Investigating the Attacks on Software Defined Networks: Summary & Recommendations

Rizwan Iqbal[*], Rashid Hussain[*] and Sheeraz Arif[**]

[*] Faculty of Engineering Sciences and Technology, Hamdard University, Karachi, Pakistan
[**] Faculty of Information Technology, Salim Habib University, Karachi, Pakistan

Corresponding author: Rizwan Iqbal (rizwaniqbal88@gmail.com)

Abstract- SDN has significantly made conventional networks flexible. But as technology evolves, it is getting involved more and more in consumer's daily life, and the threat of cybercrime is making consumer life unsafe. The proposal is about providing security applications to the majority, i.e., the normal users who cannot afford expensive stand-alone firewalls nor do they have enough technical knowledge to upgrade and maintain them. The main purpose of this article is to review the work done on the enhanced security of SDN networks and develop a framework that will protect home user devices from attacks by implementing SDN based firewall. Proposed firewall design and made simulation model to present the results. Performance evaluation of the proposed solution on the benchmark problem set.

Index Terms- SDN, Firewall, Attacks on SDN Networks, Software Defines Home Networks

I. INTRODUCTION

SDN has accepted significant interest from the academic world, business, and government in recent years. SDN to build more active, adaptable, and flexible networks that are more responsive, cost-effective, efficient, speedily configured, and diverted as necessary. More SDN advantages for government networks taken in a Juniper survey are, Improved network performance and efficiency (26%), Simplified network operations (19%), Cost saving on operations (13%), Increased agility via automation and orchestration(13%), improved services (12%), enable greater security (9%) [1].

In conventional networks, both the control plane and the data plane elements were confined in proprietary; one or a combination of vendors was used to circulate an integrated code. In 2008, the OpenFlow standard was created and was recognized as the very first architecture of SDN. The OpenFlow protocol defines how the data and control plane components can be separated and communicated using the OpenFlow protocol. The OpenFlow standard was created and is managed by Open Network Foundation. In SDN architecture, packaged in a single integrated unit. More information about the state of the entire network can be provided to applications using this architecture compared to traditional network architecture.[2].

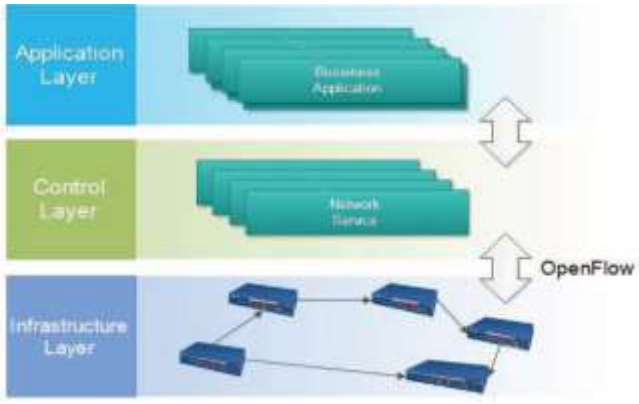

FIGURE 1. **Basic Architecture of SDN [3]**

The basic architecture of SDN is shown in Figure 1. network devices such as switches, hubs, and routers are located in the infrastructure layer. This layer is also called the data layer. Control layers collect one or more controllers' complete network knowledge to optimize flow management. Controllers connect the data layer by the northbound API and the application layer by the northbound API (Open flow). The application layer holds different routing, security, and business applications [3].

The security aids of SDN are more extensive as they transition to traditional networking protocols. Since SDN empowers uncomplicated collecting and studying of network traffic, it renders it undemanding to verify, identify and lessen network intimidation. Indeed, the technology can destroy over-dependence on manpower in spotting security pressures by responding to various threats as algorithms programmed to restrict and split traffic cantered on security threats like malware or network attacks [4]. The main purpose of this article is to review the work done on the enhanced security of SDN networks and develop a framework that will protect home user devices from attacks by implementing SDN based firewall. Proposed firewall design and made simulation model to present the results. Performance evaluation of the proposed solution on the benchmark problem set.

Section II is based on a literature review; Section III delineates the problem statement, section IV objectives of the research, section V describes the methodology, and section VI is based on the conclusion.

II. LITERATURE REVIEW

A literature review is needed to explore the selected area of research. For this reason, mentioned papers have been studied to find the problems for specific topics, i.e., SDN. According to this literature review, researchers work on different areas of SDN in different eras. Some authors mention the history of SDN, recent advancements, and future directions in their research papers. Some authors discuss security challenges and opportunities. Some identify threats and attacks of SDN-based home networks and provide security by making a firewall using different techniques.

