Quest Journals
Journal of Software Engineering and Simulation
Volume 7 ~ Issue 9 (2021) pp: 01-08
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

A Review on Software Defined Network (SDN) Based Network Security Enhancements

Ahmad Ajiya Ahmad[1],Prof. Souley Boukari[2], Abdullahi Musa Bello[1], Muhammad Alhaji Madu[1], Sa'adatu Gimba[1]

[1]*Department of Computer Science, Faculty of Science, Federal University Gashua, Yobe State, Nigeria*
[2]*Mathematical Science Department, Abubakar Tafawa Balewa University, Bauchi Sate, Nigeria*

ABSTRACT:*SDN is an emerging technology that is considered a flexible, secure, and well-managed network.The fundamental idea behind SDN technology is the separation ofthe data (forwarding) layer from the control layer. Contrary, the traditional network comprises the data layer and the control layer together. The framework of the SDN offers a logically centralized network control and its management through a central controller. The communication devices in the data layer forward traffic according to control requests. It also provides dynamic programming and reconfiguration of rules and policy settings, which decreases the risk of cybercrime attacks. The downside of SDN separation led to innovative network security challenges, such as Denial-of-Service (DoS) threats. These problems gained momentous attention from both academic researchers and the IT industry. Various IT research groups have been launched to deliberate the security issues and solutions. For the time being, researchers have provided solutions to some SDN security problems these range from intrusion detection, SDN security design, controller imitation through policy and rule conflict resolution to authorization and authentication procedures.In this paper, potential network security features of different research works are reviewed, presented, and analysedon network security enhancement in SDN.*
KEYWORDS:*SDN, DoS, data layer, control layer, and traditional network*

Received 21 August, 2021; Revised: 03 September, 2021; Accepted 05 September, 2021 © The author(s) 2021. Published with open access at www.questjournals.org

I. INTRODUCTION

The legacy network is the network architecture that has been in practice for ages. Hence, it is incapable to address issues concerning modern-day systems. In the 1980s, legacy network mechanism was explored followed by lively networks in 1990s to present programmability into the traditional network. According to [29] it has become challenging nowadays to handle new conventional and vigorous systems applications effectively in an efficient way by the legacy network [41]. At the moment, the dynamic application concerning central/programmable features is less effective in the traditional network. To overcome the inadequacy of the legacy networks architecture, a new dynamic and scalable technology is developed, called Software-defined networking (SDN), it has been established as an innovative model for the imminent contemporary Internet. That is the arrival of cloud computing and virtualization in the Database-centric Architecture or data-centric architecture for processing, storing, and distributing data and applications efficiently, the right application for SDN was explored [25]. The main feature of the SDN architecture is the separation of the data forwarding and control layers, which has changed SDN to a more centralized model and flexible for networks. The conceptual differences between the SDN architecture and legacy architecture are shown in figure 1. SDN first originated into reality at Stanford University by OpenFlow protocol which is the first SDN standard protocol [46]. The Open Networking Foundation (ONF) provided interest for acceptance and implementation of SDN by developing the OpenFlow protocol. It is accountable for intercommunication between the SDN control and the data forwarding layer. OpenFlow was suggested in 2008 to offer flexibility and programmability [51].

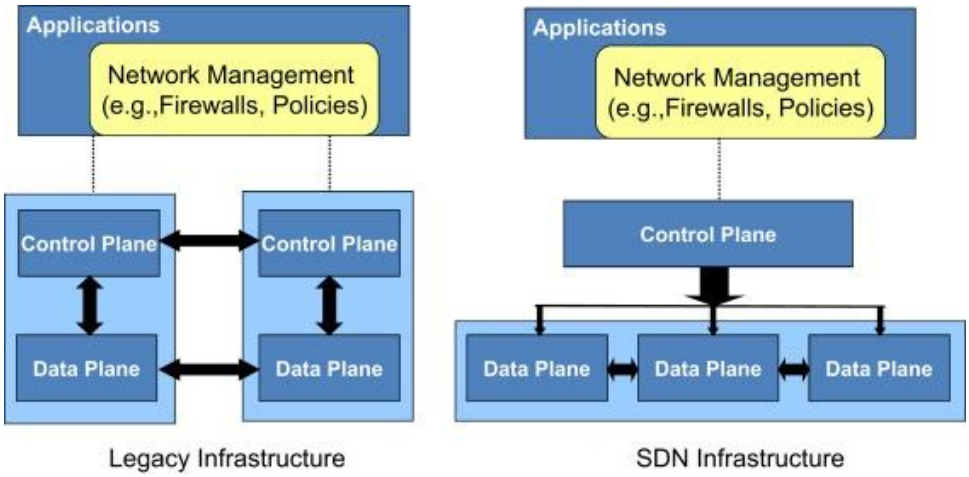

Figure 1: Overview of Legacy and SDN Infrastructure

SDN allows scholars to design and implement new inventive network applications, functions, and protocols in a considerable manner, easier and flexible approach. In specific, OpenFlow is now the best-deployed SDN scheme, which offers communication among the switches and the controller.

