Computers, Materials & Continua
DOI:10.32604/cmc.2020.012475
Article

Tech Science Press

Multilayer Self-Defense System to Protect Enterprise Cloud

Shailendra Mishra, Sunil Kumar Sharma* and Majed A. Alowaidi

College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
*Corresponding Author: Sunil Kumar Sharma. Email: s.sharma@mu.edu.sa
Received: 01 July 2020; Accepted: 19 August 2020

Abstract: A data breach can seriously impact organizational intellectual property, resources, time, and product value. The risk of system intrusion is augmented by the intrinsic openness of commonly utilized technologies like TCP/IP protocols. As TCP relies on IP addresses, an attacker may easily trace the IP address of the organization. Given that many organizations run the risk of data breach and cyber-attacks at a certain point, a repeatable and well-developed incident response framework is critical to shield them. Enterprise cloud possesses the challenges of security, lack of transparency, trust and loss of controls. Technology eases quickens the processing of information but holds numerous risks including hacking and confidentiality problems. The risk increases when the organization outsources the cloud storage services through the vendor and suffers from security breaches and need to create security systems to prevent data networks from being compromised. The business model also leads to insecurity issues which derail its popularity. An attack mitigation system is the best solution to protect online services from emerging cyber-attacks. This research focuses on cloud computing security, cyber threats, machine learning-based attack detection, and mitigation system. The proposed SDN-based multilayer machine learning-based self-defense system effectively detects and mitigates the cyber-attack and protects cloud-based enterprise solutions. The results show the accuracy of the proposed machine learning techniques and the effectiveness of attack detection and the mitigation system.

Keywords: Cybersecurity; cyber threats; cyber-attacks; attack mitigation system

1 Introduction

Cloud computing devices provide the platform needed to enhance and expand the world. Cloud computing continues to revolutionize the way people communicate and conduct their businesses. However, some security concerns continue to derail the expansion of the cloud-based systems into all parts of human life. Companies and even governments store enormous amounts of data in clouds for ease of use; the servers used in the processes are invaluable to many people [1]. Cloud technology separates the activities into a model termed as private, community, public and hybrid, depending on the preferences of the individual or company. Additionally, this technology can serve as software, platform, or infrastructure. The most significant derailment in the advancement of cloud computing is the insecurity of data [2,3].

The systems which operate on the web face many cyber-threats and attacks from malicious parties [4]. Denial of service attacks (DDoS) has been the most frequent type of security attack targeted by cybercriminals, thereby reducing network performance. DDoS attacks affect almost all aspects of information available on the systems, thereby proving to be one of the most dangerous and also leading to substantial financial losses to organizations. Such attacks severely compromise data security, completeness, and efficiency [5]. Criminals utilize innovative approaches for implementing attacks by leveraging evolving technologies like artificial intelligence, machine learning, and blockchain [6,7]. Advanced cyber-attacks take numerous forms, including Trojan, virus, spyware, spear phishing, rootkit, drive-by download, and malicious email attachments [8].

Due to rapid changes in the network and digital technologies, data security experts have to develop and maintain technological setups to protect the network [9]. Cloud computing services are widely utilized in all government establishments. Therefore, organizations are encountering cyber-attacks regularly. A large number of cyber-threats and their conduct are hard to comprehend and hence challenging to restrict during the early stages of the cyber-attacks [10]. The cybersecurity business is continuously innovating and utilizing artificial intelligence-driven methods and advanced machine learning to investigate network conduct and prevent rivals from winning. Hence, while threats linger and grow, the guards against them also keep developing simultaneously. It is significant to recall these historical events to combat the looming attacks [11].

The endpoint shield platforms have gradually emerged as the most efficient safety solutions for opposing a growing rate of worm attacks and possibly other associated malware. However, technological advances also boost cyber-attacks to grow [12]. Therefore, a fast and effective self-defense system is needed to protect the enterprise cloud.

This research aims to explore all probable ways for the earliest and successful detection and resolution of cyber-attacks. It is necessary to prevent delicate information from getting compromised and an effective machine learning-based system must be designed to detect and mitigate the attacks. Interpretive as well as quantitative techniques need to be used to evaluate the impact of attacks and propose an effective machine learning-based multilayer self-defense system for protecting cloud-based enterprise solutions.

In this research, we proposed and simulated a software defined networking (SDN) based multilayer self-defense system to detect and mitigate the DDoS attack and protect the enterprise cloud. Simulation results show that security solutions are fast and effective in mitigating the attacks. The support vector machine (SVM) technique has been used for the classification of network traffic. The performance of the SVM algorithm has been evaluated using sensitivity, specificity, accuracy, precision, recall, and F1 score, all in the range of 98.33 to 98.90%.

The remainder of this paper has been divided into seven sections. Section 1 outlines the introduction significance and objectives of the research. Section 2 gives the related work-study. Section 3 discusses the research methodology. Section 4 details the proposed SDN-based Multilayer Self-defense System, while the Experimental Setup is discussed in Section 5. The main findings are discussed in Section 6 the conclusion in Section 7.

2 Related Work

This section includes relevant works in cloud computing security, cyber threats, machine learning-based attack detection, and mitigation systems. The ideas of shared resources emerged from the need for centralized storage and operations. In cloud computing technology, information can be accessed from anywhere and anytime; it is also known as utility computing [13]. The idea of shared resources has continued to grow as a collection of interconnected computers; the proliferation of the Internet has led into a further

examination of the technology under scrutiny with a sharp focus on the communication sector and storage of information [14].

Cloud technology separates the activities into a model termed as private, community, public, and hybrid depending on the preferences of the individual or company. Additionally, the CC technology can serve as software, platform, or infrastructure. These models vary for the resources needed and the level of control given to the client. Many companies fear extensive use of cloud computing because of the implied security risk in the contemporary era. The information or systems that operate on the web face the vulnerability of attacks from malicious parties [15,16].

