ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 11, November 2025

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811034

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Framework for SDN Forensic Readiness and Cybersecurity Incident Response

S. Suganya[1], M. Gobinath[2], T.Sathishkumar[3], Dr.G.Singaravel[4], Dr.K.Balamurugam[5], Dr.S.Anguraj[6]

Assistant Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[1]

II Year M.Tech, Department of Information Technology, K.S.R. College of Engineering(Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[2]

Assistant Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[3]

Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[4]

Associate Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[5]

Associate Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Namakkal District, Tamil Nadu, India[6]

ABSTRACT: The search for better networking paradigms has fostered the emergence of Software Defined Networking (SDN), which allows the decoupling of the data plane from the control plane and to configure the network dynamically. SDN provides network operators with significant visibility and granularity of their networks leading to more flexibility in programming these networks. Typically, with every new technology paradigm, the security concerns represent a serious challenge. In this paper, we provide a comprehensive SDN security review including the different vulnerabilities and attacks that SDN suffers from. The objective is to entice the SDN community to address such issues inherently and not as an afterthought. The paper also reviews the different security proposals that have been presented or implemented for SDN and by SDN. A general discussion is included to shed light on the pending security issues and some proposed solutions are presented.

KEYWORDS: SDN; software defined networking; application plane; control plane; data plane; SDN security.

I. INTRODUCTION

The software-defined network (SDN) has become one of the top networking architectures for simplifying network management by enabling innovation in network communication. The fundamental characteristic of SDN architecture is to decouple the control plane from the data plane. A control plane is logically centralized to maintain the network state and gives instructions to the data plane [1]. In the data plane network, devices forward data packets by following the control instructions. However, this architectural transformation has received immense attention from the network industry and academic fields. Additionally, the advantages of SDNs have been proven in different scenarios, such as Google B4, NTT's edge gateways, and Microsoft's public cloud [2,3,4].

SDN also offers a standardized or consistent application programming interface (API) for adding up-to-date programmable features to the network to overcome flexibility and programmability issues in traditional networks. In addition, SDNs help network service providers to obtain a more flexible, manageable, and programmable network architecture [5]. These properties of SDNs help to empower the control plane and accomplish a global view of network topology to dynamically modify the functionalities of the network. Although SDNs manage networks in a more centralized way, it is now endorsed by both academic and industrial practitioners. This is because security has become

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811034

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

a major concern at all levels, especially in newly designed network systems, such as cloud networks and peer-to-peer networks. Therefore, despite the number of advantages, SDNs have many inherent network security challenges, including scalability, reliability, controller placement, and latency [6]. Moreover, several security attacks were also investigated by other researchers and were examined in other network systems [7,8,9,10]. On the downside, the increased potential of security attacks on SDN layers has become a prime concern. The increased potential of security threats, including the consistency of flow rules, controller vulnerability, legitimacy, malicious applications, and standardized and northbound and southbound communications, occurs due to a lack of best practices of SND functions, components, and the open programmability of networks. From the literature, it is clear that due to the multi-layered architecture of SDN, security threats to different layers are different.

SDN architecture is presented in Figure 1, with the most common and major security challenges on SDN layers. The application layer is also known as the management layer and is the topmost layer in the SDN architecture. All business and security applications that are designed by developers are executed on this layer. Applications controlled by this layer consist of firewall implementation, access control, load balancer, intrusion prevention system (IPS), intrusion detection system (IDS), and network virtualization.