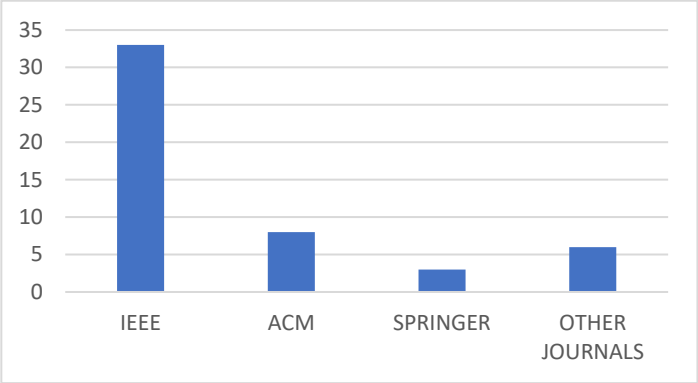

FIGURE 2. **Publication-wise Number of Paper**

Figure 2 shows that the initial search resulted in 50 articles: 33 from IEEE Xplore, eight from the ACM library, three from springer, and six from other journals from 2011 to 2020.

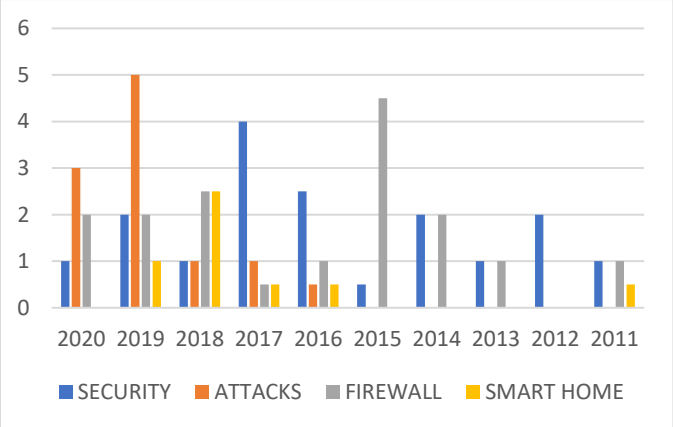

FIGURE 3. **Topic and Year-wise Number of Paper**

Figure 3 shows that in 2020, researchers working on Secure methods of Firewall Directions in Software-Defined Networks will also deploy different technologies in SDN, [5], [6], [7], [8], SDN-Enabled different strategies for DDOS (distributed denial of service) attacks on the internet of things as implemented in the industry [9], make algorithms to detect different types of attacks [10].

The research in 2019 on artificial intelligence (AI) and fuzzy rule interpolation (FRI) based detectors to protect cyber security and used different tools for data analysis [11], [12], [13], [14].

Survey on 5G Technologies Possible Solutions, Current Developments and Upcoming Directions [15], Comparative Analysis of Data Traffic for SDN-Based Firewall [16] and Different Attacks on SDN and Methods to Mitigate [17]. Make standalone and cooperative stateful firewall [18], Survey on cyber security to protect home network [19], [20].

The study in 2018 was based on a survey of SDN-based Secure Smart Home Network Architecture for Internet of Things [21], [22], [23], Challenges and Implementation of SDN-based Firewall using different techniques [24], [25], used other tools for Data Management [26] to Protect Home User Devices[27].

In 2017 researchers worked on Security Challenges and Opportunities of Software-Defined Networking for home users [1], [4], [28], [29], [30], and constructed a mathematical model for detecting inconsistencies caused by a port scan attack [31].

In the 2016 era, Enhanced SDN Security using Firewall in a Distributed scenario and wireless network [3], [32], [33],[34], [35] improve the detection rate of stealth port scan attacks using modified rules by port scan tools [36].

In 2015 Outsourcing Coordination and Management of Home Wireless Access Points through an Open API [37], [38], [39], [40], [41].

In 2014 researchers provided an overview of programmable networks and, in this context, examined the emerging field of Software-Defined Networking (SDN) [2], [42], [43], [44].

In 2013, researchers provided solutions against challenges in SDN like network performance, scalability, security, interoperability, and virtual security services [45], [46].

In 2012, scholars worked on the effective security mechanism of the control plane by using an open flow protocol [47], [48].

In 2011, Home Network Management Interfaces with SDN controller and protocols and traffic anomaly detection using software-defined networking [49], [50].

The categorization of the research in SDN has four major areas: Security, attacks, firewall, and smart home; all the research papers are related to these four areas. Most of the articles focus on an area of research, while some research paper discusses more than one area.