The increasing number of organizations using digital platforms attracts hackers because of the higher chances of profitability. The fact remains that no matter how secure an organization is in the physical activities and processes; they remain at risk when they use online services. The upsides of the cloud technology are immensely appealing to a point where risking the confidentiality of operations is a trade-off for a company looking forward to thriving in the current technological climate [17]. The Internet of Things (IoT) has developed from the concept of connection created by cloud computing and leads to the empowering of physical resources. The ability to connect one computer to the next, irrespective of distance and control processes, leads to the IoT [18,19]. The current technological environment accommodates the demands of cloud computing and IoT. The advancement in cloud computing and various applications of networking systems makes it easy to incorporate them into company operations, which means that insecurity affects many companies across the globe and needs further attention [20].

The major threats to information systems are ransomware, IoT vulnerabilities, social engineering, and the DDoS attack [21]. DDoS is a self-imposed mechanism to disrupt regular network traffic through the flooding of the network to the extent that the network or related resources slow down considerably or comes to a standstill. By using multiple under control computer systems as a source of attack traffic, DDoS attacks are very effective. The DDoS assault may appear as a bottleneck that is created by the bridge and blocks normal traffic at its desired location. In [22], researchers presented an algorithm to improve the efficiency and robustness of the low-rate DoS (DDoS) detection system by combining PSD-entropy and Support Vector Machine (SVM). Entropy application efficiently reduces the number of calculations, while SVM supports the proposed method by organizing the dataset around its most pertinent characteristics.

In [23], researchers used data from SNMP-MIB to detect patterns of DDoS attacks that may affect the network. To classify the dataset, they used three machine learning algorithms. In [24], researchers analyzed the latest tests of the identification system of DDoS attacks using a smart detection/defense system for DDoS attacks. The system used the results from the DDoS assault fitting and the usual traffic as feedback, post which they carried out the second stage of model design. A sniffer used to track IP packets in the network and detect malicious and natural traffic packets. Successful and accurate assessment results obtained using the SVM and C 4.5 supervised learning algorithm [25]. In [26], researchers created an SDN environment using Mininet and Floodlight and simulated the DDoS attack. For DDoS attack detection, SVM machine learning algorithms used. The computed accuracy of attack detection using SVM was 95.24%.

In [27], researchers used SVM machine learning algorithm and decision tree algorithms to detect the DoS attacks in a virtualized cloud environment and trained traditional SVM classifiers on data set using a 10-fold cross-validation model. Simulation results provide rational system parameters like the evaluation coefficient and demonstrate the efficiency of the proposed scheme. A performance measure used to evaluate the algorithms are false positive, false negative, attack detection and accuracy rate, average accuracy obtained using the proposed model being 97.6%.

In [28], researchers presented an algorithm to improve the efficiency and robustness of the DDoS detection system by combining PSD-entropy and SVM. They analyzed the dataset to detect attacks using Random Forest, KNN, and Support Vector Machine (SVM) algorithms to classify the network traffic as usual and malicious. Entropy application efficiently reduces the number of calculations, while SVM supports the proposed method by organizing the dataset around its most pertinent characteristics. Adjusting the two thresholds in the detection method can regulate the detection frequency and detection amount. The thresholds have an emphasis on reliability to achieve a higher detection rate. Experimental results show that the proposed model performs better in comparison to other algorithms, and the accuracy of the DDoS attack detection using SVM is (97%), which is higher than the other.

In [29,30], the authors discussed botnet attacks, which is dangerous to the security system. The DDoS assault may appear as a bottleneck that is created by the bridge and blocks regular traffic at its desired location. The malware compromises computers and other systems (such as IoT devices), transforming each one of them into a bot (or zombie). The hacker then remotely controls a group of bots group, called a botnet, by sending updated instructions to each bot. Because every bot is a legitimate Internet device, it can be challenging to separate attack traffic from regular traffic and endanger the security system. Five-tuple (source IPs per unit times per second, the standard deviation of incoming flow packets, speed of flow entities, and a ratio of an iterative and the total number of flows) characteristic values extracted and based on it the DDoS attack can be detected. Experimental results show that the average accuracy rate to detect DDoS using the SVM algorithm is 96.23% [29]. In [31], the authors proposed the dynamic pricing algorithm with malicious users (DPAMU) and unstable energy providers to get the ideal cost and forced necessity. Robust dynamic traffic partitioning schemes against malicious attacks have a better execution regarding parcel dissemination [32]. Android malware takes clients' private data and installs dangerous notice (promotion) libraries, which execute hazardous codes and harm the clients [33]. The improved SVM model has quicker computational time and higher prescient precision, and it can likewise abbreviate the preparation time and improve the presentation of SVM [34].

This study aims to explore all probable ways cyber-attacks could be resolved and detected before they compromise delicate information. The purpose of the attack detection and mitigation framework is to test and establish clear actions that a company can and must take to decrease the effect of a data breach from internal and external threats. Vulnerabilities and faults are results of a poorly developed system that could be easily abused by the intruders. For establishments with highly treasured data with a high-risk degree, a formal strategy is not enough, and they require to be more intelligence-driven and practical in threat-hunting abilities. Developing an attack mitigation framework has been a fundamental information safety tenant for numerous years and lasts to be a significant portion of an establishments' data security program. New protocols continue to push the necessity for a documented, reliable, robust and tested incident response program. Detecting malware continuously has been an inordinate challenge. Currently, with the growing amount of information available, there is a possibility to utilize more precise cataloging techniques. Attack detection and mitigation framework is the final line of stability during a data breach, shielding the company from additional harm and restoring operations, credibility or revenue most rapidly. Apart from direct outlays, a cyber-attack could have less obvious long-term consequences linked to reputation harm, especially for information breaches.