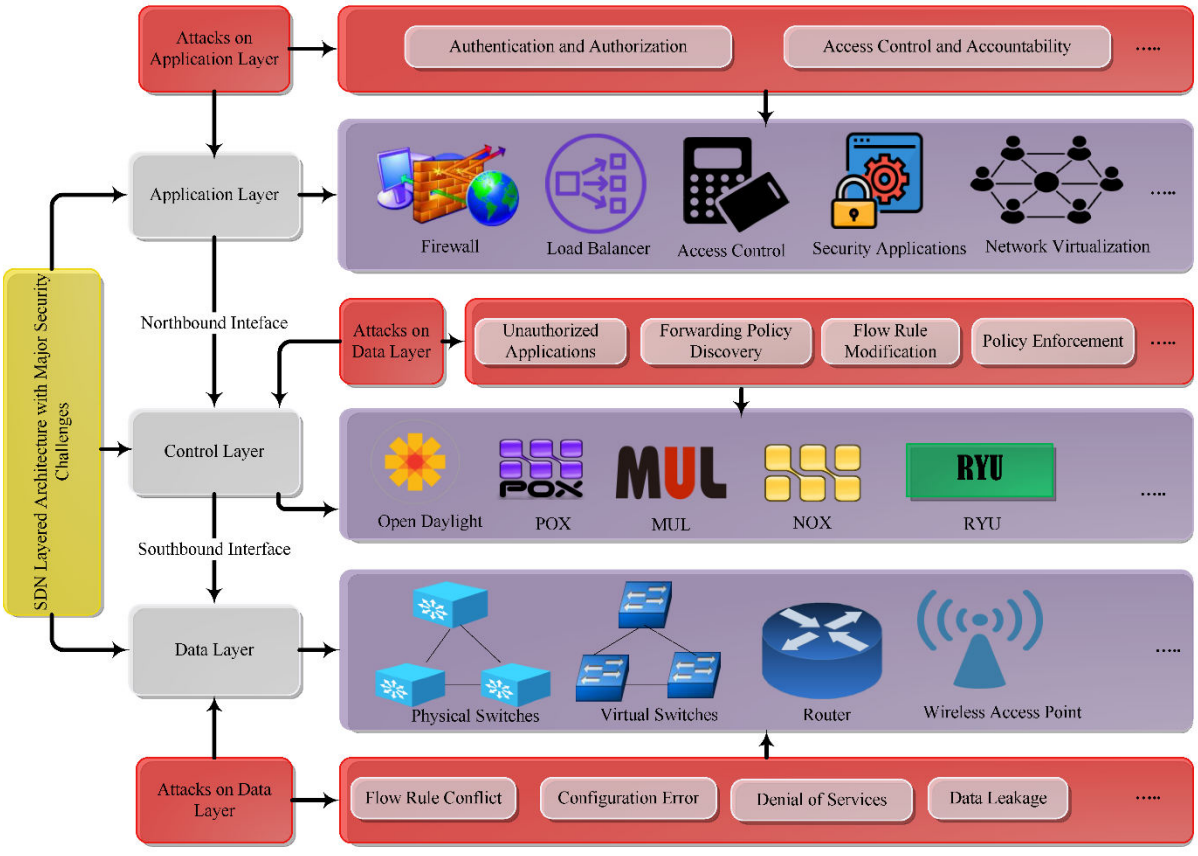

Figure 1. SDN Architecture with major security attacks.

The application layer communicates with the control layer by using northbound API [**11**]. Although applications deploy multiple network services in SDN, there are still some major security challenges in SDN due to the emerging abilities of hackers. The most common security threats at this layer are authentication, authorization, access control, and accountability. The control layer is the mediator between the application layer and the data layer, which consists of the SDN controller or network operating system (NOS). The overall responsibility of this layer is to manage the functionality of the entire network by taking decisions on packet forwarding and routing [**12**]. The control layer communicates with its lower layer (data layer) by using southbound API. The logically centralized controller consists of node flows like flood light, POX, NOX, MUL, Jaxon, etc.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This layer is only responsible for decision making due to its logically centralized controller; therefore, it is easily targeted in order to perform malicious tasks across the entire network. Major security challenges on this layer are unauthorized applications, flow rule modification, policy enforcement, and forwarding policy discovery. The data layer is responsible for packet forwarding, according to the assigned policies of forwarding devices, such as physical switches and virtual switches.

To deploy packet forwarding policies in SDN, OpenFlow switches are used to support the flow tables and flow rules, because OpenFlow is the most widely used southbound interface in SDN scenarios. Flow tables are the main data structure in OpenFlow devices that contain a set of flow entries. Packet forwarding devices analyze the incoming packets through flow tables and take corrective measures regarding the received information. However, flow rules are used to control the behavior of packet forwarding, which is identified via matching packet fields as well as other features, such as packet counters. When the first packet arrives from the new host at the open flow switch, it is necessary for the controller in the flow table to install a new flow rule. However, due to the space constraint, every switch has a limitation on flow table entries, which generates new security issues. The most common security challenges that arise at this layer are DoS, configuration errors, flow rule conflicts, and data leakage. Over the last few years, many meetings and conferences have been held to discuss security issues as well as solutions. Apart from this, researchers and practitioners have also presented some security solutions related to SDNs through authentication mechanisms and policy conflict resolutions. However, there is a need for an further degree of attention in order to achieve SDN deployment in data centers or individual organizations.