To identify the research gap, 45 research articles have been studied; all papers mainly discuss the SDN environment, history of SDN and their security, limitations of security mechanism, challenges of SDN security, implementation of SDN in the home network, attacks on SDN based home network mainly port scan attack their types, categorization, techniques, and tools then how firewall implement in SDN environment to secure network using artificial intelligence (AI) and fuzzy rule interpolation (FRI) and types of the firewall with their controllers. In this literature review, some papers are simulation-based, some are experimental, some are analytical, and some papers are survey-based. A technically unaware audience of the home user using SDN can address the security issue. Attackers find out the different ways to demolish network security and continuously scan vulnerable devices of IoT. Researchers are working on exploring different types of attacks, including the horizontal port scan. To provide a secure network, a firewall performs a major role and protecting the network from threats and attacks.

TABLE I
OVERVIEW OF PORTSCANNING

POSSIBLE ATTACKS [11]			
Worm Attack	Botnet Attack	Information Retrieval Attack	Denial of Service Attack
• Internet worm • Email worm • File sharing worm	• Internet relay chat botnet • Peer-to-peer botnet • HTTP botnet	• Port scans • SSH brute force attack	• Smurf attack • TCP SYN attack • UDP attacks
PORT SCAN [12]			
The port scan method is "To scan open ports and break the network security" using different methods.			
TYPES OF PORT SCAN [13]			
Horizontal	Vertical	Block	
The scan is performed against a group of IPs for a single port.	A single IP being scanned for multiple ports	Combination of both vertical and horizontal scan	
CHARACTERIZING PORT SCANS [10]			
Source & Destination Ports	Vertical & Horizontal Scans	Scan Validation	IP Version	The Magnitude of Target Hosts and Scans Probes	Source IP Subnet and Geolocation
HORIZONTAL SCANS [27]			
A horizontal scan scans a single port across multiple IP addresses.			
PORT SCANNING TECHNIQUE [14]			
TCP SYN Scanning	Indirect Scanning	Decoy Scanning	Stealth Scanning
Scanning the selected IP SYN segment's selected port is transmitted and performs the same function as an active open.	This type of scanning used the IP address of another host to be masking the actual scanning system.	In decoy scanning, some packets are delivered to the same target.	Combining other scanning techniques like FIN, Xmas, Null, and Ack is to make stealth scanning.
PORT SCANNING TOOLS [14]			
Snort	Wireshark	MONOSEK	NMAP
Snort is a network intrusion outline that monitors to the network traffic in real-time.	Wireshark is an analyzer for packets and is also used for troubleshooting the network.	MONOSEK is used for Network Packet Processing and Network Session Analysis.	NMAP is an open-source scanner developed by Fyodor and is one of the most popular port scanners for Unix/Linux machines.

Table I is designed from selected research papers in the literature review. It shows the general layout of possible attacks, their types, Port scan, characterizing port scans, port scanning techniques, and some tools used in port scanning.

Possible attacks and their types are defined in the paper [11]. In this paper, the author discusses four types of attacks used to damage the network: worm attack, botnet attack, information retrieval attack, and denial of service attack. Worm attack is further divided into three types, i.e., Internet worm, Email worm, and File sharing worm. Botnet attacks are divided into three types, i.e., Internet relay chat botnet, Peer to peer botnet, and HTTP botnet. Information Retrieval Attack is divided into two parts, i.e., Port Scan and SSH brute force attack and Denial of Service attack can be further divided into three types, i.e., Smurf attack, TCP SYN attack, and UDP attack.

A Port scan attack uses different methods to scan open ports to break network security [12]. Port scans have three types: Horizontal port scan, Vertical port scan, and Block port scan. The attacker scans a single port of multiple IPs in a horizontal port scan. In a vertical port scan, the attacker scans multiple ports of single IP. The third type of Port scan is produced by combining horizontal and vertical port scans, i.e., Block port scan [13].

Port scan is characterized by six different parts: (i). Source & Destination Ports, (ii). Vertical & Horizontal Scans, (iii). Scan Validation, (iv). IP Version, (v). The magnitude of Target Hosts & Scans Probes and (vi). Source IP Subnet and Geolocation [10]. A Horizontal scan is used for a single port scan across more than one IP address [27]. Port scan attacks have different techniques for scanning, including TCP SYN Scanning, Indirect Scanning, Decoy Scanning, and Stealth Scanning [14].

