A Review of Security, Threats and Mitigation Approaches for SDN Architecture

Prabhakar Krishnan, Jisha S Najeem

***Abstract*: *The emergence of Software Defined Networking(SDN) is a paradigm shift that re-thinks conventional legacy network design/operations/abstractions and makes future net- works openly programmable, controllable, scalable and afford- able. As a game changer in modern internetworking technologies, SDN is widely accepted by enterprises, with use in domains ranging from private home networks to small/medium scale workgroup networks to corporate backbone to large-scale wide- area cloud networks. Employing SDN in modern networks provides the much-needed agility and visibility to orchestrate and deploy network solutions. But from the security perspectives in terms of threat attack prediction and risk mitigation, especially for the advanced persistent attacks such as DDoS and side channel attacks in Clouds, SDN stack control plane saturation attacks, switch flow table exhaustion attacks - there are still open challenges in SDN environments. In this paper, at first, we present the taxonomy of threats, risks and attack vectors that can disrupt the SDN stack and present various approaches to solve these problems, to deploy SDN securely in production environments. We survey existing research on SDN and the results of our thorough analysis, comparative study of key principles, trade-offs and evaluation of the well-known techniques for SDN security are also presented. To address the key shortcomings and limitations of the existing solutions, we propose our future work a novel framework to effectively monitor and tackle the SDN security issues. Our proposed framework includes a dynamic security se- mantic monitoring system that decouples monitoring from packet forwarding, and offers flexible fine-grained monitoring, which also integrate well with the SDN architecture. This system will employ machine-learning techniques for fingerprinting, accurate detection of behavioral patterns; attack flows and anomalies in the SDN based networks.*

Index Terms*: *Software Defined Networking, SDN, OpenFlow, network security, threat monitoring, IDS, Firewall

I. INTRODUCTION

Software Defined Networking and softwarization of net- working are the widely discussed paradigms in the inter- networking technologies today. SDN is an open network architecture proposed in recent years to address some of the key shortcomings of traditional networks. The proponents of SDN argued that the control logic of the network and network functions are two separate concepts and should therefore be separated in different layers. To this end, SDN hence introduced the concepts of Control plane and data plane: The centralized control plane (from here on, called as controller) manages the network logic, control traffic-engineering functions from the data plane (from here on, called as switch- es) that just take care of forwarding the packets between the networks. So the SDN can be considered as a physically distributed switching framework with a logically centralized control. SDN is designed for provisioning highly dynamic orchestration and quality of service/security policies.Beside SDN related security applications and routing mechanisms applications and mechanisms, current modern networks expect numerous other functionalities and policies ranging from traffic shaping to network virtualization and custom packet processing to quality of service (QoS). Even- though SDN offers powerful features such as: highly scalable programmable interface for networking traffic shaping, dynamically policy enforcement, rapid prototype development, customizable network service chaining,at the same time the architecture comes with inherent limitations and vulnerabilities, the most critical risk being the control plane saturation.The network enterprises have already widely adopted SDN and researchers from both academia/industries are thoroughly analyzing its vulnerabilities and proposing solutions to improve its security and dependability. However, many important security threats, efficient mitigation, detection accuracy, stateful and intelligent data plane mechanisms, offloading the control plane functions to switches and trustworthy aspects of SDN paradigm need more investigation with different approaches.This paper presents our review, comparative study and analysis of security threat detection, defense mitigation mechanisms from prior research. For each of the defense technique, we provide a discussion about the principle assumptions made, scope, advantages and limitations of the proposed defense and mitigation strategy.SDN is a general architectural principle: it broadly defines general guidelines and overall architecture. In this paper, while discussing SDN in real deployments, we refer to specific SDN implementations and OpenFlow protocol as the communication channel between SDN elements, primarily due to its wide adoption in industry (including companies such as Google and Microsoft). However, it is worth noting that all our recommendations, evaluation, considerations and inferences are not specifically tied to any one particular SDN stack/OpenFlow but hold true in general for any open networking standard SDN stack.

Revised Manuscript Received on March 10, 2019.

Prabhakar Krishnan, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University,Amritapuri, India.

Jisha S Najeem, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India.

This paper is organized as : Section I provides an introduction to SDN threat landscape and sets the context, emphasis to advance this research in SDN security Section II presentsthe key Security Threats, Risks and Attack Vectors in SDN architecture, Section III furnishes a time-line of prior research work and detailed evaluation of the related works in SDN security, Section IV mentions some items for future work and conclusion.