The objective of this research is to present a comprehensive systematic literature review related to security and privacy issues on SDN planes. This SLR provides contributions from four perspectives:

- This review presents all major security attacks on SDN planes, including the application plane, control plane, and data plane.
- The SLR identifies the approaches used by researchers and industry experts to present security solutions for SDN attacks on planes.
- Moreover, SLR also presents a security model after identifying malicious attacks on the SDN application plane, control plane, and data plane.
- Additionally, we also present challenges and research gaps as well as suggest future research directions to produce a sustained solution for SDN security.

II. RELATED WORK

The decoupling of the data plane and control plane represents an excellent future for networks, but it has brought new security challenges into existence. For example, the communication channels can be targeted between isolated planes in order to impersonate one plane to attack the other. Moreover, the control plane is also more appealing to vulnerable attacks due to its visible nature, such as DoS and DDoS attacks. In addition, the SDN controller will also down the whole network if there is any security compromise. Security challenges in SDN are growing gradually with the deployment of its technologies in different areas. Therefore, it is necessary to highlight the security issues so that required security measures can be properly taken in order to obtain the full advantages of SDN. In this section, we have identified the security vulnerabilities at different SDN layers. To describe the security issues in SDNs, Kreutz et al. [13] presented threat vectors, which demonstrated that there is no persuasive mechanism for building a trusted relationship between applications and the controller in SDNs. Thus, forged traffic flows can be injected into controllers and switches that can be triggered by a malicious user. In this way, an attacker will use network elements such as servers, switches, and computers to generate a DoS attack. Similarly, attacks on vulnerabilities in controllers and switches can wreak havoc on the network; therefore, malicious controllers compromise the whole network. The prevention of DDoS attacks has been a primary concern for researchers and network security administrators [14,15,16,17]. DDoS attacks are highly frequent; therefore, it is necessary to develop robust solutions that are effective in detecting and mitigating DDoS attacks [18,19]. From the literature, it can be seen that a DDoS security mechanism must be able to prevent attacks from within and outside the network [20].

Schehlmann et al. [21] presented an evaluation methodology for SDN security and a comparison with other conventional networks. SDN security measurement criteria consist of authenticity, availability, confidentiality, consistency, and integrity. Although authors argue that a number of attacks in SDN can also exist in conventional networks, they have not explored attacks on SDN layers and their impacts on the overall SDN architecture.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Abdulkarem et al. [22] have identified the DDoS attack in the SDN data layer and proposed a solution for attack detection and mitigation by implementing python language. Moreover, the central controller is one of the most vulnerable components of SDN architecture due to weak authentication, information disclosure, and incomplete encryption. Hence, if the controller on the control plane is not properly secure, then the entire network will be badly affected [19]. Switches have the weakest performance in terms of hardware because an attacker attacks communication channels in order to destroy the link between switches and controllers. According to OpenFlow, standard switches will be changed into the standalone mode or fail-secure mode [23]. Further, the multi-controller implementation will divide the whole network into multiple networks, which leads to consistency and privacy issues [24]. However, the consistency and legitimacy of flow rules are the major security issues in the data layer. During the release process, malicious tampering or transmission delays cause inconsistency issues to take place between switches and controllers [25].

Furthermore, the northbound interface also faces a number of security challenges, the biggest security vulnerability at this interface is standardization [26,27,28]. There is no consistent provision regarding authentication and authorization methods due to diversity as well as regular updates in SDN applications. By exploiting the programmability and openness of the northbound interface, an attacker can launch the attack and access the important resources in the control to change or occupy the network status. In the past few years, studies have focused on passive differential power analysis (DPA) and active differential fault analysis (DFA) by measuring the consumption of power of one or more operations. However, some attacks are considered side-channel attacks in order to obtain patterns from extracted information [29].

Moreover, the southbound interface also suffers different security attacks due to the leakage of open flow protocols, because open flow uses TLS/SSL protocol for data encryption, which is not secure [30,31,32,33,34,35]. Additionally, the southbound interface also faces data leakage, controller spoofing, eavesdropping, and many other security attacks. Scott-Hayward et al. [36] presented a comprehensive survey on different security challenges in SDNs and identified the proposed solution as well as describing the holistic approaches that are necessary for SDN security. Ahmad et al. [37] identified the security threats in SDN at the application plane, data plane, and control plane along with security platforms that can secure each plane from different attacks. Table 1 shows already published SLRs, highlighting the contribution of our research. We have compared our defined research questions with already available solution where ✓ symbol indicates the matched contribution of the study and × symbol shows the gaps of their study.