The most devastating effect of a cyber-attack happens to be lost productivity, possibly throughout the organization. A critical review is essential towards the development of a more inclusive attack detection and mitigation framework, as it provides insights into other works done, and this brings up existing gaps that the research can capitalize. Organizations and governments have tried to protect systems using the available technologies. However, attacks still happen, and therefore, there is a need for a multilayer self-defense system. Thus, numerous studies discussed in this paper have concentrated on exploring ways to

create secure systems that are inaccessible by attackers. However, in the modern world, there can never be a robust system that intruders cannot access.

3 Research Methodology

The research methodology used in this research is qualitative as well as quantitative. Research papers and multiple case studies helped in the investigation and gathering of information. Topics included cyber threats, cyber-attacks, cybersecurity, machine learning, and artificial intelligence-based attack detection and countermeasures in cloud-based technologies. After using the qualitative research methods, the quantitative ones came in the technical part of analyzing and investigating the data. The attacks simulated in a virtual network environment, a support vector machine (SVM) can be used to form a hyperplane in the high dimensional space to categorize network traffic as usual and malicious. Flows are installed in switches to mitigate malicious attack traffic. SVM classifier training parameters are the incoming number of source IPs per unit times per second (SSIP), the standard deviation of incoming flow packets (SDFP), speed of flow entities (SFE), and a ratio of an iterative and the total number of flows (RFIP) [26,27,35].

The trained SVM classifier classified the normal behavior or anomalous behavior from the network. The research design also involved a description of the machine learning-based fast and effective multilayer self-defense cyber-attack detection and mitigation system. The complete research process of the proposed work is shown in Fig. 1. The topology of the network was built using a MININET SDN emulator, and Floodlight was selected as the SDN Controller. Simulating the network and analyzing traffic were conducted under ordinary and attack conditions. Attacks generated and data were collected while the traffic was running between the gateway/host; in this step, training data was collected for traffic analysis from traffic classifiers, the data was cleaned with a machine learning approach (SVM), and training and testing sets were created to detect and mitigate the DDoS attack.

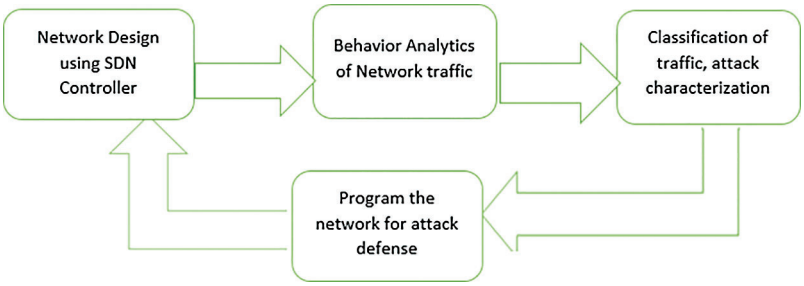

Figure 1: Research process

4 SDN-Based Multilayer Self-Defense System

Software-defined networking separates the control and logical plane (forwarding element). The forwarding devices send packet flows based on the flow policies that are programmed in these devices by the controllers. The abstracted control plane provides the flexibility to program essential network applications such as load balancer, routing algorithms, intrusion detection systems (IDS), and firewalls. The applications have effective decisions based on the overall network information provided by the control plane, and they can take the decisions from any location in the network. The control plane provides the ability to optimize the network workload, which provides high speed and intelligence of using the network resources [36]. Besides, the control plane provides practical and easy network management via network services. The network visualization of SDN supports cross tenant optimization

in cloud and data centers. A centralized network plane supports programmable network management and flexibility [37].

Application plane, which contains programs and is connected to the control plane by API, enables the network operators to configure and manage network resources; open standards-based protocols and applications simplify network design and operations. The SDN features attracted these significant companies to deploy this new technology. These features are centralized network control, open, programmable interfaces, switch management protocols, virtualized logical networks, third-party network applications and services, and centralized monitoring units. Open Networking Foundation (ONF) leads the movement of SDN [38]. A simplified view of software-defined networking (SDN) landscape is shown in Fig. 2; herein, the Software-defined datacenter is at the bottom, utilizing physical and virtual fabrics that overlay or underlay networks.

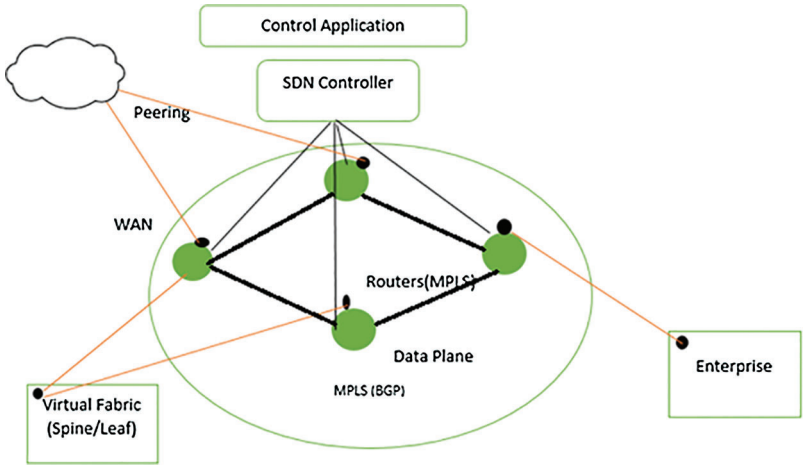

Figure 2: SDN landscape: command and control

In Fig. 2, the points marked at the data centers and the network are programmable flow enforcement points. These points are responsible for controlling cyber policy and cyber strategy. Point concedes that peering perimeter and edge networks are typically in the network. SDN controller is responsible for managing the critical networks' operations; this kind of control application can provide effective enforcement for the network. The self-defensive network is created by utilizing the defense flow, as shown in Fig. 3 a core network based on multiprotocol label switching MLPS(BGP), an enterprise network is connecting to SDN controllers and the defense flow running on top of the northbound controller API. Multiprotocol Label Switching (MPLS) is data forwarding technology that increases the speed and controls the flow of network traffic. With MPLS, data is directed through a path via labels instead of requiring complex lookups in a routing table at every stop.