- *TCP SYN Scanning:* scanning the selected IP SYN segment's selected port is transmitted and performs the same function as an active open.
- *Indirect Scanning:* this type of scanning uses the IP address of another host to mask the actual scanning system.
- *Decoy Scanning:* Some packets are delivered to the same target in decoy scanning.
- *Stealth Scanning:* combining other scanning techniques like FIN, Xmas, Null, and Ack to make stealth scanning.

Different tools for port scanning are discussed in [14]. SNORT, Wireshark, MONOSEK, and NMAP. SNORT is a network intervention exposure that monitors the network traffic in real-time. Wireshark is an analyzer for packets and is also used for troubleshooting the network. MONOSEK is used for Network Packet Processing and Network Session Analysis. NMAP stands for "Network Map." This open-source scanner, developed by Fyodor, is one of the most popular port scanners for Unix/Linux machines.

TABLE II
CATEGORIZATION OF THE SECURITY ISSUES ASSOCIATED WITH THE SDN FRAMEWORK BY LAYER/INTERFACE AFFECTED

SECURITY CONCERNS/ ATTACKS	EXAMPLE	APPLICATION LAYER	APPLICATION-CONTROL INTERFACE	CONTROL LAYER	CONTROL-DATA INTERFACE	DATA LAYER
Unauthorized Access	Unauthorized Controller Access			✓	✓	✓
	Unauthenticated Application	✓	✓	✓		
Data Leakage	Flow Rule Discovery (Side Channel Attack on Input Buffer)					✓
	Forwarding Policy Discovery (Packet Processing Timing Analysis)					✓
Data Modification	Flow Rule Modification to Modify Packets			✓	✓	✓
Malicious Applications	Fraudulent Rule Insertion	✓	✓	✓		
	Controller Hijacking			✓	✓	✓
Denial of Service	Controller-Switch Communication Flood			✓	✓	✓
	Switch Flow Table Flooding					✓
Configuration Issues	Lack of TLS (or other Authentication Technique) Adoption			✓	✓	✓
	Policy Enforcement	✓	✓	✓		

Table II shows the different security concerns or attacks concerning the SDN layer or interfaces with their examples.

1) Unauthorized Access: This attack affects the control layer, control-data interface, and data layer by unauthorized

controller access and involves the application layer by unauthenticated applications.

2) ***Data Leakage:*** The data layer affects this security concern. Side channel attacks and packet process time analysis are examples of this concern.
3) ***Data Modification:*** This attack affects the control layer, control-data interface, and data layer by inserting some modified flow rules on network devices.
4) ***Malicious Applications:*** This security concern is affected by the application layer, application control interface, and control layer by integrating malicious applications and SDN architecture.
5) ***Denial of Services:*** This attack affects the control layer, control-data interface, and data layer by flooding the packets using the controller.
6) ***Configuration Issues:*** This security concern is affected the application layer, application control interface, and control layer by compromising TLS (transport layer security).[35]

Table II shows that security concerns and attacks can impact all layers of the architecture.

TABLE III
COMPARISON OF SDN-BASED FIREWALLS

Firewall	Controller	Centralized Flow Tracking	Centralized Conflict Detection	Multi-Tenant Support	Auto Priority Handling	Violation Resolution	Concurrent Updates	Stateful
Ethane	Ethane	X	✓	X	X	X	X	X
Fort-NOX	NOX	X	✓	X	✓	X	X	X
Flow Guard	Flood Light	✓	✓	X	X	✓	X	X
FW over SDN	POX	X	✓	X	X	X	X	X
SE Flood Light	Flood Light	X	✓	X	✓	✓	X	X
Auth Flow	POX	X	✓	X	X	X	X	X
Reactive Stateful SW	RYU	X	✓	X	X	X	X	✓
Fortress Stateful	Flow Level State Transition (FAST) Supported	X	✓	X	X	X	X	✓

Table III compares different firewalls with their controller and individual potential. The potential of the firewalls is explained as follows.

1) ***Centralized Flow Tracking:*** For packets on the network, some rules are installed from source to destination.
2) ***Centralized Conflict Detection:*** When a new policy or rule is being added to the existing system, the installed firewall should provide a conflict resolution on this violation.
3) ***Multi-Tenant Support:*** The controller of the SDN has a centralized view of the whole network, so an SDN-based firewall should generate a difference between the address ranges of the entire network.
4) ***Auto Priority Handling:*** An intelligent firewall should automatically process security policies in the network and set the priority from different sources.
5) ***Violation Resolution:*** The firewall imposes a rule violation when the rule violates an SDN.
6) ***Concurrent Updates:*** Concurrent updates face a problem in the enterprise network because multiple pipelines update the same configuration data stores. Stateful: Maintaining the states of active connections gives a definite advantage to the reliability of a firewall [26].