In SDN, the central controller is responsible to determined and controls the policies and rules of the network [30]. OpenFlow protocol is also capable of retrieving network data due to its traffic flow-based forwarding technique of the SDN. There are several open-source software that can be used to implement SDN controllers. These software are floodlight, NOX, Open Daylight, Ryu, and Beacon [42]. Though this separation of SDN involves abolishing and use of the physical and switches routers, this lets one omitting the firewall that works to protect the network from intrusion and leaves the network weaker and vulnerable to more attacks [20]. Decreases the complexity of network and system configuration but [4] indicated that SDN provoked with security extortions and risk of dynamic applications. Therefore, security has turned out to be a significant area of apprehension for SDN, henceforth, requires significant deliberation from industry and academia[50]. This article aims to review and analysevarious research works on network security enhancements based on SDN models security problems.

II. REVIEW OF LITERATURE

In the 1970s, the development of computer networks shaped novel issues associated with the monitoring of individual host activities and access. Anderson [6] outlines that the United States Air Force (USAF) operations and administration department encounter and notice increasingly alert of computer security issues. The specific problem was for the reason that the security clearance unit shared the same computer systems. Anderson [7]highlights numerous approaches to increase the level of computer security threat surveillance and monitoring. Also, presents the knowledge of powering and developing the detection of intrusion attacks inside a network to identify secret individual hosts. The main idea of Intrusion Detection Systems (IDS) is to support system administrators to appraise system event logs, user access records, and file access archives. Denning [15] develop an IDS model for real-time intrusion detection and it was a prototype called Intrusion Detection Expert System (IDES). This prototype uses rule-based to identify malicious attacks and statistical anomaly detection on host data.

These have made [51] to be perceptive in his research and derived a possible solution that is SDN architecture, to separate the network into infrastructure layer and control layer [16]. Have proposed solutions to handle SDN threats including Open Networking Foundation (ONF). Though SDN research is yet in its initial stage and [28] emphasized many problems that are essential to be handled and addressed. Sooraj and Prabhakar [49] mentioned that a firewall security system is a technique of detecting intrusion on SDN, the system takes a long time to detect attack because SDN network is not compatible with firewall since it works and protect intrusion from outside the network. Various research [5], [28], [49], [34], [29], [41] have relied on a single type of attack, DoS Attack. Although SDN is usually deployed in several network environments and the technology is still under improvement [42] and the earlier record of SDN attacks is unidentified.

According to [3] SDN offersdifferent innovative research opportunities to security, and it can significantlyinfluence network security research in various ways but currently, SDN has not been well acknowledged.In this methodicalreview on SDN network, security enhancement we study how the novel features provided by SDN can aid enhance network security and data security development. Scott-Hayward et al. [46] introduced six prospective SDN-based Network Security Issues to consider for SDN enhancement as shown in figure 2. More so a taxonomy showing different research works that addressed different issues on

SDN security is displayed in figure 3. It enumerates and depicts the sequence flow of the SDN Network Security Enhancements based on various research works.