II. SECURITY THREATS, RISKS AND ATTACK VECTORS

In this section, we will categorize the threat and attack vectors in SDN architecture of an enterprise network.

While having a logically centralized controller(s) allows improving the policy-deciding process, distributing the policy- enforcement process across the switch(es) introduces new risks and security threats with regard to information disclosure. In legacy networks, the complete network functions get deployed in the form of standalone middleboxes or appliances and hence implemented independently. Hence, realizing autonomous control of configuration and access control policies in the network. In SDN based networks, only the policy-rule enforcement part of the network functions is distributed/delegated throughout the data plane switches.The control operations are executed at the control plane applications and flow-rules are installed to the data plane switches through the OpenFlow channel.

Thus, network policies, traffic shaping, security, QoS functionalities such as IPS, IDS, virtualized network functions(VNFs), bandwidth management, ACLs are managed in the data plane OF switches. The control plane installs the flow-rule/match-action entries, programmed by specific SDN applications running in application plane. Unfortunately, this dynamic programmable behavior can considerably broaden the attack surface of the whole SDN based network.The main axes on which the threat vectors are classified are : a) behavior characteristics, b) based on resources and c) key functional components. The majority of the network-based attacks use techniques such as : 1. Spoofing attacks 2. Man-in-the-Middle attack 3. Tampering 4. Repudiation 5. Information Disclosure 6. Denial of Service - Flooding and Saturating Attacks

The critical security issues include:

- Man-in-the-Middle attacks, spoofing and networktraffic modification attacks in the SDN control channel (OpenFlow). Compromised SDN control plane applications that can mis-configure and com- promise the entire network domain.
- Infecting the network devices/switches (”Flashing firmware with malware, persistent boot-kits, back-door”).
- Forcibly Downgrading device software.
- The trustworthiness of the ”Network Edge Device
- (NED)” or Gateway,
- Are only the user specified Security Application running in the NED and inspecting the traffic? Can the user be sure that no other applications are handling the data?

A general clarification of threats to critical functions/communication channels of SDN stacks, as shown in Fig. 1.

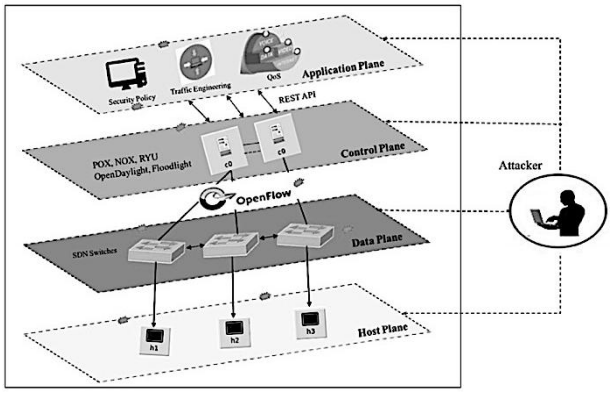

Fig.1Attacker searching for potential targets

We have also examined and categorized the risks consequences of attacks to communication at boundary, interface between layers of the SDN architecture. Our systematic study of risks to SDN is described in the Table.1.

Table.1A Sample Risk Categorization

Risk	Risk Description
Insider	An authorized user performs communication that the temperaments of security policy.
External Attack	An external entity attempting to gain unauthorized access to resources or services.
Data Access	An attacker reads or modifies data in the storage architecture or data at rest by accessing the network or transit.
Data Leakage	Sensitive data is carried out unauthorized users or written to the flash media.
Exloit	An attacker performs a protocol violation causing the system to malfunction.
Malware	Malicious code injected on the network or I/O devices removable wrong impacts of business resources.
Denial of Service	An interaction consumes extreme amounts of storage or network capacity, treatment, denial of service for authorized interactions.
Traffic Hijacking	Illegitimate takeover of routing group addresses by corrupting the routing tables.

III. DEFENSE AND THREAT MITIGATION APPROACHES

When considering potential defense countermeasures, the problem is that the main strength of the SDN architecture the programmability itself is the major vulnerable aspect exploited at will by sophisticated attack campaign. Also, this core pivotal feature of SDN cannot be removed completely as it may nullify the fundamental operation of SDN. So researchers have implemented countermeasures with custom programs or modifications or extensions to SDN elements, but taking advantage of this SDN programmability.