The Explanation of the firewalls and their specified controller, which are given in the table, is as follows.

1) ***Ethane*** firewall enables Ethane controller to permit network administrator to define one network policy and apply it to every device.
2) ***FortNOX*** firewall enables NOX controller to avoid unauthorized access to control plane and users end.
3) ***Flow Guard*** firewall enables Floodlight to detect flow policy violations.
4) ***FW over SDN*** firewall enable POX open flow-based controller to handle redundancy of hardware-based firewall.
5) ***SE-Floodlight*** firewall enables Floodlight controller, an extension of FortNOX.
6) ***Auth Flow*** firewall enables POX open flow-based controller to apply the security policies in the data link layer to handle address spoofing and communication overhead.
7) ***Reactive Stateful SW*** firewall enables the RYU controller to provide security on the state of active connections in the network [26].
8) Flow-level State Transition (FAST) is a stateful application on the data plane. It allows memorizing the state transition of each flow autonomously [18].

III. PROBLEM STATEMENT

1. The world is shifting towards SDN due to its flexible, cost-efficient infrastructure.
2. In SDN, one can operate and perform several network management tasks using APIs. One can design APIs for security, which can assist the need for safety for numerous security issues.
3. A technically unaware audience of home users using SDN can address security issues.
4. SDN devices are very involved in our personal and public systems. But SDN devices are the easy target for attackers too.
5. In the SDN architecture, the controller is a target for threats, especially when open to unauthorized access.
6. Attacks on the controller can cause serious damage to the network, as it is responsible for controlling the entire network. Moreover, an attacker could impersonate a controller and carry out malicious deeds.
7. Smart devices used in smart home promise to make our lives easier, but they also raise security and privacy concerns.

Key challenges posed by SDN, namely:

- Scalability
- Flexibility and Performance
- Security
- Interoperability

IV. OBJECTIVES

The main objectives of this research are:

1. A comprehensive literature review of SDN Environment, SDN-based home networks, devices, and security.

2. To analyze Different attacks on SDN and SDN-based home networks.
3. To understand different approaches to Attacks, mainly horizontal port scans.
4. Evaluate the malware detection, authentication, and firewalling for SDN infrastructure to secure home network attached devices.
5. Protect the home user from horizontal port scan attacks by implementing a firewall on the SDN controller.
6. To understand FleXight, Python, Linux, Open vSwitch, Mininet, Virtual Box, and MATLAB to implement the proposed framework.
7. Implement a framework to prevent home network devices against port scan attacks with the proposed firewall.

V. METHODOLOGY

To design a simulation model and present the results. Compare the results with state-of-the-art technologies provided in the literature.

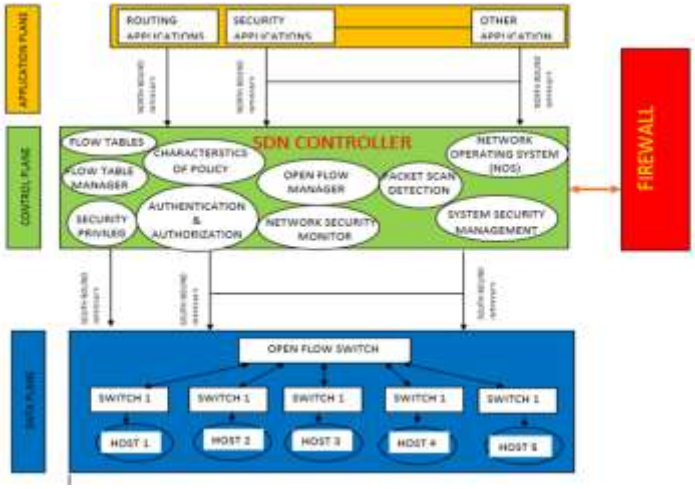

FIGURE 4. **SDN functional structure with firewall**

Figure 4 shows the SDN functional structure with a firewall. The Figure shows three planes of SDN: Application plane, Control plane, and Data plane.

The Application plane is where unlimited innovative applications can be formed by leveraging every part of the network's information about different network parameters like network state, network topology, network statistics, etc. The applications can be of distinct sorts and facilitate a network in various aspects and regions, such as network automation, configuration, monitoring, security, etc. Such SDN applications can deliver several end-to-end resolutions for real-world data centers and enterprise networks.

