a memetic algorithm for aberrant traffic identification and tested it on the NSLKDD and KDD-CUP 99 datasets, two well-known deep learning models [13]. In order to create an efficient framework for intrusion detection, feature augmentation has been combined with SVM [24]. This has produced reliable results in terms of false alarm rates. Researchers have utilized multilevel intrusion detection for this purpose [25]. For intrusion detection, a unique deep learning model has been designed to increase accuracy [26]. Increasing network connectivity and the incorporation of terrestrial networks into satellite networks provide new security concerns and difficulties. One of the most frequent assaults that affect satellite-terrestrial integrated networks is DDoS, which slows down service. For identifying DDoS in satellite and terrestrial networks, many research works have been carried out. An adaptive strategy based on Q-learning and a jamming detection system were proposed by Mowla et al. [27]. It has been suggested to use machine learning models to monitor traffic linked to socket programming [28]. It has been built to identify DDoS attacks dynamically using fuzzy logic [29].

These research projects aim to develop appropriate methods for intrusion detection in satellite and terrestrial networks. Table 1 presents a comparative analysis of the research papers that have been addressed.

Table 1. Comparative analysis of the existing approaches.

Ref.	Methods	Dataset	Findings
[13]	Memetic	NSL-KDD & KDD99	PSO with higher accuracy
[14]	SC4ID algorithm	UNM & ADFA-LD	A new, more accurate approach for handling abnormal system calls.
[15]	SVM-ANN	NSL-KDD	High performance by a hybrid model
[16]	PCA-LDA-SVM	KDD-CUP 99	Dimensionality reduction
[22]	Deep learning	KDD-CUP 99 & NSL-KDD	Deep learning model with reliable outcomes.
[23]	Sparse autoencoder	CICIDS 2017	Uses trigonometric simplexes
[24]	SVM	NSL-KDD	The logarithmic marginal density ratio
[25]	MSML	KDD-CUP 99	Multi-level intrusion detection
[27]	Q learning	CRAWDAD	Federated jamming
[28]	DT, KNN, NB & DNN	KDD-CUP 99, open-stack cloud	Socket programming and OpenStack firewall
[29]	Fuzzy logic	DDoS attack (T-shark)	Dynamic DDoS attack detection
[30]	SVM-KNN-PSO	KDD 99	High precision ensemble model utilising a weighted method.
[31]	MDRA	KDD-CUP 99	Real-time attack detection
[32]	MINDFUL	KDD-CUP 99, UNSW-NB 15, CICIDS 2017	Multi-channel for deep feature learning
[33]	Deep hierarchical	NSL-KDD & UNSW-NB15	Data balancing using SMOTE
[34]	DT-RFE	KDD-CUP 99 & NSL-KDD	Stacked approach

3. CPS Architecture, Layers and Components

In this section, CPS architecture, along with its layers and components, is discussed. A CPS consists of several components and can have a complex structure between the physical system and cyber software. It is difficult to analyze its entire architecture. Therefore, the CPS architecture is classified into three main layers; the physical layer, the network layer, and the application layer. Intuitive and simple layered architecture is presented in Table 2.

3.1. Physical Layer

The physical layer includes the objects of the physical system that are utilized in the real world. In this layer, the CPS system involves sensors and actuators in which information is transferred through sensors to the cyber world, and the actuator operates according to commands. Physical processes are performed by sensing and actuating in a continuous-time domain. Sensor-based devices such as radio frequency identification tags (RFID) and global positioning system (GPS) collect data in real-time to track objects of the physical systems. Data examples include heat, location, electric consumption, sound, and light signals [35]. Sensors collect data according to its type from the local or wide range and transfer it to the network layer which is later sent to the application layer for further analysis. Efficient security protocols are required according to the capability of devices for reliable communication between these layers. In a complex system, the physical system has constraints due to the power of an external battery. To solve this problem, the physical layer connects to the computation system using a network layer.

Table 2. Layered architecture with complete functionality and attack details.