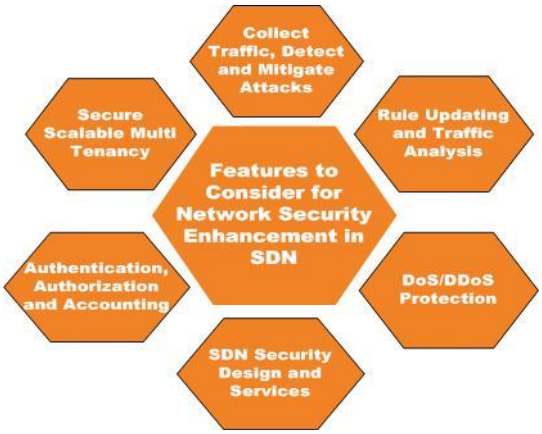

Figure 2: Prospective SDN based Network Security Issues

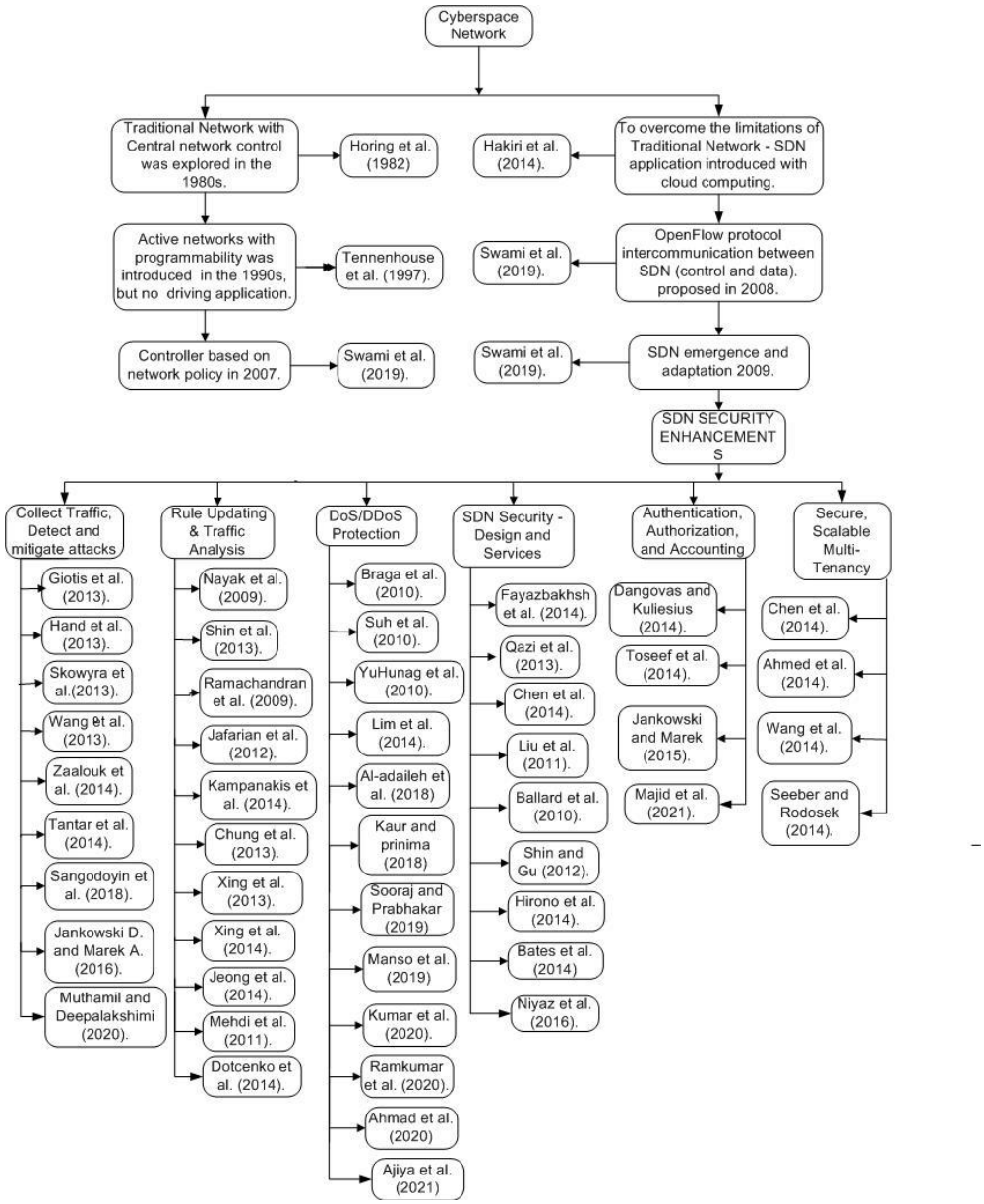

Figure 3: Taxonomy of SDN based research works on Network Security Enhancements

III. DISCUSSION ON SDN NETWORK SECURITY

According to [46] six features could be identified to achieve and obtain the prospective network security improvements based on the implementation of SDN infrastructure and deployment. The identification of these features provides effectiveness to build up or develop more secure and reliable SDN applications or SDN infrastructure. This section reviewed, the opportunities introduced by SDN to network security from various research works. This will offernovel insights for future research in this significant area.These classes are identified as presented in figure 3.

3.1 Collect Traffic, Detect and Mitigate Attacks

In this stage, a method involved collecting intelligence data from previous Intrusion Detection Systems and Intrusion Prevention Systems, followed up by investigation and consolidated reprogramming of the network, which can offer the SDN more efficient and reliable to intrusion attacks than traditional networks [46] will be discussed. This process is well illustrated as Step onethe Collector, in which traffic information is collected through the OpenFlow protocols. Step two the intrusion Detection, at this stage analysis is performed on the statistics, and intrusion is identified. Step three the intrusion Mitigation, at this stage flow-entry can be injected to override the known attack [46].In Table 1, a comprehensive fact of the problems and solutions presented for each research work introduced under collect, detect, and mitigateto protect and provide Network Security Enhancements in SDN is provided.

Table 1:- Research Works Based on Collect-Traffic, Detects, and Mitigates Attacks.