In this section, we analyze and compare approaches that are proposed for securing the SDN Architecture in prior research (Fig.2). Our analysis is based on various evaluation criteria and fundamental attributes of secure communication network Confidentiality, Integrity, and Availability, portability and modifications to existing SDN elements, secure monitoring mitigation overhead, Efficacy of the approach in more sophisticated attack environment.

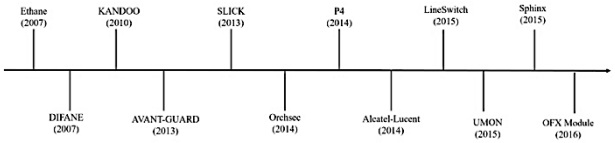

Fig 2 Literature survey on SDN

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

We have classified the SDN threat mitigation countermeasures as: 1. Data plane 2. Control Plane or Controller and 3. Communication channel between Data plane Control Plane, Applications.

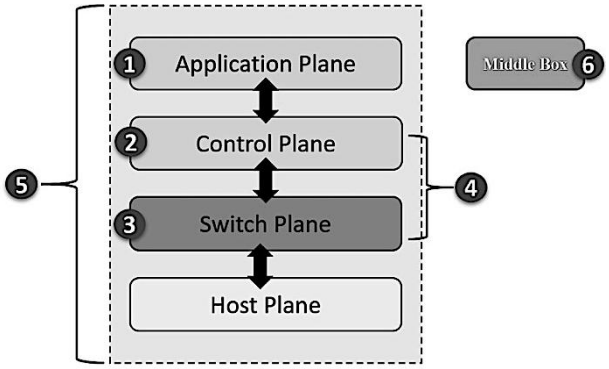

Fig 3.Various Solution Approaches

Discussion on Solution Approaches (Fig.3):

1. Application plane: Running the security monitoring application and interacting with the controller to ensure trust policies, validating the flow rules and enforcement in SDN elements.
2. Control plane: Extending the functionality of controllers and new monitoring and defense mechanisms implemented into the control logic.
3. Data plane: Hardening the switch, by implementing functions in hardware-switching logic or in packet processing logic. Flow tables analytics, connection proxy and migration, DDoS rate-limiting functions.
4. Control-Data Plane Co-operative System Control plane process and switch module interacting through agent processes, some control logic operations offloaded to the switch or creating a intermediate proxy control layer in the switch.
5. Multi-Plane Co-operative Framework - Multi plane/layer co-operative monitoring framework that consists of active probes/sensors that can be implemented in both agent-based and agent-free mode. The management and defense control, chain of trust and policy enforcement are implemented with southbound interfaces (”Openflow, IPFIX, NetFlow, sFlow or SNMP”) Middlebox system Offloading the security aspect to another network device/element in the SDN architecture (similar to IDS) through a standard API such as Openflow/NetFlow.

Various approaches proposed in our literature survey are listed in the Table 2. Here we identify and discuss some recently proposed security monitoring and defence approaches (Fig.3) for SDN Stack.

Table 2.Summary of Security Comparisons at SDN stack

Security Comparison at switch level

Technique	Year	Confidentiality	Integrity	Availability	Attacks
DIFANE	2010	√	√		
FlowChecker	2010	√	√		
KANDOO	2012	√	√		STRIDE, DoS, DDoS, MITM (Man-in-the-Middle)
VeriFlow	2012	√	√		
OF-GUARD	2014	√	√	√	
FlowMon	2015	√	√		
FS-OpenSecurity	2016	√	√	√	

Security Comparison at controller level

Technique	Year	Confidentiality	Integrity	Availability	Attacks
VAVE	2011	√	√	√	
NICE	2012	√	√		Hijacked/Rougue Controller, Malicious Applications
Fort-NOX	2012	√	√	√	
FRESCO	2013	√	√	√	
FlowGuard	2014	√	√		
SE-Floodlight	2015	√	√	√	
FS-OpenSecurity	2016	√	√	√	