Layer	Function	Attack	Target Area	Safety Measure
	Analysis of Data & Information	Code Injection Botnets Malware Trojans Worms Buffer Overflow	Security Privacy Authentication Safety	Firewall Strong Authentication Strong Authorization Trust Management
	Transmission of Data & Information	DoS/DDoS Repudiation Man in the middle Meet in the middle	Confidentiality Integrity Availability Authentication	Strong Password Policy Encryption Secure Tunneling
	Collection of Data & Information	Passive Replay Port Scan Eavesdropping	Privacy Authentication Confidentiality	Secure System Data Protection Source Authentication Trust Management

In order to build a re-configurable radio-based environment of the propagation channel and increase the received signal power, re-configurable intelligent surfaces (RIS) have been studied as a possible approach. A study focused on joint beamforming design and optimization for hybrid satellite-terrestrial relay networks with RIS support, when links from the satellite and base station (BS) to numerous users are blocked [36]. A satellite system should be secure and energy efficient in designing a communication system. A design is proposed by the researcher to improve security and decrease power consumption in [37].

3.2. Network Layer

The second layer of CPS architecture is the network layer. This layer is used for the communication of the physical layer (real world) and the application layer (cyber world). Due to the network in the CPS, it is possible to control physical systems remotely. A local area network is used for local data transmission and communication protocols involving 4G, 5G, ZigBee, Wi-Fi, and Bluetooth. This layer assures data transmission and routing using cloud computing, firewalls, gateways, and an intrusion detection method. These features make CPS cost-effective and better than the previously point-to-point controlling system. Before transferring data to the next layer, it is important to secure the transmission by avoiding malicious attacks including malware, denial of service, distributed denial of the surface, and unauthorized access. For example, wireless networks such as WirelessHart and ZigBee remotely enable the controlling of industrial processes in real time. Moreover, in the smart grid, the distributed network protocol (DNP) provides a system of centralized monitoring and control. There is a great challenge for power-restricted devices due to the overhead of power and processing.

3.3. Application Layer

The interactive and third layer of the CPS architecture is the application layer where intelligent tasks are performed in the cyber world. It performs processing on the received information from the network layer which obtains that from the physical devices such as sensors or actuators. After executing applications, the system predicts the next time step and provides intelligent functionality to the CPS user. Decision-making complex algorithms are applied to the aggregated data [38]. Information based on the automated rightly invoked actions at the physical layer is processed by this layer. Protecting and preserving private data are required against leakage. In CPS, the application layer has no power or computational constraints, and it can operate efficiently. For example, the smart grid planning system predicts the electric power consumption of the region based on the readings observed by sensors at the physical layer from the previous data. It helps in electric power generation in plants. Likewise, in smart factories, digital twin technology can predict the throughput of the production line and can improve production. The most commonly used approach is data masking, secret sharing, and privacy maintenance. Furthermore, this layer needs a strong authentication process to avoid unauthorized access. In this layer, a huge amount of generated data handling and its protection in an efficient manner is a challenging task.

4. Security Threats and Attacks

Security measures and services are not integrated into CPSs by design like other networking systems. This makes the CPS system more vulnerable to security threats and opens doors for attackers in launching security attacks. The reason behind this is the heterogeneous nature of the physical devices concerning their operations and the different protocols and technologies used for communication in CPS. In recent years, cyber-attacks targeting CPS are increasing, and some of the CPS attacks are presented in Figure 2.

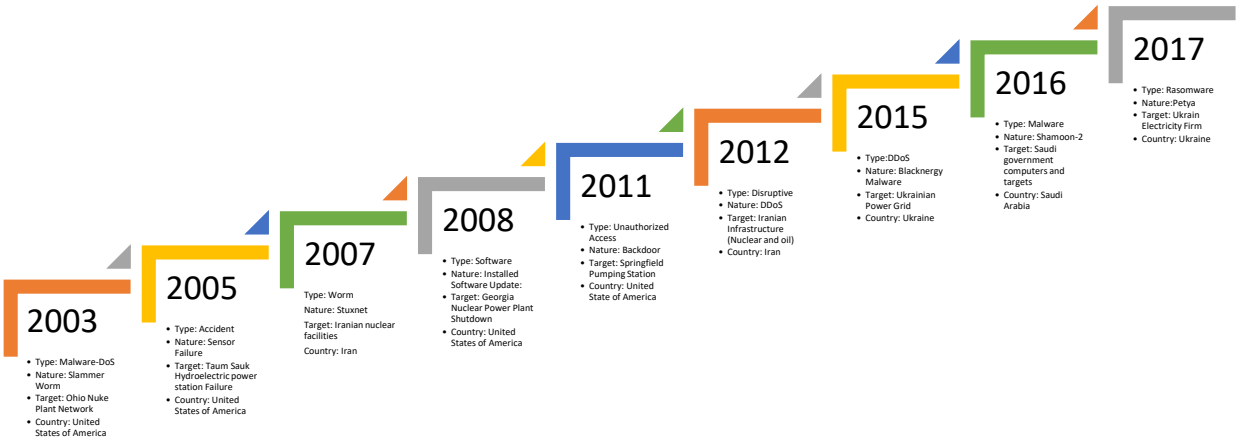

Figure 2. Real CPS attacks in recent years.