III. RESEARCH METHOD

The primary objective of a SLR is to present inclusive knowledge from the literature in the research field in an organized and holistic way. Apart from that, a SLR can also help to identify existing research gaps as well as the consequent recognition of avenues for research in the future. In this section, we define the method used to conduct this SLR. The method involved research questions (RQ), search string, data sources, eligibility criteria (inclusion and exclusion criteria), screening and selection process, and quality assessment (QA) criteria.

3.1. Research Questions

The objective of this SLR is to provide a comprehensive review of security and privacy issues in SDNs. Therefore, we designed seven research questions in the first phase of this SLR. We evaluated the security attacks/threats on SDN layers/planes and proposed solutions for those attacks. The RQs are given in **Table 2** with their corresponding motivations.

3.2. Search String

The search was conducted at the start of December 2020 by applying the search string to different databases. We applied the search string via the Boolean operators “ANDs” and “ORs” as follows: (“Software Defined Networks” OR “SDN”) AND (“SDN security” OR “SDN threats”) OR (“SDN Security Solutions” OR “SDN Layers”).

3.3. Data Sources

The next phase was to search for the source references. In this phase, multiple search terms were implemented, such as search keyword, search source, relevant papers selection, and filtering. The main research was carried out by looking at the keywords, paper titles, and abstracts for each paper or journal. There were four types of publication, namely journals, conferences, symposiums, and reports. The obtained results from each database are shown in **Figure 2**. The

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

digital search process was carried out by implementing the search query in seven different databases. The chosen databases were:

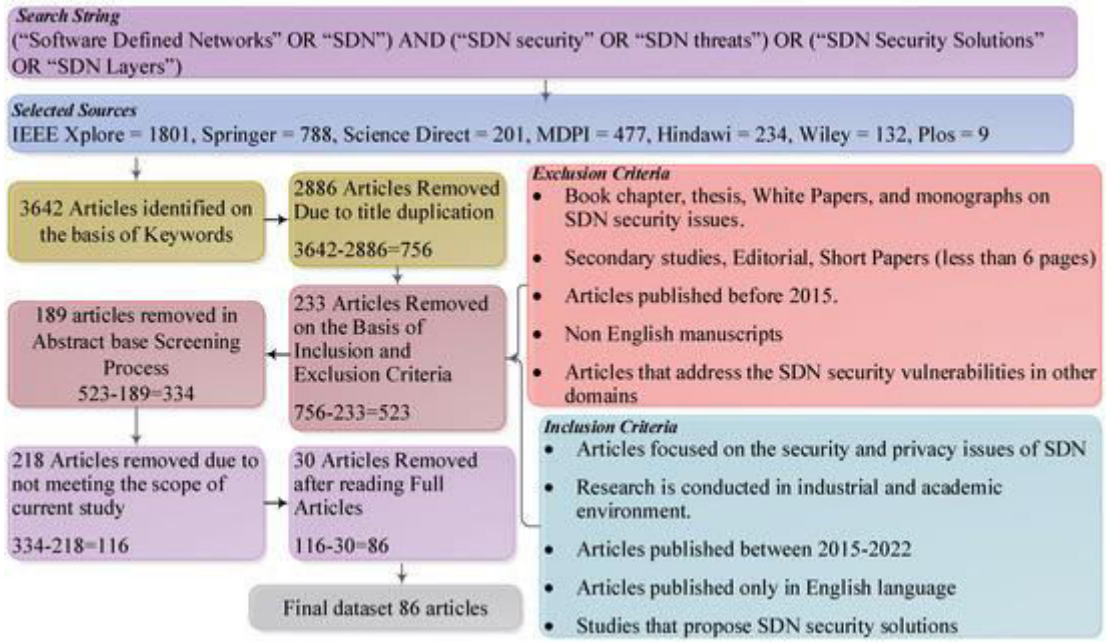

Figure 2. Selection and screening process

- IEEE Xplore (**ieeexplore.ieee.org**) in 1 April 2023.
- Science Direct (**sciencedirect.com**) in 2 January 2023.
- Springer (**springerlink.com**) in 1 February 2023.
- Hindawi (**hindawi.com**) in 15 February 2023.
- MDPI (**mdpi.com**) in 25 February 2023.
- Plos (**plos.org**) in 15 April 2023.