The Control plane controls the network infrastructure. It is the level of the control plane, the layer where intellectual judgment in SDN controllers manages. Every network vendor works in this area to develop its product of SDN frameworks or Controllers. A bunch of business logic is coded in this layer; the reason is transcribed in the controller to sustain and retrieve numerous forms of network info, topology details, network state particulars, etc. As we know, SDN controllers are used to managing the systems, so they ought to assist the control logic for the real-world network cases routing, switching, L2 VPN, firewall, security rules, DNS, L3 VPN, clustering, and DHCP. Suppliers and open-source societies are in work on applying all such use cases in their SDN controllers. Once employed, the services distribute their APIs, making administration and implementation easy for network administrators, who can then organize, monitor, and control the underlying network by using these apps on top of controllers. The Control layer resides in the middle and is exposed to two different interfaces.

North Bound Interface: The interface enables communication with the upper, Application layer and is realized via REST APIs of SDN in general.

South Bound Interface: The communication with the lower infrastructure layer is destined through it; generally, the interfaces are realized via southbound protocols like OpenFlow.

The Data planes are composed of different networking equipment. The equipment is combined to form an underlying network that forwards the network traffic. This layer usually consists of routers and switches in the data center; it is generally a physical layer on which the network virtualization is placed through the control layer.

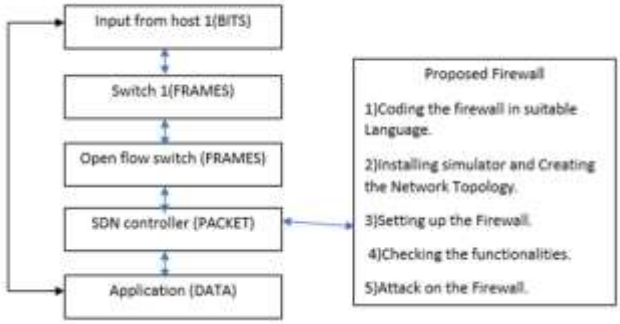

FIGURE 5. **Flow chart of the proposed system**

Method of the proposed system described as first take input from any smart device; data go through the switch in the form of frames to open flow switch which is connected to SDN controller, controller attached to the proposed firewall so, after analyzing legal data part of that data go to the application layer and received**.**

VI. CONCLUSION

This article reviews the work done on the enhanced security of SDN networks. It develops a framework that will protect home user devices from attacks by implementing SDN based firewall. In the SDN architecture, the controller is a target for threats, especially when open to unauthorized access. Attacks on the controller can cause serious damage to the network, as it is responsible for controlling the entire network. Moreover, an attacker could impersonate a controller and carry out malicious deeds. Proposed firewall design and made simulation model to present the results. Performance evaluation of the proposed solution on the benchmark problem set.

REFERENCES

[1] J. H. Cox et al., "*Advancing software-defined networks: A survey*," IEEE Access, vol. 5, pp. 25487–25526, 2017.

[2] B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, "*A survey of software-defined networking: Past, present, and future of programmable networks*," IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014.

[3] D. Satasiya, R. Raviya, and H. Kumar, "*Enhanced SDN security using a firewall in a distributed scenario*," Proc. 2016 Int. Conf. Adv. Commun. Control Comput. Technol. ICACCCT 2016, no. 978, pp. 588–592, 2017.

[4] M. C. Dacier, "*Security Challenges and Opportunities of Software Define Networking",* IEEE Security & Privacy 2017.

[5] S. Kim, S. Yoon, J. Narantuya, and H. Lim, "*Secure Collecting, Optimizing and Deploying of Firewall Rules in Software-Defined Networks*," IEEE Access, vol. 8, pp. 15166–15177, 2020.

[6] S. Ali, M. K. Alvi, S. Faizullah, M. A. Khan, A. Alshanqiti, and I. Khan, "*Detecting DDoS Attack on SDN Due to Vulnerabilities in OpenFlow*. (arXiv:1912.12221v3 [cs.CR] UPDATED)."

[7] T. Alharbi, "*Deployment of blockchain technology in software-defined networks: A survey*," IEEE Access, vol. 8, pp. 9146–9156, 2020.

[8] Y. Kim, "*Formal Verification of SDN-Based Firewalls by Using TLA +*", IEEE Access, vol. 8, pp. 52100–52112, 2020.

[9] M. Du and K. Wang, "*An SDN-Enabled pseudo-honeypot strategy for distributed denial of service attacks in the industrial internet of things*", IEEE Trans. Ind. Informatics, vol. 16, no. 1, pp. 648–657, 2020.

[10] S. Haas, F. Wilkens, and M. Fischer, "*Scan Correlation -- Revealing distributed scan campaigns*," 2020 IEEE.