S/N	Reference	Problem	Solution
1	[19]	Control layer DoS traffic overload during OpenFlow traffic collection.	Developed an SDN-based Intrusion detection system and intrusion prevention system on traffic Collection Modules for intrusion Detection and intrusion Mitigation.
2	[21]	Defective and Uncertain Programmable Security Infrastructure.	Provided Network Response Control that providing consistent security.
3	[48]	Issues of intrusion detection for embedded portable devices.	Used OpenFlow SDN to identify intrusion traffic and reconfigure the network.
4	[55]	Avoid data centre network congestion challenges.	Used OpenFlow proxy device to identify traffic overload based on flow aggregation.
5	[59]	To overcome weaknesses of existing network security applications.	Orchestrator-based SDN model to implement security applications.
6	[52]	To provide effective security to SDNs at the infrastructure layer.	A cognitive module is applied in the infrastructure layer.
7	[43]	Issues of DDoS overload in SDN.	A confidence interval and mean throughput are applied at the SDN controller to identify intrusions.
8	[25]	The problem of monitoring and detection of anomalies behaviour at the data layer.	Introduced intrusion detection to classify and validate using machine learning algorithms.
9	[36]	The problem of DDoS attack congestion at the SDN controller.	Introduced entropy-based mechanism and machine learning-basedC4.5 technique to identify specific congested traffic paths and drop the packets.

3.2 Rule Updating and Traffic Analysis

This category of SDN security enhancements s recognized by their effort on a particular intrusion detection and prevention scheme enforced. Precisely, the high-level security rules are established based on network traffic analysis and applied by computerized switches to enforce policy or rule updating [57]. This system is introduced for securing enterprise networks and its results are range from dynamic access control to traffic tagging an3108d filtering [56], [46]. Generally, tools are used to checks a distinct traffic statistic condition against locally collected traffic packets to define an appropriate action or request [45], [27]. In Table 2, a summary of the problems and solutions offered for each research work presented under Rule Updating and traffic analysis on Network Security Enhancements in SDN is supplied.

Table 2:- Research Works Based on Rule Updating and Traffic Analysis

S/N	Reference	Problem	Solution
1	[37]	To increase the capacity of enterprise network attack response.	Provided Dynamic access control system for securing enterprise networks.
2	[45]	To Protect the Control layer against DoS intrusions and dynamics flow response.	Introduced Connection Migration Tool dropping data-control layer communication and Initiating Prompt to install flow rules.
3	[40]	To Protect enterprise networks against Computer viruses (malware) distribution.	Introduced Traffic flow monitoring and classification for flow tracking and filtering.
4	[23]	To recurrently change host IP addresses for mobile defense targets.	Presented Random Host Mutation using virtual-to-real IP translation.
5	[27]	To protect against network and service exploration.	SDN-based mobility Target network defense systems.
6	[13]	To protect exposed virtual systems in cyberspace	Introduced Network anomaly detection, measurement, and

		from being compromised.	countermeasure assortment framework.
7	[56]	Overcome the performance flexibility problems of present Intrusion Prevention Systems.	Introduced an enhanced OpenFlow-based Intrusion Prevention Systems to improve latency and accuracy.
8	[57]	The problem of reconfiguring cloud networking on the fly with the Intrusion Prevention Systems.	An enhanced SDN-based Anomaly Prevention solution.
9	[26]	Issue of increasing capacity of network traffic.	Provided Scalable IDS model with sampling rate modification technique.
10	[35]	Issues of home/ office network security problems.	Introduced Intrusion Detection techniques mounted in NOX controller.
11	[17]	To Use SDN to identify and secure the network from malicious attacks.	Develop a fuzzy logic-based information security management system for SDN.

3.3 DoS/DDoS Protection

The DoS attack was identified in [10], [31], [50], [5] as a weakness of SDN. Though, several solutions were exploited to create an efficient and robust DoS/DDoS protection scheme by combining traffic analysis at the control layer and the data layer programmability [50]. In each case, traffic statistics are introduced to identify the DDoS intrusion with the particular technique conditional on the network environment. In Table 3, a precise description of the problems and solutions provided for each research work presented under DoS/DDoS Protection on Network Security Enhancements in SDN is conveyed.

Table 3:- Research Works Based on DoS/DDoS Protection

S/N	Reference	Problem	Solution
1	[10]	Issue of DDoS attack detection.	Presented Statistical information with self-organizing maps method to categorize traffic flow as normal or malicious.
2	[50]	Issues of DDoS attack detection and response in the content-oriented network.	The rate and pattern of content requests are examined to identify DDoS attacks.
3	[58]	The problem of DDoS attack detection and response.	Use OpenFlow to identify and drop DDoS traffic based on traffic flow capacity.
4	[31]	To Overcome the problem of detecting and blocking DDoS attacks by botnet	Introduced DDoS blocking solution for SDN-managed network.
5	[5]	Problems of DoS at the Controller and performance flexibility.	Introduced Entropy-based rule and Correlation-based rule to identify DDoS attacks against SDN controllers.
6	[28]	To stop Threat targeting and overloading the SDN controller.	Presented an optimized technique to Classify and identify malicious traffic flow based on Traffic Statistics.
7	[49]	Problems of DoS attack identification and mitigation on OpenStack Cloud.	The introduced firewall security system is an efficient model for protecting OpenStack cloud infrastructures.
8	[34]	Issues of network performance due to DoS cyber-attacks.	Implemented security scheme on SDN model, at the client-side.
9	[29]	Ineffectiveness of machine learning classifiers in classifying DoS traffic redundancy.	Applied feature selection methods for data pre-processing.
10	[41]	Issues of traffic overload at the controller.	Introduced mean entropy and the rate of percentage drop to stop the occurrence of DDoS attacks.
11	[1]	Issue of DoS attack flooded at the controller affecting SDN performance.	Introduced a NID scheme to improve the performances of the SDN controllers against DoS attacks.
12	[3]	SDN lacked an effective mechanism to detect malicious traffic. The problem of using a single controller. Issue of correlated data in an available dataset.	Proposed machine learning-based NIDS methods for detecting. Introduced multiple controller systems to tackle new incoming packets. Introduced feature selection methods to a produced redundancy-free dataset.