A security attack on the CPS system causes malfunctioning of the physical device or processes of the system. A CPS system is a combination of the physical, networking, and computing system, if any of these systems are attacked by an attacker, the CPS system become unstable. The CPS system is more vulnerable because of the connectivity of the different networks. CPS systems lack protection and security measures in their design and operation. Different CPS attacks are discussed regarding each layer.

4.1. Attacks on Physical Layer

Physical systems transmit a control signal and sensor data through the network. When an attacker accesses the network, it can modify the control-related data on the network which results in divergence from the physical state. Attackers can manipulate it in three ways: the physical layer, firstly it manipulates sensor data, secondly, it manipulates control signals, and thirdly the attacker manipulates both sensor data and control signals.

During a sensor attack, sensor movement is manipulated to deceive the computing system in performing state estimation which causes computational faults in input data of the actuating process. Then, this faulty input creates malfunctioning of the physical system. In the physical layer, sensor attacks require more attention such as pole dynamic attack (PDA) is a famous sensor attack where attackers use matrices of the physical system and then swiftly change its state which creates difficulty in detecting PDA by traditional detecting methods. The controller attack is another type of physical layer attack which is the modification of the input signal. Attackers or malicious users destabilize the physical system by unpredicted control signals. Controller attacks affect the dynamics and operation of the physical system. In the cyber study, controller attacks on input signals are called zero dynamics attacks (ZDA). During ZDA, the internal state of the physical system diverges toward infinity which is not detected by sensor data due to the property of zero dynamics. A combined attack is a combination of a sensor attack and a controller attack; it launches on both channels. Therefore, it is difficult to launch a combined attack by using sensor and control signals both. However, the detection of combined attacks requires more resources in handling both types of attacks. Attackers have complete knowledge of the physical dynamics of the system in launching a covert attack that is a combined attack. Hackers or malicious users use complete information in generating control input signals from the sensors.

4.2. Attacks on Network Layer

The network layer takes information from the physical layer and transmits it to the application layer in real time. This layer is responsible for the reliable exchange of information in layers. In this layer, attackers destabilize the system by disturbing data transmission in real time. There are three types of CPS attacks at the network layer. The

first is the denial of service (DoS) attack that drops data packets and specifically prevents the transmission of control data. These attacks interrupt the data transmission and cause a communication jam. In a wireless network, it is easy to interrupt the transmission, but, in wireless networks, jamming signals are generated by the specialized antenna for signal interference. Man-in-the-middle is a DoS attack that creates vulnerabilities in the network and stops packet forwarding and destabilizes the system by diverting the state. In a communication-based train control system, communication failure occurs if an attacker launches a jamming attack.

The second is the flooding attack that causes a delay in data transmission by exhausting resources, such as network bandwidth or device memory, intentionally. In this attack, a massive amount of data traffic is generated to block a network, and the memory of devices is also filled. A flooding attack can be launched without having enough information about the network and make CPS unstable. During a flooding attack, the physical system switches to fail-safe mode and reduces the operation for safety purposes.

The third is the packet manipulation attack which consists of two phases; the first is packet stealing and the second is packet manipulation. In the first phase, the attacker accesses the network nodes and devices using vulnerabilities of the network; then, the network packet is forwarded to the attacker. However, in the second phase, the attacker modifies that packet and sends it back to the destination. If the hacker manipulates by adhering to network protocols then the destination node deceives by packet manipulation. If the control information is modified, then it has an equal effect on the network as attacks on the physical layer. For example, in a communication-based train control system, packet manipulation can cause train accidents by manipulating the route direction. However, a Sybil attack deceives different nodes on the traffic road in a vehicular ad-hoc network and causes traffic congestion. Sending incorrect messages results in inconvenience for vehicle traffic.