[11] J. Fesl,V. Gokhale, J. Cehak, M. Feslova, M.Lejtnar and J.Janecek "*Towards HPC-Based Autonomous Cyber Security System*," 2019 IEEE.

[12] M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, "*Detecting Slow Port Scan Using Fuzzy Rule Interpolation,*" 2019 2nd Int. Conf. New Trends Comput. Sci. ICTCS 2019 - Proc., pp. 0–5, 2019 IEEE.

[13] M. S. Kumar, J. Ben-Othman, K. G. Srinivasagan, and G. U. Krishnan, "*Artificial Intelligence Managed Network Defense System against Port Scanning Outbreaks*," Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019, 2019 IEEE.

[14] R. Banu, T. Jyothi, M. Amulya, K. N. Anju, A. Raju, and S. N. Kashyap, "*MONOSEK - A network packet processing system for analysis detection of TCP xmas attack using pattern analysis*," 2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019, no. Iciccs, pp. 952–956, 2019 IEEE.

[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "*A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*," IEEE Commun. Surv. Tutorials, no. JULY, pp. 1–1, 2019.

[16] M. F. Monir and S. Akhter, "*Comparative analysis of UDP traffic with and without SDN-based firewall*," 1st Int. Conf. Robot. Electr. Signal Process. Tech. ICREST 2019, pp. 85–90, IEEE 2019.

[17] M. D. Hatagundi and H. V. Kumaraswamy, "*A comprehensive survey on different attacks on SDN and approaches to mitigate,"* Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019, no. Iccmc, pp. 624–627, IEEE 2019.

[18] M. Caprolu, S. Raponi, and R. Di Pietro, *"FORTRESS: An efficient and distributed firewall for stateful data plane SDN*," Secur. Commun. Networks, vol. 2019, no. iii, 2019.

[19] J. C. Sapalo Sicato, P. K. Sharma, V. Loia, and J. H. Park, "*VPNFilter Malware Analysis on Cyber Threat in Smart Home Network*," Appl. Sci., vol. 9, no. 13, p. 2763, 2019.

[20] E. Anthi, L. Williams, M. Słowi, G. Theodorakopoulos, and P. Burnap, "*A Supervised Intrusion Detection System for Smart Home IoT Devices*," vol. 6, no. 5, pp. 9042–9053, 2019 IEEE.

[21] R. Amin, M. Reisslein, and N. Shah, "*Hybrid SDN networks: A survey of existing approaches*," IEEE Commun. Surv. Tutorials, vol. 20, no. 4, pp. 3259–3306, 2018.

[22] P. K. Sharma, J. H. Park, Y. S. Jeong, and J. H. Park, "*SHSec: SDN based Secure Smart Home Network Architecture for Internet of Things*," Mob. Networks Appl., vol. 24, no. 3, pp. 913–924, 2018.

[23] A. M. Alshnta, M. F. Abdollah, and A. Al-Haiqi, *"SDN in the home: A survey of home network solutions using Software Defined Networking,"* Cogent Eng., vol. 5, no. 1, pp. 1–40, 2018.

[24] P. Krongbaramee and Y. Somchit, *"Implementation of SDN Stateful Firewall on Data Plane using Open vSwitch,"* Proceeding 2018 15th Int. Jt. Conf. Comput. Sci. Softw. Eng. JCSSE 2018, pp. 1–5, IEEE 2018.

[25] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Li, "*SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks*," IEEE Access, vol. 6, pp. 8292–8301, 2018.

[26] V. H. Dixit, S. Kyung, Z. Zhao, A. Doupé, Y.

Shoshitaishvili, and G. J. Ahn, *"Challenges and preparedness of SDN-based firewalls,"* SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018, vol. 2018-Janua, pp. 33–38, 2018.

[27] S. Shirali-Shahreza and Y. Ganjali, "*Protecting Home User Devices with an SDN-Based Firewall*," IEEE Trans. Consum. Electron., vol. 64, no. 1, pp. 92–100, 2018.

[28] P. Rengaraju, S. S. Kumar, and C. H. Lung, "*Investigation of security and QoS on SDN firewall using MAC filtering*," 2017 Int. Conf. Comput. Commun. Informatics, ICCCI 2017, pp. 0–4, IEEE 2017.

[29] C. E. Stewart, A. M. Vasu, and E. Keller, "*CommunityGuard: A crowdsourced home cyber-security system*," SDN-NFVSec 2017 - Proc. ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, co-located with CODASPY 2017, pp. 1–6, 2017.

[30] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, *"A Survey on the Security of Stateful SDN Data Planes,"* IEEE Commun. Surv. Tutorials, vol. 19, no. 3, pp. 1701–1725, 2017.