3.4 SDN Security Design and Services

It's important to consider SDN security challenges and middleboxeswhen designing and deploying SDN architecture [46]. SDN security problems, middleboxes, andapplication service necessities to identify the vibrant platforms in which SDN will be deployed e.g. cloud, data centre, and mobile [44].SDN characteristics are provided to incorporate network layer with security middleboxes such as intrusion prevention system or Firewall to stopintruders at the network end.To offer protected visibility of networks through dynamic and multiple networks, innovative security designs will be essential [46]. SDN-based Security models or applications have related to improving network security when integrated with intrusion detection systems or prevention systems [46], [18]. In Table 4, a summary of the problems and solutions identified for each research work provided under SDN Security design and services for Network Security Enhancements in SDN is presented.

Table 4:- Research Works Based on SDN Security Design and Services

S/N	Reference	Problem	Solution
1	[18]	To Guarantee consistency in network policy enforcement in the presence of SDN Architectures.	SDN architecture adds tags to outgoing traffic flow to provide correct context.
2	[39]	To provide Efficient SDN-specific traffic steering.	Tag and tunnel traffic between SDN architecture.
3	[11]	To overcome the problem of Quality of Service assurance in security traversal.	Introduced dynamic security traversal scheme with SDN models.
4	[32]	To Restrict secret traffic channels.	Introduced Multi-level security network switch using Open Flow filter.
5	[8]	To control network traffic flow through security monitoring applications.	Used Open Flow to implement trigger policy for identifying and handling traffic paths.
6	[44]	To improve monitoring activities for cyberspace networks.	Introduced SDN Application to control and direct traffic flows through security services.
7	[22]	Use SDN to protect the internal network from intrusions.	Secure traffic analysis system to trace malicious behaviours on internal networks.
8	[9]	Problems of data exploration and conspiracy between compromised nodes.	Presented an SDN-based forensic model that monitors, investigates and tracks network behaviours.
9	[38]	Problems of program network devices flexibility to eliminate the need for third-party vendor-specific hardware.	Presented an SDN-based multi-vector DDoS detection system to secure enterprise network infrastructure.

3.5 Authentication, Authorization, and Accounting (AAA)

AAA signifies Authentication, Authorization, and Accounting. It involvesin a group of protocols that facilitate network access control [53].Scott-Hayward et al. [46]defined AAA as a structure for logically controlling access to computer data and information, implementing policies/rules, checking network usage, and offering the data essential to bill for service requests. Moreover, accounting stands forrecord-keeping, monitoring, andtracing of clientevents on a computer network.

In [53]an authentication and access control were introduced as a solution to the problem of unauthorized access in SDN models. The capability of an OpenFlow-based SDN to aid access control to match services to identities could be involved as an SDN network security enhancement [14], [53]. An SDN-based authentication, authorization, and accounting system are introduced in [53]to improve network security. In Table 5, a summary of the problems and the solutions proposed for each research work presented under Authentication, Authorization, and Accounting for Network Security Enhancements in SDN is conveyed.

Table 5:- Research Works Based on Authentication, Authorization, and Accounting.

S/N	Reference	Problem	Solution
1	[14]	Reinforce network security by SDN-driven access control.	Provided OpenFlow cantered controller with authentication.
2	[53]	To Provide robust, efficient security management for SDN experimental facilities.	Presented a certificate model that encloses authentication, authorization, and accounting for SDN experimental facilities.
3	[24]	Issue of unauthorized activities in SDN.	Offered a measurement system that assembles network traffic flow factors to detect unauthorized activities using machine learning.
4	[33]	Issue of sophisticated attack traffic and a large number of users accessing an unauthorized network resource.	Introduced robust entropy-based method to stop massive attack traffic flow in an SDN network.

3.6 Secure Scalable Multi-Tenancy

Scott-Hayward et al. [46] describe multi-tenancy in a typical SDN network, multi-tenancy involves multiple consistent switches represented in a shared physical discrete such that each entity can signify individual tenants or customers. One of the features of SDN identified in [46] is virtualized analytical networks and the fact that SDN supports multi-tenancy. Some solutions have been introduced that exploit the features of SDN to offer multi-tenant network security. In Table 6, a detailed description of the problems and the solutions provided for each research work presented under Secure Scalable multi-tenancy for Network Security Enhancements in SDN is delivered.