4.3. Attacks on Application Layer

The application layer performs complex and intelligent functions in the CPS system. Attackers can access important information from the computing systems via network interface cards or serial ports. The attacker can distract the computation of important components including the process scheduler and file systems. As the size of CPS increases, it becomes more complex and vulnerable to attackers. Two types of attacks occur at the application layer. The first is the hardware attack at the application layer by disturbing the working of computational components like the power supply, CPU, and DRAM of CPS. Hardware attacks create intentional faults to the hardware such as system crashes by cutting off the power supply. When the computational system stops working, it lost control over the physical system. These types of attacks are executed by intriguing malicious malware. Hardware attacks include power viruses, thermal attacks, and row hammer attacks.

The second is the software attack that disturbs the flow and execution of applications by generating system errors. These attacks generate wrong and faulty responses to requests of the physical layer. These faulty commands lead to defective control over the system. Software attacks at the application layer include black door attacks, false-code execution, Stuxnet attack, BlackEnergy malware, and Triton. These application layer attacks cause malfunctioning of software by changing parameter settings causing degradation of performance and emergency stop of autonomous service. A cyberattack known as a "man-in-the-middle" (MitM) involves the interception of communications between two parties, frequently in order to acquire login credentials or personal data. Numerous cryptographic techniques, including multi-party computation, proxy re-encryption, and homomorphic encryption, are used to protect the privacy of devices and data integrity [39].

5. Securing CPS

Over the last few years, an alarming increase has been witnessed in the rate of cyber-attacks on CPS with disastrous results. Due to the heterogeneity and complex nature of

CPS, it is highly prone to malicious attacks. These attacks can collapse the whole system as presented in Figure 2. A detailed description of these attacks can be found in [35]. Different types of attacks on CPS include eavesdropping (obtaining sensitive information from network traffic), password cracking, phishing emails, DoS/DDoS, and different types of malware. However, securing a CPS is not an easy task due to the increase of challenges and limitations in existing solutions. IoT and CPSs rely on privacy, security, reliability, and consistency, and these characteristics are combined to develop a trustworthy system. A secure environment for CPS can be maintained by fulfilling security goals. Security goals for CPS are presented in Figure 3.

Figure 3. Security goals of CPS.

To maintain the confidentiality of CPS, cryptographic techniques have been adopted, while the integrity of CPS can be maintained by avoiding any modification (physical or logical) in data. Availability of different devices is the main goal of CPS that can be achieved by encryption techniques to avoid DoS/DDoS attacks. Authentication is the first step of defense, and it should be well designed and maintained. User authentication can be ensured by using biometric parameters. However, preserving the privacy of CPS while dealing with big data are not easy. Different techniques are designed to avoid any possible malicious event or cyber-attack.

For securing CPS, non-cryptographic solutions have also been designed. Any solution against malicious events in a network is designed by considering different factors such as cost, configuration, and placement in a network.

5.1. Intrusion Detection Technique

An intrusion detection system can be employed at the borderline of any router in an IoT-based network or in any physical system of CPS to avoid malicious attacks. Previously, machine learning-based solutions have been provided by many researchers for the detection of malicious behavior in CPS. Therefore, we present a deep learning-based model for intrusion detection on CPS. We use a simple and customized deep learning model, multilayer perceptron (MLP) to illustrate the process of intrusion detection and malicious URLs detection in CPS. The purpose of the experiment is not to propose a sophisticated deep learning model; instead, we aim to show the running performance and usage of the deep learning model. This effort can provide deep insight to readers that can assist them in further research along similar lines. The materials and methods used in the experiments are presented below.

5.2. Approach

We used two datasets for experiment purposes; one is the malicious user dataset while the other is the KDD cup 1999 dataset [40]. URL reputation is treated as a binary classification problem where positive examples present malicious URLs and negative examples present benign URLs. It consists of 2.4 million examples of URLs while the number of features is 3.2 million. The second dataset is KDD Cup 1999 Data [41] that was used in the competition of Knowledge discovery and data mining tool for intrusion detection in a network. In the case of attack or intrusion, the connection is considered as 'bad' otherwise 'good'; data simulation is performed in a military environment. NSL-KDD [42] is also widely used for evaluating intrusion detection models. Each record of intrusion has symbol features (three-dimensional) and digital features (42-dimensional). The labels are mainly divided into normal, DoS, Prob, U2R, and R2L types of attacks. It contains a total of 125,973 samples in the train set and 22,544 samples in the test set.