Attacks are running and captured by the enterprise data center. Attack metadata information is captured and provided to the controller; the controller can pick up open flow, net flow information process, and provide that kind of statistical telemetry to the defense flow. The defense flow utilizes behavioral algorithms to detect attacks. In the case of attack detection, we move from peacetime into attack time and create a set of operations to address and mitigate the attack by using programmable change policies in the network such as traffic redirection IP and reputation activating access control list. An attack mitigation system is the best solution to protect online services from emerging cyber-attacks [39,40]. Once the threat of leaks saturation has been removed, the traffic is diverted back to the enterprise, and if necessary, attack traffic can be mitigated.

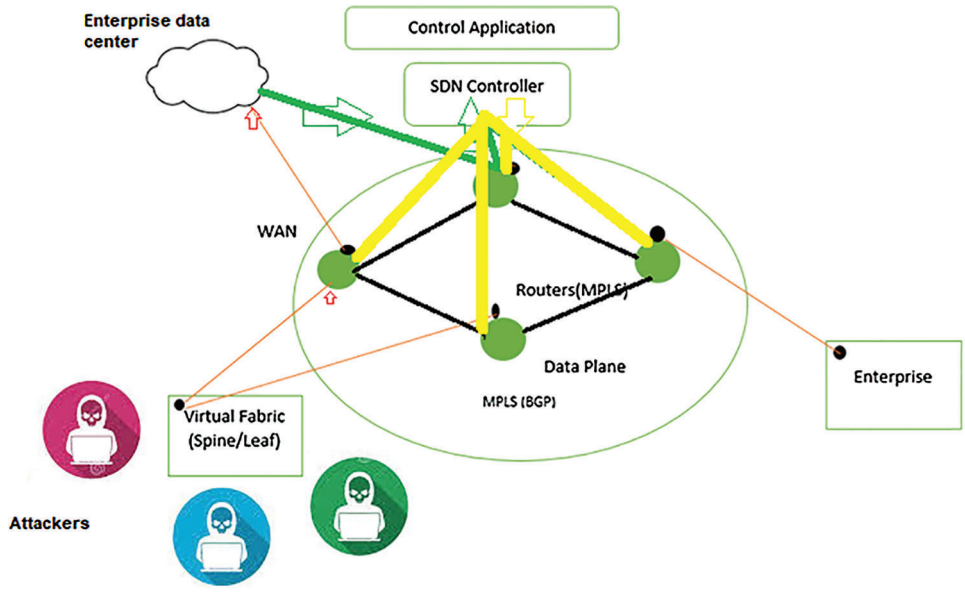

Figure 3: SDN multilayer self-defense flow system

5 Experimental Setup and Analysis

SDN emulator Mininet [41] that creates a virtual network used for the testbed runs on Ubuntu Linux. Floodlight [42] open flow SDN Controller for this testbed, the network topology is a tree topology, and S-FlowRT [43] used to analyze the network traffic. Floodlight offers web program-based design devices rather than charge line interfaces and is consequently more natural to understand. Floodlight can be tried with both physical and virtual OpenFlow-based switches. With this controller, the applications can be system vigilant, instead of customary systems where the system is application vigilant. Attacks are generated in a virtual simulated cloud network; network traffic is classified as usual and malicious traffic using SVM; flows are installed in the switches to mitigate malicious attack traffic. SVM seeks a hyperplane, which best splits the various classes. SVM trains data to find multiple support vectors, which define the hyperplane. The prediction only relies on the support vectors. The simulated network is shown in Fig. 4. The four switches (s1 to s4) have been connected to aggregation switch s1, which links all the other switches. Twenty hosts, five on each switch, are connected to s1 to s4. Switch six represents the deep packet inspection box in the network. Host 1 is the potential victim of the DDoS attack. The flow parameter of switch 1 is monitored every three seconds.

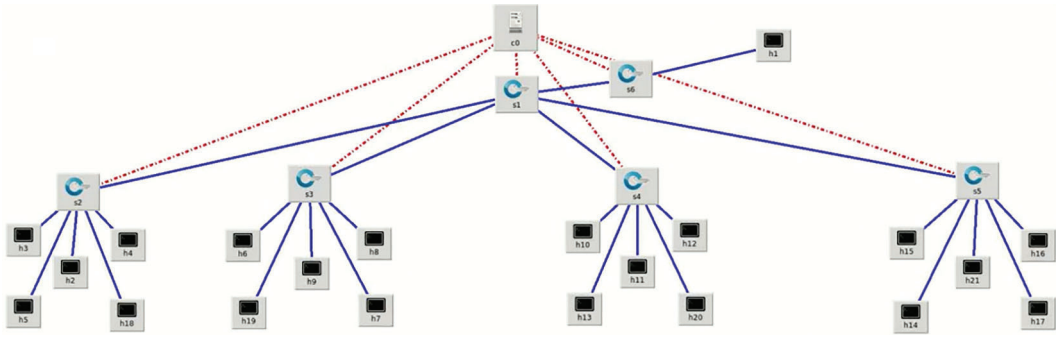

Figure 4: Simulated network (host 1 as a potential victim of the DDoS attack)

Two distinct datasets are computed for standard traffic simulation, making use of hping3, and simulating the traffic from 20 different hosts at random durations. Then the target host machine is pinged using hping3, with a random number of packet bytes and the host. DDoS attack is simulated using hping3 again. However, in this case, randomly spoofed high rate IPs are to be used with 10 packets for a second. To start regular traffic, pingall has to be checked first to confirm that all the nodes are connected. Fig. 5 shows the status of the network under the reasonable condition with zero percent dropped.