Table 6:- Research Works Based on Secure Scalable Multi-Tenancy

S/N	Reference	Problem	Solution
1	[12]	To Address network security in numerous tenant datacentre networks.	Suggested a collaborative network security model with smart traffic monitoring using SDN.
2	[2]	To Support multi-tenancy whereas solving scalability issues.	Introduced SDN model supporting multi-tenancy and flexible separation between tenant networks.
3	[54]	To deliver network security services for a tenant cloud system.	Provided Security Workload scheme for fine-grained dynamic network security defense.
4	[47]	To offer system and service network security in cloud frameworks.	Developed a sensibly centralized archive to offer the newest system and service security information.

Moreover, these potential network security features presented for network security enhancement will simplify the implementation and deployment of SDN-based networks and offers a clear benefit to IT business enterprises.

IV. CONCLUSION

This article reviewed and analysed various research works on network security enhancements based on SDN Security challenges. The article is able to introduced network security enhancements presented by SDN.The conclusion is that the review on SDN-based network security enhancements is established and this issupported by the commercially developed applications. We observed that SDN can enhance network security functions in various ways. SDN can offer flexible implementation of security functions because of its capability of monitoring dynamic network traffic flows and simplicity of programmability.Though, research solutions have been offered to tackle some of the security challengesprovided by SDN, such as how to reduce the possibledestruction from a bargained application. Effort on these issues is developing encouraged by the growing security attention of industry research groups and academia. To this extend, network security can be enhanced using SDN when the research and industry approach to security issues in SDN technology.However, the network security features identified in this article for network security enhancement impacted positively inimproving the capacity of effective and efficient SDN implementation and deployment.This will be beneficial and advantageous to IT business enterprises and academic researchers conducting studies into the field of SDN.

REFERENCES

[1]. Ahmad, F. A., Fatty, M. S., Ashraf, T. and Mohamed, H A. (2020). Performance Analysis and Evaluation of Software Defined Networking Controllers against Denial of Service Attacks. Journal of Physics: Conference Series.Conf. Ser. 1447 012007.

[2]. Ahmed, M. F. Talhi, C., Pourzandi, M., and Cheriet, M. (2014). "A Software Defined Scalable and Autonomous Architecture for Multi-tenancy," Cloud Engineering (IC2E), 2014 IEEE International Conference. pp. 568–573.

[3]. Ajiya, A. A., Musa, A. B. and Aliyu, M. M. (2021). Solution Model for Intrusion Detection in Software Defined Networking (SDN) using Machine Learning. Quest Journals: Journal of Software Engineering and Simulation, Volume 7,Issue 8, pp: 40-47.

[4]. Akhunzada,A., Iram, B., Jahanzaib, M. and Tanzila, S.(2019). Intelligent intrusion detection system using deep learning in Software defined network. https://www.researchgate.net/publication/341756680.

[5]. Al-adaileh, M., A. A., Mohammed, A., Yung-Wey, C., and Ahmed, A. (2018). Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS). MATEC Web of Conferences.218, 02012.https://doi.org/10.1051/matecconf/201821802012.

[6]. Anderson, J. P. (1972). "Computer security technology planning study," Oct. 1972.[Online; accessed 2021-04-04].

[7]. Anderson, J. P. (1980). "Computer security threat monitoring and surveillance,".[Online; accessed 2021-04-04].

[8]. Ballard, J. R., Rae, I., and Akella, A. (2010) "Extensible and scalable network monitoring using OpenSAFE," Proc.INM/WREN.

[9] Bates, A., Butler, K., Haeberlen, A., Sherr , M. and Zhou, W. (2014). "Let SDN Be Your Eyes: Secure Forensics in Data Center Networks," Workshop on Security of Emerging Networking Technologies (SENT).

[10]. Braga, R., Mota, E., and Passito, A. (2010)."Lightweight DDoS flooding attack detection using NOX/OpenFlow," IEEE 35th Conference on Local Computer Networks (LCN). IEEE, pp. 408–415.

[11]. Chen, Y. J., Lin, F. Y., and Wang, L. C. (2014). "Dynamic Security Traversal in OpenFlow Networks with QoS Guarantee," International Journal of Science and Engineering, vol. 4, no. 2, pp. 251–256.

[12]. Chen, Z., Dong, W., Li, H., Cao, J., Zhang, P., and Chen, X. (2014). "Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing," Tsinghua Science and Technology, vol. 1, p. 009.

[13]. Chung, C.J., Khatkar, P., Xing, T., Lee, J., and Huang, D. (2013). "NICE: Network intrusion detection and countermeasure selection in virtual network systems," IEEE Transactions on Dependable and Secure Computing, p. 1.