MLP is used to perform classification tasks, which is a feed-forward neural network consisting of the input layer, hidden layer, and output layer. Each neuron of the input layer represents the feature; hidden layer neurons process the data and store weights during the training phase and neurons of the output layer represent the output variable. The number of nodes or neurons in the input layer is the same as the number of features feeds to the neural network layer and the number of nods or neurons in the output layer represents the number of target classes. The number of nodes in the hidden layer is an architectural issue, and the main focus is to generalize it and optimize it with the appropriate number of parameters for the classification task. MLP works on backpropagation that is based on the gradient descent method. Figure 4 presents the architecture of MLP.

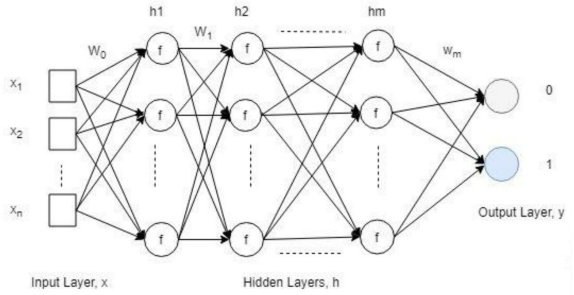

Figure 4. Architecture of MLP used for experiments.

It has been used in various classification tasks. Hyperparameters of the deep learning model include epochs, number of layers, and batch size. Considering limited computing power and the training time, the model is kept simple, having only three layers with a batch size of 32, and Relu is used as an activation function. We utilized 80% data for training and 20% for testing the model.

Figure 5 presents the experimental results of MLP in terms of accuracy, precision, recall, and F1 score. Results reveal that a simple deep learning-based model is very effective in predicting malicious URLs and intrusion detection. Having low computational power in a wireless network, a simple deep learning model is showing robust results with 99.62% for the malicious URL detection dataset and 99.87% for intrusion detection on the KDD Cup 99 dataset.

Table 3 shows the classification results of the proposed approach and other methods in the literature [34,40,41]. The proposed MLP outperforms other methods in terms of all evaluation measures for both datasets. In the detection of malicious URLs, the proposed approach exceeds the results proposed in [40] using SVM. Lian et al. [34] proposed feature reduction based on correlation by combining recursive feature elimination with a decision tree, but the results are still lower than the proposed approach on the KDD Cup 99 dataset. Overall, the proposed method has shown better performance in KDD Cup 99 and malicious URL detection datasets.

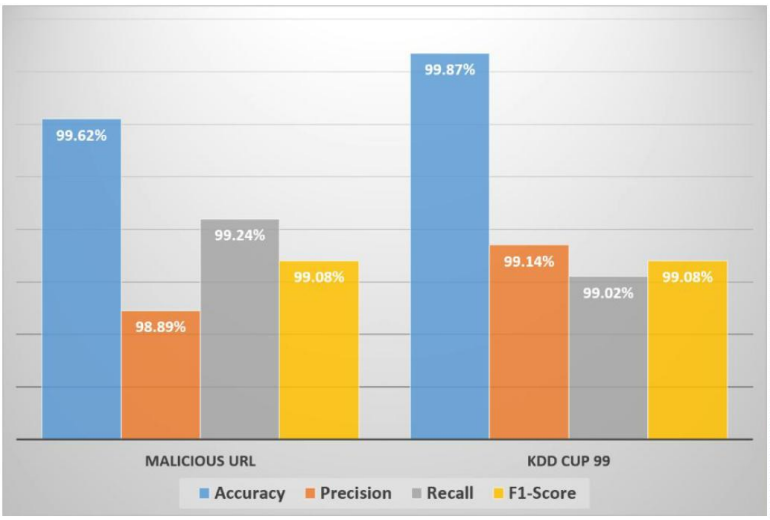

Figure 5. Performance of the deep learning model.

Table 3. Classification result of all learning models.

Method	Dataset	Accuracy	Precision	Recall	F1-Score
Proposed	Malicious URL Detection	99.62	98.89	99.24	99.08
SVM [40]		90.70	93.43	88.45	-
RF [40]		96.28	91.44	94.42	-
Proposed	KDD Cup 99	99.87	99.14	99.02	99.08
Deep Learning [41]		92.00	-	-	-
Rule Based Model [41]		89.00	-	-	-
DT-RFE [34]		99.21	-	-	-

Table 4 shows 10-fold results to show the generalizability and consistency of the proposed model. Table 5 shows the performance comparison of the proposed approach with existing techniques using KDD-CUP and NSL-KDD datasets. It can be observed that the proposed can provide higher accuracy regarding different kinds of attacks like DoS, R2L, etc.

Table 4. 10-fold cross-validation results using MLP.