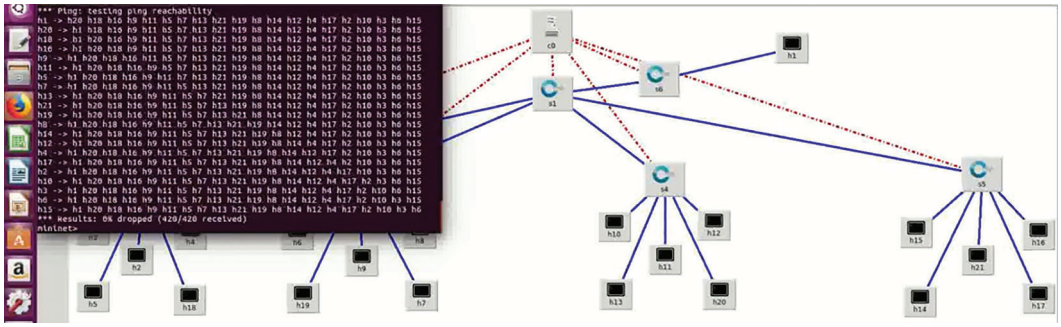

Figure 5: Network is up and working successfully under normal flow

Test.sh script is used to create normal flow while CollectE.sh script is used to extract the traffic feature. The extracted feature is used to train SVM classifiers to ensure classification of normal or anomalous behavior from the network. It shows that the network option on network operation is in normal status right now. The trained SVM classifier classifies the normal or anomalous behavior from the network. Also, Input-Output [IO] graph using the S-Flow network analyzer shows that operation is normal, which means data transfer rate is in the normal range, as shown in Fig. 6.

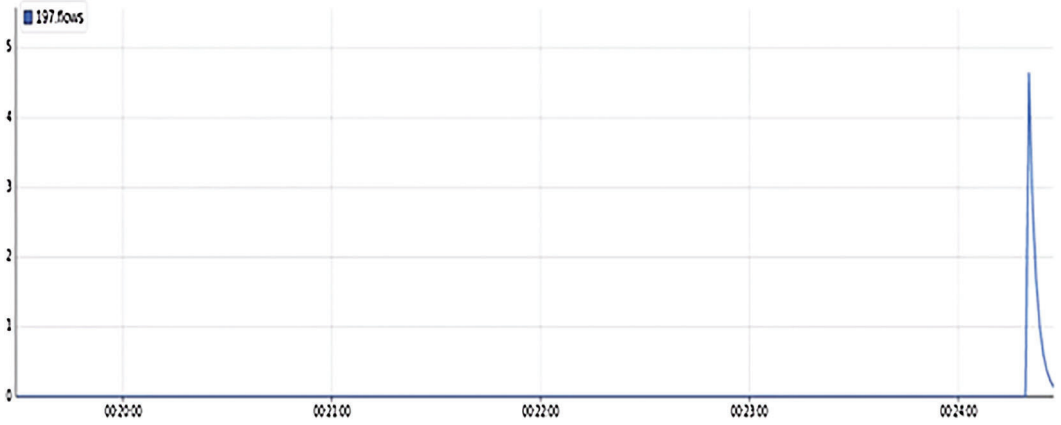

Figure 6: The input-output graph under normal operation

Fig. 7 shows the DDoS Attack from host h2 to host h1; the packet rate is about a hundred packet per second, with all the packets sent from random IPs; this indicates that the attack has started successfully. Once the DDoS attack runs successfully, host h6 is not able to ping host 1 (h6 ping h1), as shown in Fig. 7 (destination not reachable).

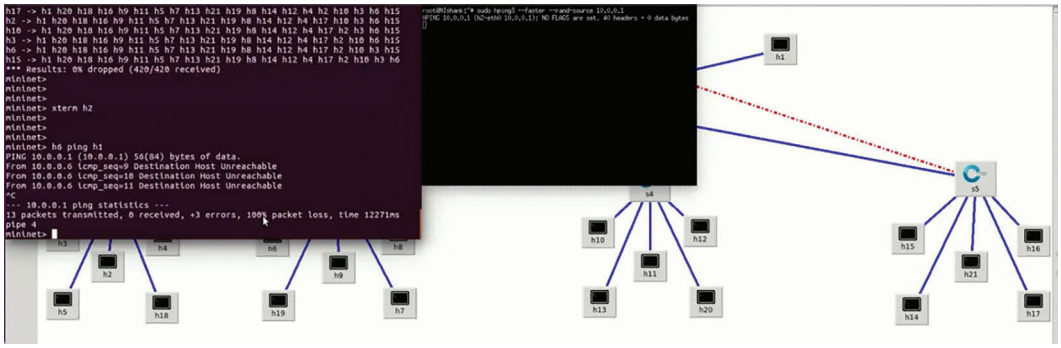

Figure 7: Network under DDoS attack

The script classifies the network traffic as anomalies and started adding the mitigating flows using deep packet inspection boxes to mitigate the attacks shown in Fig. 8. Two thousand data were collected during traffic analysis; the dataset contained five columns as a feature. Features of normal and malicious traffic are given in Tabs. 1 and 2, respectively. Under normal conditions, the standard deviation inflow of packets and inflow of bytes, as well as the speed of flow entries, is small, and the ratio of the iterative and total number of flows remains constant for all speeds of source IP(SSIP).