[14]. Dangovas, V. and Kuliesius, F. (2014)."SDN-Driven Authentication and Access Control System," International Conference on Digital Information, Networking, and Wireless Communications (DINWC2014). The Society of Digital Information and Wireless Communication, 2014, pp. 20–23.

[15]. Denning, D. E. (1987)."An intrusion-detection model," IEEE Trans. Softw. Eng., vol. 13,pp. 222–232.

[16]. David, J. D. and Benjamin, M. B. (2011).A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines.The Fifth International Conference on Digital Society.187-192.

[17]. Dotcenko, S., Vladyko, A., and Letenko, I. (2014). "A fuzzy logic-based information security management for software-defined networks, "Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, pp. 167–171.

[18]. Fayazbakhsh, S. K., Chiang, L., Sekar, V., Yu, M., and J. Mogul, C. (2014)."Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags," in Proc. NSDI.

[19]. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., and Maglaris, V. (2013).Combining OpenFlow and sFlow for an effective and scalable Anomaly Detection and Mitigation mechanism on SDN Environments, Computer Networks.

[20]. Hakiri, A., Aniruddha G., Pascal B., Douglas C. S.t, and Thierry G. (2014). Software-defined networking: Challenges and research opportunities for future internet. Computer Networks. 75, 453–471. DOI:http://dx.doi.org/10.1016/j.comnet.2014.10.015.

[21]. Hand, R., Ton, M., and Keller, E. (2013) "Active Security," ACM SIGCOMM Hot Topics in Networks.

[22]. Hirono, S., Yamaguchi, Y., Shimada, H., and Takakura, H. (2014)."Development of a secure traffic analysis system to trace malicious activities on internal networks," Computer Software and Applications Conference (COMPSAC), IEEE, pp. 305–310.

[23] Jafarian, J. H., Al-Shaer, E., and Duan, Q. (2012). "Openflow random host mutation: transparent moving target defense using software defined networking, "Proceedings of the first workshop on Hot topics in software defined networks. ACM, pp. 127–132.

[24]. Jankowski, D. and Marek, A. (2015).Intrusion Detection in Software Defined Networks with Self-organized Maps. Institute of Telecommunication, Faculty of Electronics, Military University of Technology.

[25]. Jankowski, D. and Marek, A. (2016). On Efficiency of Selected Machine Learning Algorithms for Intrusion Detection in Software Defined Networks.International Journal of Electronics and Telecommunications. VOL. 62, No. 3, pp. 247-252. DOI: 10.1515/eletel-2016-0033.

[26]. Jeong, C., Ha, T., Narantuya, J., Lim, H., and Kim, J. (2014).“Scalable network intrusion detection on virtual SDN environment,” in Cloud Networking (CloudNet), International Conference on.IEEE,pp. 264–265.

[27]. Kampanakis, P., Perros, H., and Beyene, T. (2014). “SDN-based solutions for Moving Target Defense network protection,” A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on. IEEE, pp. 1–6.

[28]. Kaur, G. and Prinima, G. (2018).Proposed Optimization Technique to detect DDOS Attacks on Software Defined Networks.4th International Conference on Computers and Management (ICCM).281-287.

[29]. Kumar, S. D., Raihan, U. and Mahbubur, R. (2020).Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach.International Joint Conference on Computational Intelligence, Algorithms for Intelligent.pp.483 494.

[30]. Lakshmanan, A.(2018).Enhanced Software Defined Networking (SDN) with security &performance in cloud computing. https://www.researchgate.net/publication/329735894.

[31]. Lim, S., Ha, J., Kim, H., Kim, Y., and Yang, S. (2014). “A SDN-oriented DDoS blocking scheme for botnet-based attacks,” in Ubiquitous and Future Networks (ICUFN), InternationalConf on. IEEE,pp. 63–68.

[32]. Liu, X., Xue, H., Feng, X., and Dai, Y. (2011).“Design of the multi-level security network switch system which restricts covert channel,” International Conference on Communication Software and Networks (ICCSN).IEEE, pp. 233–237.

[33]. Majid, R. A. U., Zeeshan, P., Keshav, D., Wajahat, A., Asad, M. K. and Bashir, H. (2021). Entropy Based Features Distribution for Anti-DDoS Modelin SDN. Sustainability: MDPI.https://doi.org/10.3390/su13031522.

[34]. Manso, P., Jose, M. and Carlos, S. (2019). SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks.Information-Open Access Journal.10.106.1-17.

[35]. Mehdi, S. A., Khalid, J., and Khayam, S. A. (2011). “Revisiting traffic anomaly detection using software defined networking,” Recent Advances in Intrusion Detection. Springer, pp. 161–180.

[36]. Muthamil, K. S. and Deepalakshm, P. (2020).A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique.Journal of High Speed Networks. No. 26, pp 55–76. DOI 10.3233/JHS-200630.

[37]. Nayak, A. K., Reimers, A., Feamster, N., and Clark, R. (2009).“Resonance: dynamic access control for enterprise networks,” Proceedings of the 1st ACM workshop on Research on enterprise networking. ACM, pp. 11–18.