Sr#	Accuracy	Precision	Recall	F-Score
1st-Fold	99.5%	98.6%	99.1%	99.1%
2nd-Fold	99.2%	98.7%	99.2%	98.6%
3rd-Fold	99.1%	98.3%	99.3%	98.4%
4th-Fold	99.8%	98.7%	99.9%	99.5%
5th-Fold	100.0%	99.1%	99.8%	99.3%
6th-Fold	99.6%	98.6%	99.7%	99.2%
7th-Fold	99.4%	98.7%	99.6%	99.1%
8th-Fold	100.0%	99.4%	99.5%	99.7%
9th-Fold	99.2%	98.4%	99.4%	99.8%
10th-Fold	99.7%	98.5%	99.7%	99.9%
Average	99.60%	98.81%	99.16%	99.01%

Table 5. Accuracy comparison of classifiers on KDD-CUP and NSL-KDD datasets.

Ref.	Model	Dataset	DoS	Prob	R2L	U2R	Avg. Accuracy
Proposed	MLP	KDD-CUP 99	1.00	0.99	0.99	0.99	0.99
[43]	PCA+MCA		0.99	0.98	0.97	0.81	0.94
[32]	DNN		-	-	-	-	0.92
[34]	DT-RFE		0.99	0.99	0.97	0.99	0.99
Proposed	MLP	NSL-KDD	1.00	0.99	0.99	1.00	0.99
[15]	SVM-ANN		1.00	0.99	0.77	0.88	0.91
[33]	Deep hierarchical		0.96	0.68	0.60	0.61	0.83
[34]	DT-RFE		0.99	0.99	0.98	0.99	0.99

6. Open Issues and Research Directions

Although researchers have shown decent efforts in improving the security of CPS, they are still in their infancy and several open issues are remaining for further exploration. Challenges faced by CPS and corresponding research opportunities are highlighted here:

- Delay in encryption and decryption process cause network latency;
- Weak scheme for user authentication and lack of multi-factor verification in devices;
- Lack of firewall protection;
- Insufficient Intrusion detection techniques;
- Need of cipher algorithms for CPS security;
- Strong user authentication;
- Data availability and verified backups.

Some potential research opportunities are discussed as under:

- Many studies have been conducted for attack detection, but there is a need to consider real-time monitoring of CPS security. To employ real-time CPS security, the complexity of predictive models should be reduced to avoid data transmission delay.
- A resilient design of a CPS system for recovery after sensor attacks and software faults needs to be devised.
- Artificial intelligent-based models require sufficient data for training, so there is a need to generate a dataset for training and learning of malicious behaviors.

7. Conclusions

CPS combines physical and computing systems and becomes more vulnerable to security threats and cyber-physical attacks. These attacks disturb the functionality of CPS and systems crash in the real world. An increase in the connectivity of different components of CPS makes it complex and large and reduces the security of the system. To ensure the reliability and safety of the CPS model, it is inevitable to adopt novel techniques to increase the security level of CPS. This paper discusses CPS architecture as a layered model that provides a clear abstraction of complex components of CPS into three layers: the physical layer, network layer, and application layer. After that, different attacks on each layer are discussed, and some real-world attacks are also highlighted briefly. In addition, we provide a simple deep learning model for intrusion detection in a CPS. Finally, open issues and future directions for CPS are briefly discussed.

Author Contributions: Conceptualization, H.S. and K.A.; Formal analysis, K.A.; Funding acquisition, H.S.; Investigation, R.M.A. and S.S.; Methodology, K.A., S.S. and M.U.; Project administration, I.A. and R.M.A.; Resources, A.A.E. and H.K.; Software, S.S. and M.U.; Supervision, A.A.E.; Validation, A.A.E. and I.A.; Visualization, R.M.A. and H.K.; Writing—original draft, S.S. and M.U.; Writing—review & editing, I.A. and H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2022R192), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding is done by Abdullah Mohamed from Research Centre, Future University in Egypt, New Cairo, 11745, Egypt.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results

Abbreviations

The following abbreviations are used in this manuscript:

Acronyms	Definition
ANN	Artificial neural network
BS	Base station
CRL	Certificate revocation list
CPS	Cyber-physical system
CPU	Central processing unit
DDoS	Distributed denial-of-service
DNP	Distributed network protocol
DoS	Denial of service
DRAM	Distributed random access memory
DT	Decision tree
GPS	Global positions system
IoT	Internet of things
MCA	Multiple correspondence analysis
MitM	Man-in-the-middle
MLP	Multilayer perceptron
PCA	Principal component analysis
PDA	Pole dynamic attack
PSO	Particle swarm optimization
R2L	Remote to user
RF	Random forest
RFID	Radio frequency identification
RIS	Reconfigurable intelligent surfaces
SMOTE	Synthetic minority oversampling technique
SVM	Support vector machine
U2R	User to root
URL	Uniform resource locator
ZDA	Zero dynamics attack

References

1. Lee, J.; Bagheri, B.; Kao, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
2. Lee, J.; Lapira, E.; Yang, S.; Kao, A. Predictive manufacturing system-Trends of next-generation production systems. *Ifac Proc. Vol.* **2013**, *46*, 150–156. [CrossRef]
3. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360. [CrossRef]
4. Wehrmeister, M.A.; Freitas, E.P.; Pereira, C.E.; Wagner, F.R. An aspect-oriented approach for dealing with non-functional requirements in a model-driven development of distributed embedded real-time systems. In Proceedings of the 10th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC'07), Santorini, Greece, 7–9 May 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 428–432.
5. Kim, S.; Won, Y.; Park, I.H.; Eun, Y.; Park, K.J. Cyber-physical vulnerability analysis of communication-based train control. *IEEE Internet Things J.* **2019**, *6*, 6353–6362. [CrossRef]
6. Khalid, F.; Rehman, S.; Shafique, M. Overview of security for smart cyber-physical systems. In *Security of Cyber-Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 5–24.
7. Alladi, T.; Chamola, V.; Zeadally, S. Industrial control systems: Cyberattack trends and countermeasures. *Comput. Commun.* **2020**, *155*, 1–8. [CrossRef]
8. Rawat, D.B.; Bajracharya, C. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Process. Lett.* **2015**, *22*, 1652–1656. [CrossRef]
9. Shin, J.; Baek, Y.; Lee, J.; Lee, S. Cyber-physical attack detection and recovery based on RNN in automotive brake systems. *Appl. Sci.* **2018**, *9*, 82. [CrossRef]