[31] E. V. Ananin, A. V. Nikishova, and I. S. Kozhevnikova, "*Port scanning detection based on anomalies*," 11th Int. IEEE Sci. Tech. Conf. "Dynamics Syst. Mech. Mach. Dyn. 2017 - Proc., vol. 2017-Novem, pp. 1–5, 2017.

[32] C. R. Taylor, C. A. Shue, and M. E. Najd, "*Whole home proxies: Bringing enterprise-grade security to residential networks*," 2016 IEEE Int. Conf. Commun. ICC 2016, 2016.

[33] S. Luo, J. Wu, J. Li, and L. Guo, "A multi-stage attack mitigation mechanism for software-defined home networks," IEEE Trans. Consum. Electron., vol. 62, no. 2, pp. 200–207, 2016.

[34] P. Gallo, K. Kosek-Szott, S. Szott, and I. Tinnirello, "*SDN@home: A method for controlling future wireless home networks,"* IEEE Commun. Mag., vol. 54, no. 5, pp. 123–131, 2016.

[35] Sandra Scott-Hayward, Sriram Natarajan, and Sakir Sezer, "*A Survey of Security in Software Defined Networks*", IEEE Communication Surveys & Tutorials, Vol. 18, No. 1, First Quarter 2016.

[36] S. K. Patel and A. Sonker, *"Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort*," Int. J. Futur. Gener. Commun. Netw., vol. 9, no. 6, pp. 339–350, 2016.

[37] J. Schulz-Zander, C. Mayer, B. Ciobotaru, S. Schmid, and A. Feldmann, "*OpenSDWN: Programmatic control over home and enterprise WiFi*," Symp. Softw. Defin. Netw. Res. SOSR 2015, ACM 2015.

[38] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "*Network-level security and privacy control for smart-home IoT devices*," 2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2015, pp. 163–167, 2015.

[39] M. Lee, Y. Kim, and Y. Lee, "*A home cloud-based home network auto-configuration using SDN*," *ICNSC 2015 - 2015 IEEE 12th Int. Conf. Networking, Sens. Control*, pp. 444–449, 2015.

[40] M. Chetty, H. Kim, S. Sundaresan, S. Burnett, N. Feamster, and W. K. Edwards, *"UCap: An internet data management tool for the home,"* Conf. Hum. Factors Comput. Syst. - Proc., vol. 2015-April, pp. 3093–3102, ACM 2015.

[41] P. Id, "*Outsourcing Home Access Point Coordination and Management through an Open API," IEEE Infocom 2015*, pp. 1454–1462, 2015.

[42] S. Wang, X. Wu, H. Chen, Y. Wang, and D. Li, *"An optimal slicing strategy for SDN based smart home network,"* Proc. 2014 Int. Conf. Smart Comput. SMARTCOMP 2014, pp. 118–122, IEEE 2014.

[43] N. Feamster *et al*, "*The Road to SDN: An Intellectual History of Programmable Networks*," ACM SIGCOMM Computer Communication ReviewApril 2014.

[44] M. Boussard et al., "*The Majord'Home: A SDN approach to let isps manage and extend their customer's home networks*," Proc. 10th Int. Conf. Netw. Serv. Manag. CNSM 2014, pp. 430–433, 2014.

[45] W. Lee, Y. H. Choi, and N. Kim, *"Study on Virtual Service Chain for Secure Software Defined Networking",* Advanced Science and Technology Letters, vol.29, pp.177-180, 2013.

[46] S. Sezer, "*Are We Ready for SDN? Implementation Challenges for Software-Defined Networks",* IEEE Communications Magazine, July, 2013.

[47] J. H. Jafarian, E. A. Shaer, Q. Duan, *"OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking",* HotSDN'12, Helsinki, Finland. ACM 978-1-4503-1477, 2012.

[48] A. Gember, P. Prabhu, Z. Ghadiyali, and A. Akella, *"Toward Software-Defined Middlebox Networking",* Hotnets '12, October 29–30, 2012, Seattle, WA, USA, ACM 978-1-4503-1776, 2012.

[49] R. Mortier et al., "*Supporting novel home network management interfaces with openflow and .NOX*," Proc. ACM SIGCOMM 2011 Conf. SIGCOMM'11, pp. 464–465, 2011.

[50] S. A. Mehdi, J. Khalid, and S. A. Khayam, *"Revisiting Traffic Anomaly Detection Using Software Defined Networking",* LNCS 6961, pp. 161–180, 2011. Springer-Verlag Berlin Heidelberg 2011.