[38]. Niyaz, Q., Weiqing, S. and Ahmad, Y. J. (2016). A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN). https://www.researchgate.net/publication/310671661.

[39]. Qazi, Z. A., Tu, C. C., Chiang, L., Miao, R., Sekar, V., and Yu, M. (2013).“SIMPLE-fyingMiddlebox Policy Enforcement Using SDN.” ACM SIGCOMM.

[40]. Ramachandran, A., Mundada, Y., Tariq, M. B., and Feamster, N. (2009). “Securing enterprise networks using traffic tainting,”.

[41]. Ramkumar, M. P., Emil, S. and Bavani, K. (2020).Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined.International Conference on Advanced Computing & Communication Systems (ICACCS).No. 6.pp. 380 -385.

[42]. Said, M. E., Nhien-An, L. and Anca, J. (2020). InSDN: A Novel SDN Intrusion Dataset. DOI10.1109/ACCESS.2020.3022633, IEEE Acces

[43]. Sangodoyin, A., Babagana, M., Irfan, A., Jules, P. D. (2018). An approach to detecting distributed denial of service attacks in software defined Networks. International Conference on Future Internet of Things and Cloud.DOI 10.1109/FiCloud.2018.00069. pp. 436 – 443.

[44]. Shin, S. and Gu, G. (2012). “CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?),” IEEE: International Conference on Network Protocols (ICNP). pp. 1–6.

[45]. Shin, S., Yegneswaran, V., Porras, P., and Gu, G. (2013) .“AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks,” Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security. ACM, pp. 413–424.

[46]. Scott-Hayward, S., Natarajan, S., and Sezer, S. (2016). A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials, 18(1), 623-654. https://doi.org/10.1109/COMST.2015.2453114

[47]. Seeber, S. and Rodosek, G. D. (2014). “Improving Network Security through SDN in Cloud Scenarios,” pp. 376–381, 2014.

[48]. Skowyra, R., Bahargam, S., and Bestavros, A.(2013). “SoftwareDefined IDS for Securing Embedded Mobile Devices,”.[Online]. Available: http://www.cs.bu.edu/techreports/pdf/2013-005- software-defined-ids.pdf.

[49]. Sooraj, V. H. and Prabhakar, K. (2019). SDN based Intrusion Detection System for OpenStack Cloud. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 8, 9, 2443-2449.

[50]. Suh, J., Choi, H., Yoon, W., You, T., Kwon, T., and Choi, Y. (2010).“Implementation of Content-oriented Networking Architecture (CONA): A Focus on DDoS Countermeasure,” European NetFPGA Developers Workshop.

[51]. Swami,R., Mayank,D. and Virender,R.(2019).Software-defined Networking-based DDoSDefense Mechanisms. ACM Computing Surveys.Vol.52, No. 2, Article 28, pp. 28 -36.

[52]. Tantar, E., Palattella, M. R., Avanesov, T., Kantor, M., and Engel, T. (2014). Cognition: A Tool for Reinforcing Security in Software Defined Networks, ser. EVOLVE-A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation V. Springer, pp. 61–78.

[53]. Toseef, U., Zaalouk, A., Rothe, T., Broadbent, M., and Pentikousis, K. (2014). “CBAS: Certificate-based AAA for SDN experimental facilities,” European Workshop on Software Defined Networks (EWSDN). IEEE, pp. 91–96.

[54]. Wang, X., Liu, Z., Li, J., Yang, B., and Qi, Y. (2014).“Tualatin: Towards network security service provision in cloud data centres,” Computer Communication and Networks (ICCCN), 2014 23rd International Conference on. IEEE, pp. 1–8.

[55]. Wang, Y., Zhang, Y., Singh, V., Lumezanu, C., and Jiang, G. (2013) “NetFuse: Short-circuiting traffic surges in the cloud,”IEEE International Conference on Communications (ICC). IEEE, pp. 3514–3518.

[56]. Xing, T., Huang, D., Xu, L., Chung, C.J., and Khatkar, P. (2013).“Snortflow: Aopenflow-based intrusion prevention system in cloud environment,” Research and Educational Experiment Workshop (GREE), 2013 Second GENI. IEEE, pp. 89–92.

[57]. Xing, T., Xiong, Z., Huang, D., and Medhi, D. (2014). “SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds,” pp. 308–311.

[58]. Yu Hunag, C., MinChi, T., YaoTing, C., YuChieh, C., and YanRen, C. (2010).“A novel design for future on-demand service and security,” in Communication Technology (ICCT), IEEE International Conference on, pp. 385–388.

[59]. Zaalouk, A., Khondoker, R., Marx, R., and Bayarou, K. (2014). “OrchSec: An orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions,” Network Operations and Management Symposium (NOMS), IEEE. IEEE, 2014, pp. 1–9.