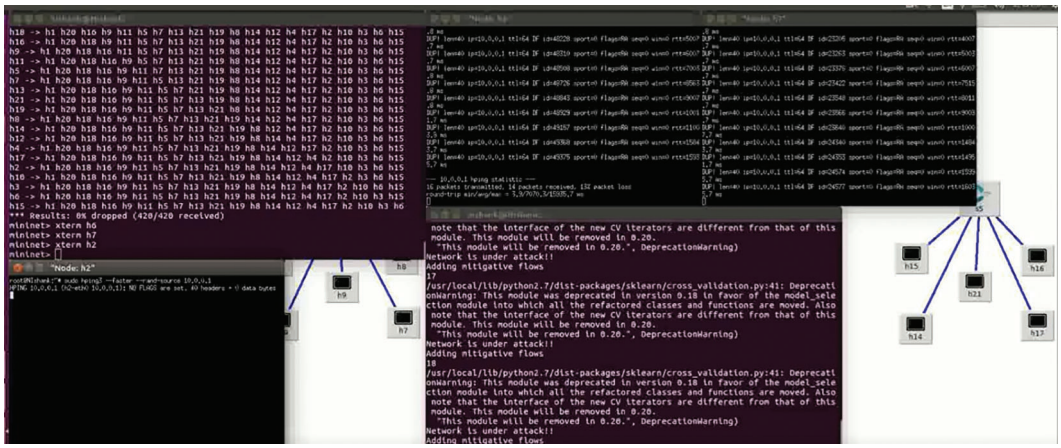

Figure 8: Network under normal flow after mitigation

Table 1: Features of normal traffic

SVM training parameters				
SSIP	**SDFP**	**SDFB**	**SFE**	**RFIP**
14	0.57	360.08	20	1
13	0.54	356.87	22	1
12	0.53	335.98	23	1
11	0.52	352.87	24	1
10	0.48	341.98	25	1

Table 2: Features of malicious traffic

SVM training parameters				
SSIP	**SDFP**	**SDFB**	**SFE**	**RFIP**
40	0.329	50.86	42	0.51
41	0.312	54.76	42	0.53
42	0.412	71.45	43	0.54
43	0.413	84.86	43	0.52

At the time of the attack, flooding takes place, and flow changes abruptly due to virtual IP and port number. SDFP and SDFB are small, and the flow of bytes (SFE) does not remain constant for all SSIP.

Fig. 9 shows that the network is again under normal flow after mitigation, which means the flows are successfully filtered out, and the normal flows are successfully being led to the network state, which was changed from normal to abnormal (attack) after 00.2450 sec. Under normal operation, traffic flow is normal to 00.240 sec.; flooding takes place from different hosts to h1 (victims) and the number of flows per second is increased, resulting in sudden spikes at 00.245 sec. represents the network is under attack. High spike shows the attack was occurring due to flooding of the packets from a malicious user, lower spikes imply that mitigation has been applied, and the network is again normal after 00.25.00 sec.

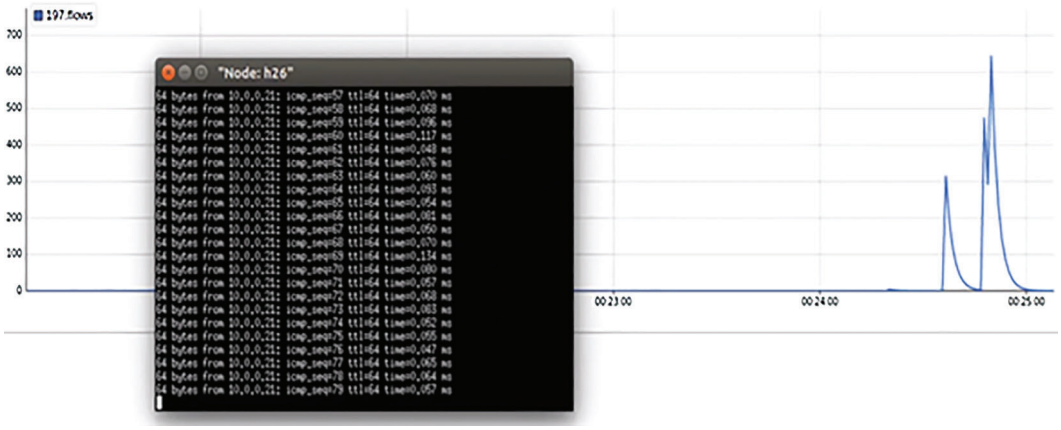

Figure 9: IO mitigation graph

The performance of the SVM algorithm was evaluated using sensitivity, specificity, and accuracy represented by Eqs. (1), (2) and (3). Accuracy is deemed to be perfect if it is in the range of 90% to 100% [26,27,30,37–41]. TP represents true positive cases when the SVM classifier detects malicious traffic correctly. At the same time, reject cases are represented by tr67ue negative (TN), and false positive represents the classifier classifying normal traffic as malicious; false negative represents the classifier classifying the malicious traffic as normal traffic.

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{1}$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{2}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{3}$$

Accuracy is not sufficient as a performance measures and other parameters like precision, recall, and F1 score are needed for exactness, completeness, and balance between precision and recall [43].

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP})} \tag{4}$$

It gives the exactness of the classifier; a low percentage predicts a large number of FP.

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

It gives the completeness of the classifier, and a low percentage predicts many FN.

$$F1\ Score = 2 * (Precision * Recall) \tag{6}$$

F1score represents the balance between precision and recall. The results indicate that the support vector machine (SVM) algorithm has high accuracy, sensitivity, and specificity. Also, the performance of the SVM classifier in terms of precision, recall, and F1 score is high, and it depicts the exactness and completeness of the classifier. The performance of the SVM algorithm is evaluated using sensitivity, specificity, accuracy, precision, recall, and F1 score, with all performance measures found to be in the range of 99.33% to 98.90%. Accuracy, sensitivity, specificity, precision, recall, and F1 scores have been computed, as shown in Tab. 3. These were compared with the results of previous works reported in [26–29] for validation (Fig. 10).