IV. CONCLUSIONS

A systematic review has been presented by providing a comprehensive discussion based on collected studies available in the field of SDN security and privacy issues. In this research, we highlighted the security issues of the application plane, control plane, and data plane of SDNs and presented a taxonomy of attacks. We also identified the causes of attacks on the basis of their impacts. Thereafter, we summarized the existing security solutions for these planes that were proposed by researchers. Based on the identified security issues and solutions, a collaborative security model was proposed. Then, we presented some ongoing security challenges and gaps on SDN planes. Lastly, we provided suggestions for future research that may be beneficial for researchers to mitigate security attacks on SDN layers. Such an extensive systematic review will surely help researchers and policymakers to provide more reliable and robust security solutions in SDNs.

REFERENCES

1. Raghavan, B.; Casado, M.; Koponen, T.; Ratnasamy, S.; Ghodsi, A.; Shenker, S. Software-defined internet architecture: Decoupling architecture from infrastructure. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks, Redmond, WA, USA, 29–30 October 2012; pp. 43–48. [Google Scholar]
2. Jain, S.; Kumar, A.; Mandal, S.; Ong, J.; Poutievski, L.; Singh, A.; Venkata, S.; Wanderer, J.; Zhou, J.; Zhu, M.; et al. B4: Experience with a globally-deployed software defined WAN. *ACM SIGCOMM Comput. Commun. Rev.* 2013, *43*, 3–14. [Google Scholar] [CrossRef]

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. Natarajan, S.; Ramaiah, A.; Mathen, M. A software defined cloud-gateway automation system using OpenFlow. In Proceedings of the 2013 IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, CA, USA, 11–13 November 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 219–226. [Google Scholar]
4. Patel, P.; Bansal, D.; Yuan, L.; Murthy, A.; Greenberg, A.; Maltz, D.A.; Kern, R.; Kumar, H.; Zikos, M.; Wu, H.; et al. Ananta: Cloud scale load balancing. *ACM SIGCOMM Comput. Commun. Rev.* 2013, *43*, 207–218. [Google Scholar] [CrossRef]
5. Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Pérez-Díaz, J.A.; Zareei, M. Towards security automation in software defined networks. *Comput. Commun.* 2022, *183*, 64–82. [Google Scholar] [CrossRef]
6. Jammal, M.; Singh, T.; Shami, A.; Asal, R.; Li, Y. Software defined networking: State of the art and research challenges. *Comput. Netw.* 2014, *72*, 74–98. [Google Scholar] [CrossRef]
7. Hong, S.; Xu, L.; Wang, H.; Gu, G. Poisoning network visibility in software-defined networks: New attacks and countermeasures. In Proceedings of the NDSS, San Diego, CA, USA, 8–11 February 2015; Volume 15, pp. 8–11. [Google Scholar]
8. Kreutz, D.; Ramos, F.M.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. *Software-Defined Networking: A Comprehensive Survey*; IEEE: Piscataway, NJ, USA, 2014; Volume 103, pp. 14–76. [Google Scholar]
9. Lee, S.; Yoon, C.; Lee, C.; Shin, S.; Yegneswaran, V.; Porras, P.A. DELTA: A Security Assessment Framework for Software-Defined Networks. In Proceedings of the NDSS, San Diego, CA, USA, 26 February–1 March 2017. [Google Scholar]
10. Lee, S.; Kim, J.; Woo, S.; Yoon, C.; Scott-Hayward, S.; Yegneswaran, V.; Porras, P.; Shin, S. A comprehensive security assessment framework for software-defined networks. *Comput. Secur.* 2020, *91*, 101720. [Google Scholar] [CrossRef]
11. Voellmy, A.; Kim, H.; Feamster, N. Procera: A language for high-level reactive network control. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, Helsinki, Finland, 13 August 2012; pp. 43–48. [Google Scholar]
12. Dhamecha, K.; Trivedi, B. SDN Issues A Survey. 2013. Available online: https://www.researchgate.net/publication/269667437_SDN_Issues_A_Survey (accessed on 5 June 2023).
13. Kreutz, D.; Ramos, F.M.; Verissimo, P. Towards secure and dependable software-defined networks. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, Hong Kong, China, 16 August 2013; pp. 55–60. [Google Scholar]
14. Deepa, V.; Sudar, K.M.; Deepalakshmi, P. Detection of DDoS attack on SDN control plane using Hybrid Machine Learning Techniques. In Proceedings of the 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 13–14 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 299–303. [Google Scholar]
15. Aladaileh, M.A.; Anbar, M.; Hasbullah, I.H.; Chong, Y.W.; Sanjalawe, Y.K. Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller—A Review. *IEEE Access* 2020, *8*, 143985–143995. [Google Scholar] [CrossRef]

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com