10. Olowononi, F.O.; Rawat, D.B.; Liu, C. Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps. *IEEE Commun. Surv. Tutor.* **2020**, *23*, 524–552. [CrossRef]
11. Tidjon, L.N.; Frappier, M.; Mammar, A. Intrusion detection systems: A cross-domain overview. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3639–3681. [CrossRef]
12. Shojafar, M.; Taheri, R.; Pooranian, Z.; Javidan, R.; Miri, A.; Jararweh, Y. Automatic clustering of attacks in intrusion detection systems. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–8.
13. Mohammadi, S.; Namadchian, A. A new deep learning approach for anomaly base IDS using memetic classifier. *Int. J. Comput. Commun. Control* **2017**, *12*, 677–688. [CrossRef]
14. Marteau, P.F. Sequence covering for efficient host-based intrusion detection. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 994–1006. [CrossRef]
15. Hussain, J.; Lalmuanawma, S.; Chhakchhuak, L. A two-stage hybrid classification technique for network intrusion detection system. *Int. J. Comput. Intell. Syst.* **2016**, *9*, 863–875. [CrossRef]
16. Aburomman, A.A.; Reaz, M.B.I. Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection. In Proceedings of the 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, 3–5 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 636–640.
17. Yan, M.; Chen, Y.; Hu, X.; Cheng, D.; Chen, Y.; Du, J. Intrusion detection based on improved density peak clustering for imbalanced data on sensor-cloud systems. *J. Syst. Archit.* **2021**, *118*, 102212. [CrossRef]
18. Cho, E.M.; Perera, M.N.S. Efficient certificate management in blockchain based internet of vehicles. In Proceedings of the 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, VIC, Australia, 11–14 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 794–797.
19. Khan, S.; Zhu, L.; Yu, X.; Zhang, Z.; Rahim, M.A.; Khan, M.; Du, X.; Guizani, M. Accountable credential management system for vehicular communication. *Veh. Commun.* **2020**, *25*, 100279. [CrossRef]
20. George, S.A.; Jaekel, A.; Saini, I. Secure identity management framework for vehicular ad-hoc network using blockchain. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
21. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
22. Akashdeep; Manzoor, I.; Kumar, N. A feature reduced intrusion detection system using ANN classifier. *Expert Syst. Appl.* **2017**, *88*, 249–257. [CrossRef]
23. Musafer, H.; Abuzneid, A.; Faezipour, M.; Mahmood, A. An enhanced design of sparse autoencoder for latent features extraction based on trigonometric simplexes for network intrusion detection systems. *Electronics* **2020**, *9*, 259. [CrossRef]
24. Gu, J.; Wang, L.; Wang, H.; Wang, S. A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Comput. Secur.* **2019**, *86*, 53–62. [CrossRef]
25. Yao, H.; Fu, D.; Zhang, P.; Li, M.; Liu, Y. MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. *IEEE Internet Things J.* **2018**, *6*, 1949–1959. [CrossRef]
26. Jia, Y.; Wang, M.; Wang, Y. Network intrusion detection algorithm based on deep neural network. *IET Inf. Secur.* **2019**, *13*, 48–53. [CrossRef]
27. Mowla, N.I.; Tran, N.H.; Doh, I.; Chae, K. AFRL: Adaptive federated reinforcement learning for intelligent jamming defense in FANET. *J. Commun. Netw.* **2020**, *22*, 244–258. [CrossRef]
28. Virupakshar, K.B.; Asundi, M.; Channal, K.; Shettar, P.; Patil, S.; Narayan, D. Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. *Procedia Comput. Sci.* **2020**, *167*, 2297–2307. [CrossRef]
29. Alsirhani, A.; Sampalli, S.; Bodorik, P. DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 936–949. [CrossRef]
30. Aburomman, A.A.; Reaz, M.B.I. A novel SVM-kNN-PSO ensemble method for intrusion detection system. *Appl. Soft Comput.* **2016**, *38*, 360–372. [CrossRef]
31. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef]
32. Andresini, G.; Appice, A.; Di Mauro, N.; Loglisci, C.; Malerba, D. Multi-channel deep feature learning for intrusion detection. *IEEE Access* **2020**, *8*, 53346–53359. [CrossRef]
33. Jiang, K.; Wang, W.; Wang, A.; Wu, H. Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access* **2020**, *8*, 32464–32476. [CrossRef]
34. Lian, W.; Nie, G.; Jia, B.; Shi, D.; Fan, Q.; Liang, Y. An Intrusion Detection Method Based on Decision Tree-Recursive Feature Elimination in Ensemble Learning. *Math. Probl. Eng.* **2020**, *2020*, 2835023. [CrossRef]
35. Gaddam, N.; Kumar, G.S.A.; Somani, A.K. Securing physical processes against cyber attacks in cyber-physical systems. In Proceedings of the National Workshop for Research on Transportation Cyber-Physical. Systems: Automotive, Aviation, and Rail, Washington, DC, USA, 18–20 November 2008; pp. 1–3.
36. Lin, Z.; Niu, H.; An, K.; Wang, Y.; Zheng, G.; Chatzinotas, S.; Hu, Y. Refracting RIS aided hybrid satellite-terrestrial relay networks: Joint beamforming design and optimization. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 3717–3724. [CrossRef]

37. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, 1–4. [CrossRef]
38. Saqib, A.; Anwar, R.W.; Hussain, O.K.; Ahmad, M.; Ngadi, M.A.; Mohamad, M.M.; Malki, Z.; Noraini, C.; Jnr, B.A.; Nor, R.; et al. Cyber security for cyber physcial systems: A trust-based approach. *J. Theor. Appl. Inf. Technol.* **2015**, *71*, 144–152.
39. Khan, S.; Luo, F.; Zhang, Z.; Rahim, M.A.; Ahmad, M.; Wu, K. Survey on Issues and Recent Advances in Vehicular Public-key Infrastructure (VPKI). *IEEE Commun. Surv. Tutorials* **2022**, *24*, 1574–1601. [CrossRef]
40. Do Xuan, C.; Nguyen, H.D.; Nikolaevich, T.V. Malicious URL detection based on machine learning. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 148–153.
41. El-Sappagh, S.; Mohammed, A.S.; AlSheshtawy, T.A. Classification procedures for intrusion detection based on KDD CUP 99 data set. *Int. J. Netw. Secur. Appl. (IJNSA)* **2019**, *11*. [CrossRef]
42. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1–6.
43. Jia, B.; Ma, Y.; Huang, X.; Lin, Z.; Sun, Y. A novel real-time ddos attack detection mechanism based on MDRA algorithm in big data. *Math. Probl. Eng.* **2016**, *2016*, 1467051. [CrossRef]