Security Comparison at Communication Channel

Technique	Year	Confidentiality	Integrity	Availability	Attacks
FlowVisor	2010	√	√		DoS/DDoS, Control-Data Link Plane Attacks(MITM, Black-hole), Buffer Saturation Attack
AVANT-GUARD	2013	√	√	√	
LineSwitch	2015	√	√	√	
UMON	2015	√	√		
SPHINX	2015	√	√		
OFX Module	2016	√	√	√	
FS-OpenSecurity	2016	√	√	√	

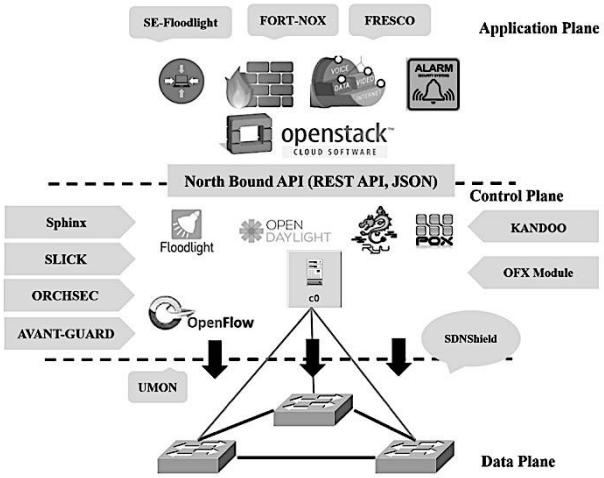

Fig 4.Different approaches for securing SDN Architecture

A. DIFANE

Existing network mechanisms rely highly on SDN controllers, results in scalability issues and performance degrades. The first proposal that came is DIFANE (Doing it Fast and Easy)[1], a scalable distributed flow based novel architecture that provides an efficient result keeping track of the network flow in the data plane, by extracting particular or critical flows through the intermediate OpenvSwitch(es) that store particular flow rules. The DIFANE architecture encapsulates a distributed controller integrated with an authority switches that act as a subset of the existing SDN OpenvSwitch in the network or legacy switches(including ingress/egress switches) incorporating colossal memory and processing capability. Once the traffic received from the ingress port of the host, if ”match/action” fails in OpenFlow pipeline on the switch ,the ”ingress switch” forwards that packet to corresponding ”authority switch”. The authority layer switch checks with the cached flow tables and replies with the matching action rule to ingress switch. The subsequent packets of that flow will match this flow rule and so forwarded directly to the egress switch, in the fast path.

B. AVANT-GUARD

Shin et al.,[2] introduced AVANT-GUARD to the SDN Switch (OVS) called OpenvSwitch, another countermeasure for attacks on control plane integrates two modules : (1) ”connection migration” technique deployed in the OF switches to detect ”TCP SYN” flooding attacks. (2) actuating trigger continuously notify the network status and prior information about the payload and headers to the control plane. The above method shielded the control plane from TCP SYN floods but opened up a vulnerability to buffer attacks.

C. LineSwitch

LineSwitch[3], solution at the data plane switch level, their implementation approach improves on AVANT-GUARD on 2 aspects:1. efficient buffer-overflow detection mechanisms and 2.less connection state management for proxy, using delayed TCP connection migration method.

D. OpenFlow Extension Framework (OFX)

Motivated by customized OpenFlow extensions and modules by Avant-Guard came another framework OFX module. AVANT-GUARD and LineSwitch has performance, overhead and deployment challenges. OFX [4] enables dependable SDN applications within an existing OpenFlow infrastructure, by dynamically loading software modules that includes security applications such as BotMiner, DDoS Detector etc. This OFX modules contains OFX library as a prerequisite to perform specific network monitoring tasks that emphasis as a new security functionality enabling data plane OFX agent to handle the module packets.

E. KANDOO

Another vulnerability that limit the OVS includes over-heads due to concurrent incidents in the data plane. Hence requires a new framework KANDOO[5], which guarantees a configurable and scalable secure control plane, that maintains the scalability issues by not altering the SDN switches. With efficient offloading of control applications by splitting the control plane into two layers. The KANDOO framework aggregates bunch of flow table functions in a pseudo control lower layer and distributes the control functions in the upper layer of the control plane. While maintaining the state of the art, KANDOO’s framework allows operators to replicate existing controllers in the SDN based network, on the fly and this could lead to inconsistent bottlenecks.