Table 3: Performance parameter of the SVM algorithm

SSIP	TP	FN	FP	TN	Sensitivity%	Specificity%	Accuracy%	Precision%	Recall%	F1 Score%
Normal Traffic	1356	19	10	615	98.62	98.40	98.55	99.27	98.62	98.94
TCP-SYN-Flood	1362	20	9	609	98.55	98.54	98.55	99.34	98.55	98.95
UDP-Flood	1299	23	8	670	98.26	98.82	98.45	99.39	98.26	98.82
Average					98.48	98.59	98.52	99.33	98.48	98.90

6 Discussion

Network attacks are the highest priority in the list of security issues faced by concurrent systems, including cloud. DDoS attacks affect almost all aspects of information available on the systems, thereby proving to be one of the most dangerous and leading to substantial financial losses for organizations. By applying the machine learning detection model, new data can quickly update the detection model. Machine learning techniques have found application across a broad spectrum of fields and have the potential to provide DDoS attack detection. The significant details of the experiment include the IO graph and DDoS detection, with simulation results depicting fast and speedy detection and mitigation scheme. Feature extraction of normal and malicious traffic and the mitigation of the cyber-attacks and the return to normalcy and performance evaluation of the proposed SVM machine learning algorithm used.

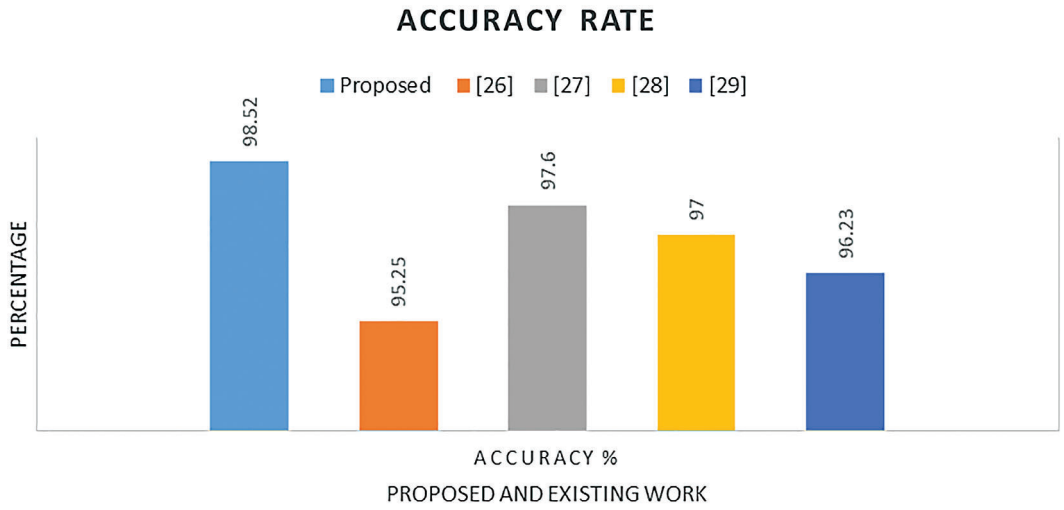

Figure 10: Comparison of the accuracy performance parameter of the proposed method with existing research

The performance of the proposed SVM algorithm was evaluated and all performance measures were found to be in the range of 97.37% to 98.79%. This was comparable with previous reports [26–29]. An attack mitigation system is the best solution to protect online services from emerging cyber-attacks. Also, mitigation starts immediately and automatically and does not require traffic diversion. However, 15% of the attacks that are handled by the third party turn into volumetric attacks that could threaten to saturate the Internet pipe of the protected enterprise. These attacks must be mitigated from the cloud since the defense messages share information about the attack before the traffic is diverted. The clean traffic is then sent back to the protected enterprise, and the volumetric attack is mitigated.

Once the threat of leaks saturation has been removed, the traffic is diverted back to the enterprise, and if necessary, attack traffic is mitigated on the premise. The combination of machine learning-based attack detection and mitigation system in the cloud provides the most extensive security coverage, shortest mitigation response time. The research also helps in increasing the effectiveness of security programs. It helps in establishing effective measures that enterprises may adopt to reduce data breach from both the external and internal threats. In many enterprises, most of the systems are not properly hardened, which leads to vulnerability and open to exploitation by hackers and malicious users. The proposed SDN Multilayer Self-defense flow system may act as a competitive tool that an organization may use to beat its competitors off the market.

7 Conclusions

A detailed study was conducted on the vulnerability assessment and identification of the weaknesses of the systems. It is important to study how these vulnerabilities leave loopholes for potential cyber threats to research how to plug the same. A fast and effective multilayer self-defense cyber-attack detection and mitigation system has been developed, simulated, and their impacts discussed. SVM was used for classification, regression and detection of DDoS attacks and rerouting of flows to an in-depth inspection box. The results indicate that the SVM algorithm has high accuracy in cyber-attacks and multilayer self-defense in cloud-based web applications. Security solutions are fast and effective in mitigating DDoS attacks. The performance of the SVM algorithm was evaluated using sensitivity, specificity and accuracy, which was found to be in the range of 97.37% to 98.79%. Future studies must focus on improved feature

coloration for including a more extensive range of attacks and use of real-world traffic because real-world traffic would help to simulate or understand a matrix of normal and malicious traffic.

Acknowledgement: The authors would like to express their heartfelt thanks to the editors and anonymous referees for their most valuable comments and constructive suggestions, which led to significant improvements in the earlier version of this manuscript.

Funding Statement: The authors would like to thank Deanship of Scientific Research at Majmaah University for supporting this work under Project No. RGP-2019-27.

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

References

[1] P. L. S. Kumari, "Big data: Challenges and solutions, " in *Security, Privacy, and Forensics Issues in Big Data*. IGI Global, pp. 24–65, 2020.

[2] S. Mishra, S. K. Sharma and M. A. Alowaidi, "Analysis of security issues of cloud-based web applications," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2020.

[3] M. S. Mahmoud, M. M. Hamdan and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber-attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.

[4] J. Srinivas, A. K. Das and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178–188, 2019.

[5] A. Cetinkaya, H. Ishii and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, pp. 210, 2010.

[6] S. Khezr, M. Moniruzzaman, A. Yassine and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, pp. 1736, 2019.

[7] T. Yigitcanlar, K. C. Desouza, L. Butler and F. Roozkhosh, "Contributions and risks of artificial intelligence in building smarter cities: Insights from a systematic review of the literature," *Energies*, vol. 13, no. 6, pp. 1473, 2020.