F. Flood Guard

One among the major drawback in AVANT-GUARD was the buffer saturation attack between control-data plane.To

secure SDN networks from such attack FLOODGUARD [6] is a defense mechanism framework which does efficient protocol- independent flow pattern analysis proactively. It employs packet migration technique in order to protect the controller overload and control plane saturation, by temporarily storing the packets (that resulted in table-miss) in the SDN controller using Threshold rate limit algorithms.

G. Open Source SDN Project DELTA

This project’s key objectives to build a automation frame-work were: i) to execute offensive test case scenarios to-wards various entity/element in SDN domain. ii) assisting to do penetration testing , vulnerability assessment of a SDN network and discover new attack vectors. Actuated by the existing penetration testing tools for traditional networking, DELTA is considered to be one of the prior works envisaged for bench-marking the SDN devices integrated with specific fuzzing techniques to determine concealed security flaws.

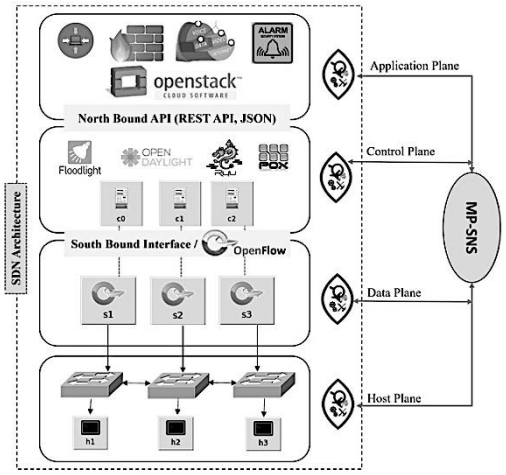

Fig 5.Conceptual Deployment scheme of MP-SNOS

IV. FUTURE WORK

To address the key shortcomings and limitations of the existing solutions, we propose our future work a novel framework to effectively monitor and tackle the SDN security issues. Our proposed framework (Fig.5) called *Multi Plane Framework for SDN Operations Security(MP-SNOS)* includes a dynamic security semantic monitoring system that decouples monitoring from packet forwarding, and offers flexible fine-grained monitoring, which also integrate well with the SDN architecture.More advanced defense mechanisms and mitigation approaches are needed to tackle these impending threats to the network and hence we envisage developing a open networking standard-based framework for dynamic security monitoring and defense.By basing decisions on multiple behavioral observations rather than a single event, our threat analytics engines analyze multiple data security layers and multiple pieces of information at the network, switching, control plane, protocol, application layers to identify and block even the most sophisticated attacks.

In traditional networks, traffic monitoring is typically done at routers or middle-boxes, with the collected information being reported to a central collector where the network management applications are running. In Modern dynamic networks, numerous security-monitoring systems based on programmable SDN are available, but it is difficult to evaluate how they perform, especially in large-scale networks. For the SDN traffic security monitoring we propose to develop a system that decouples monitoring from forwarding, a fine-grained network flows monitoring, which is an important capability for effective real time detection of security threats attacks.

This should offer flexible, dynamic and fine-grained flow-based monitoring that integrates well with the current SDN architecture. We are also investigating applications, which can utilize such a distributed SDN security-monitoring framework.

The role of this framework will be to provide monitoring and security at each layer and interface. The key security aspects include: access control,data protection and detection of network attacks such as Denial-of-Service, Spoofing, session hijacking, network protocol poisoning, topology tampering and information disclosure scanning, etc.

In our future work, we will apply machine-learning techniques for accurate detection of behavioral patterns, finger- printing, attack flows and anomalies in the SDN based net- works. These ML/Deep learning-based anomaly detection algorithms can be employed in the SDN control plane for behavioral analysis and traffic based anti-spoofing techniquesfor monitoring the communication channels in the SDNarchitecture. E.g. The Northbound Interface between Controller-Applications,TheSouthbound Interface Openflow protocol between Controller-Switch.

In real word large networks, there can be complex inter-connected network topologies that consist of a root-network and several sub-networks, each network with separate network policies. In such scenarios, as the Attacker scans learns the entire network configuration for staging an attack through side- channels or northbound/southbound channels, the framework should have multi-criteria flow analyzer that can process data from many switches, detect and prevent such attacks.

We also plan to develop reference hardened secure SDN-stack, Security application modules and conduct experiments. We will measure the efficacy of this framework in terms of network resources, Meta data flow database, acceptable memory and computational overhead for analytics, latency and other resource usage during attack time and also demonstrate the capabilities, in real world network management.

V. CONCLUSION

SDN is one of the most active developing technology, along with other virtualization and softwarization of networking, especially to address traffic engineering, network orchestration, QoS and Security. Despite significant research efforts, to the best of our knowledge very few works have addressed the security threats and attack vectors at all planes, the tradeoff between performance and fine-grained monitoring, dependability on SDN, to build a cooperative security frame- work for the whole SDN based network.

In this paper, we presented a comprehensive study of the vulnerabilities, threats and risks in the SDN architecture, in various real-life scenarios. We also proposed a novel framework that makes use of fine-grained security networksemantic monitoring to detect and defend the SDN based networks. To secure a large farm of IoT device network in the cloud, we must enumerate all possible vulnerabilities and attack vectors and build a model that can predict the attacks. We have to design programmable features of SDN for more processing/analytics at the edge, context-awareness and situational awareness, more flexible reconfiguration of devices or removal of insecure devices. Undoubtedly, modeling and verifying networks is still a great challenge and we will explore how to investigate different properties of SDNs with appropriate formal methods.

REFERENCES

1. M. Yu, J. Rexford, M. J. Freedman, and J. Wang, “Scalable flow-based networking with difane,” ACM SIGCOMM Computer Communication Review, vol. 40, no. 4, pp. 351–362, 2010.
2. S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Avant-guard: scalable and vigilant switch flow management in software-defined networks,” in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 413–424.
3. M. Ambrosin, M. Conti, F. De Gaspari, and R. Poovendran, “Lineswitch: Efficiently managing switch flow in software-defined networking while effectively tackling dos attacks,” in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015, pp. 639–644.
4. J. Sonchack, A. J. Aviv, E. Keller, and J. M. Smith, “Enabling practical software-defined networking security applications with OFX,” in Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS), 2016.
5. S. HassasYeganeh and Y. Ganjali, “Kandoo: a framework for efficient and scalable offloading of control applications,” in Proceedings of the firstworkshoponHottopicsinsoftware-defined-networks. ACM,2012, pp. 19–24.
6. H. Wang, L. Xu, and G. Gu, “Floodguard: a dos attack prevention extension in software-defined networks,” in Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Confer-ence on. IEEE, 2015, pp. 239–250.
7. K.-y. Chen, A. R. Junuthula, I. K. Siddhrau, Y. Xu, and H. J. Chao, “Sdnshield: Towards more comprehensive defense against ddos attacks on sdn control plane,” in Communications and Network Security (CNS), 2016 IEEE Conference on. IEEE, 2016, pp. 28–36.
8. R. Bifulco, J. Boite, M. Bouet, and F. Schneider, “Improving sdn with inspired switches,” in Proceedings of the Symposium on SDN Research. ACM, 2016, p. 11.
9. M. G. B. A. Nair, Mol and Nair, “A mediator based dynamic server load balancing approach using sdn,” in International Journal of Control Theory and Applications, 2016, pp. 6647–6652.
10. M. Conti, F. De Gaspari, and L. V. Mancini, “Know your enemy: Stealth configuration-information gathering in sdn,” arXiv preprint arXiv:1608.04766, 2016.
11. Y. Sung, P. K. Sharma, E. M. Lopez, and J. H. Park, “Fs-opensecurity: A taxonomic modeling of security threats in sdn for future sustainable computing,” Sustainability, vol. 8, no. 9, p. 919, 2016.
12. P. Krishnan and J. Najeem, “A multi plane network monitoring and defense framework for sdn operational security,” in International Conference on Operating System Security (ICOSS 2017), 2017.
13. Krishnan, Prabhakar, Jisha S. Najeem, and Krishnashree Achuthan. "SDN Framework for Securing IoT Networks." In International Conference on Ubiquitous Communications and Network Computing, pp. 116-129. Springer, Cham, 2017
14. Karthik Raghunath, Krishnan Prabhakar, "Towards A Secure SDN Architecture”,2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)
15. Krishnan Prabhakar, Achuthan Krishnashree, "Managing Network Functions in Stateful Application Aware SDN”, 6th International Symposium on Security in Computing and Communications (2018), Springer Communications in Computer and Information Science Series(CCIS), ISSN: 1865:0929