[8] F. T. Ngo, A. Agarwal, R. Govindu and C. MacDonald, "Malicious software threats, " in *Springer Nature Switzerland, The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. Holt, A. Bossler (eds.), Palgrave Macmillan, Cham, 2020.

[9] E. Oztemel and S. Gursev, "Literature review of industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, vol. 31, no. 1, pp. 127–182, 2020.

[10] J. Srinivas, A. K. Das and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems*, vol. 92, pp. 178–188, 2019.

[11] B. Shin and P. B. Lowry, "A review and theoretical explanation of the 'cyberthreat-intelligence capability' that needs to be fostered in information security practitioners and how this can be accomplished," *Computers & Security*, vol. 92, pp. 101761, 2020.

[12] A. Ahmad, J. Webb, K. C. Desouza and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," *Computers & Security*, vol. 86, pp. 402–418, 2019.

[13] M. Noshy, A. Ibrahim and H. A. Ali, "Optimization of live virtual machine migration in cloud computing: A survey and future directions," *Journal of Network & Computer Applications*, vol. 110, pp. 1–10, 2019.

[14] H. Shirvani and H. Vahdat-Nejad, "Storing shared documents that are customized by users in cloud computing," *Computing*, vol. 98, no. 11, pp. 1137–1151, 2016.

[15] W. Huang, A. Ganjali, B. H. Kim, S. Oh and D. Lie, "The state of public infrastructure-as-a-service cloud security," *ACM Computing Surveys*, vol. 47, no. 4, pp. 1–31, 2016.

[16] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell and E. Dubois, "Security transparency: The next frontier for security research in the cloud," *Journal of Cloud Computing*, vol. 4, no. 1, pp. 1–12, 2015.

[17] A. Arlott, T. Henike and K. Hölzle, "Digital entrepreneurship and value beyond: Why to not purely play online, " in *Digital Entrepreneurship*, R. Baierl, J. Behrens, A. Brem (eds.), Cham: Springer, pp. 1–22, 2019.

[18] A. Botta, W. De Donato, V. Persico and A. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[19] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," *Journal of Ambient Intelligence & Humanized Computing*, vol. 10, no. 10, pp. 4151–4166, 2019.

[20] F. Wu, L. Xu, S. Kumari and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2017.

[21] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3655–3682, 2017.

[22] D. Tang, L. Tang, W. Shi, S. Zhan and Q. Yang, "MF-CNN: A new approach for LDoS attack detection based on multi-feature fusion and CNN," *Mobile Networks & Applications*, pp. 1–18, 2020.

[23] A. Sahi, D. Lai, Y. Li and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[24] S. D. Kotey, E. T. Tchao and J. D. Gadze, "On distributed denial of service current defense schemes," *Technologies*, vol. 7, no. 1, pp. 19, 2019.

[25] A. H. Muna, N. Moustafa and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[26] J. Ye, X. Cheng, J. Zhu, L. Feng and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, vol. 2018, no. 4, pp. 1–8, 2018.

[27] A. Abusitta, M. Bellaiche and M. Dagenais, "An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment," *Journal of Cloud Computing*, vol. 7, no. 1, 2018.

[28] D. Li, C. Yu, Q. Zhou and J. Yu, "Using SVM to Detect DDoS Attack in SDN Network," *IOP Conference Series: Materials Science and Engineering*, vol. 466, 012003, 2018.

[29] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. Jaganathan and N. Marina, "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems," *Computational Intelligence*, vol. 44, no. 1, pp. 41, 2020.

[30] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini *et al.,* "Performance evaluation of Botnet DDoS attack detection using machine learning," *Evolutionary Intelligence*, vol. 13, no. 2, pp. 283–294, 2019.

[31] Q. Tang, K. Yang, D. Zhou, Y. Luo and F. Yu, "A real-time dynamic pricing algorithm for smart grid with unstable energy providers and malicious users," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 554–562, 2015.

[32] B. Xiong, K. Yang, J. Y. Zhao and K. Q. Li, "Robust dynamic network traffic partitioning against malicious attacks," *Journal of Network and Computer Applications*, vol. 87, pp. 20–31, 2017.

[33] X. Su, X. C. Liu, J. C. Lin, S. M. He, Z. J. Fu *et al.,* "De-cloaking malicious activities in smartphones using http flow mining," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 6, pp. 3230–3253, 2017.

[34] F. J. Kuang, S. Y. Zhang, Z. Jin and W. H. Xu, "A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection," *Soft Computing*, vol. 19, no. 5, pp. 1187–1199, 2015.

[35] H. Faris, M. A. Hassonah, A. Z. Ala'M, S. Mirjalili and I. Aljarah, "A multi-verse optimizer approach for feature selection and optimizing SVM parameters based on a robust system architecture," *Neural Computing and Applications*, vol. 30, no. 8, pp. 2355–2369, 2018.

[36] M. He, A. Varasteh and W. Kellerer, "Toward a flexible design of SDN dynamic control plane: An online optimization approach," *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1694–1708, 2019.

[37] Z. Guo, S. Zhang, W. Feng, W. Wu and J. Lan, "Exploring the role of paths for dynamic switch assignment in software-defined networks," *Future Generation Computer Systems*, vol. 107, pp. 238–246, 2020.

[38] Open Networking Foundation (ONF) 2020. [Online]. Available: https://www.opennetworking.org/.

[39] O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, "A Deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet of Things Journal*, 2020.

[40] G. Bunker, "Targeted cyber attacks: how to mitigate the increasing risk," *Network Security*, vol. 1, no. 1, pp. 17–19, 2020.

[41] Mininet 2020. [Online]. Available: http://mininet.org/.

[42] Floodlight 2020. [Online]. Available: https://github.com/floodlight/floodlight.

[43] SFlow- RT 2020. [Online]. Available: https://sflow-rt.com.