Security in OpenFlow Enabled Cloud Environment

Abdalla Alameen
Computer Science Department, College of Arts and Science, Prince Sattam bin Abdul Aziz University
Wadi Adwasir, KSA

Bhawna Dhupia
Computer Science Department, College of Arts and Science, Prince Sattam bin Abdul Aziz University
Wadi Adwasir, KSA

Sadia Rubab
Computer Science Department, COMSATS Institute of Information Technology,
Attock Campus, Pakistan

Manjur Kolhar
Computer Science Department, College of Arts and Science, Prince Sattam bin Abdul Aziz University
Wadi Adwasir, KSA

***Abstract*—Inception of flow tables as data plane abstraction, and forwarding rules that are managed by centralized controllers in emerging Software Defined Networks (SDN) has stemmed significant progress in OpenFlow based architectures. SDN is particularly fueled by data center networking and cloud computing. OpenFlow coupled with cloud solutions provide dynamic networking capabilities. With the benefits obtained from network services, security enforcement become more important and need powerful techniques for its implementation. Extensive researches in cloud security bring forward numerous methods of leveraging the SDN architecture with efficient security enforcement. The future of SDN and mobile networks is also enlightened if security models are satisfactory to cover dynamic and flexible requirements of evolving networks. This paper presents a survey of the state of the art research on security techniques in OpenFlow based cloud environments. Security is one of the main aspect of any network. A fair study and evaluation of these methods are carried out in the paper along with the security considerations in SDN and its enforcement. The security issues and recommendations for 5g network are covered briefly. This work provides an understanding of the problem, its current solution space, and anticipated future research directions.**

Keywords*—Software defined networks; OpenFlow; 5G network component; ONF; virtualization; SDN security framework; future security networks

I. INTRODUCTION

Cloud computing cannot adequately handle the increased demands of its customers with the traditional network management techniques. Network devices are complex devices, which require individual configuration to change the network behavior. Therefore, to achieve high level of connectivity and communication, cloud computing deployment architectures are propelled by Software Defined Networks (SDN). SDN is introduced as a flexible way to control network in a more sophisticated and planned manner, with OpenFlow as the most commonly used SDN protocols [29]. SDN with centralized control on the network devices, make network open and programmable. Instead of configuring the network devices individually, an administrator can program the behavior of a network centrally. The organizations can develop and install applications for specific network behaviors. These applications can be for security, traffic engineering, QoS, switching, routing, virtualization, load balancing and many others based on network evolution and new innovations. The core of SDN is to introduce flexibility that evolves with the speed of software. SDN is an enabling technology for 5G [53]. SDN with separated control and forwarding plan has also been applied in wireless networks [54]. The SDN architecture is presented in Fig. 1. The OpenFlow acts as an interface between the control plane and forwarding layer. Section I of the paper gives a brief introduction of SDN and related work. In Section II of the paper Dynamic Cloud Network Management is discussed, which includes various virtualization techniques and its implementation. It also explains the scope of cloud services in a virtualized environment. Section III of the paper elaborates the types of security considerations in SDN and their enforcement in various layers of SDN. Section IV deals with the detail regarding cloud security and OpenFlow. A brief discussion about the security in future network is also added in the last section of the paper. To start with, next section is regarding the OpenFlow based SDN.

A. OpenFlow based SDN

The OpenFlow is a network control protocol maintained by Open Networking Foundation [1]. SDN concept decouples the control plane from the data plane, whereas OpenFlow define the rules for the communication between the controller and a switch [4]. While managing the network traffic, OpenFlow generates a flow table. The OpenFlow table contains match, priority, counters, instruction, time-outs and cookie fields. All these fields work together to identify and manage network traffic [30]. SDN implemented on OpenFlow offers many advantages for cloud environments. The OpenFlow in SDN can be programmed to streamline the network traffic with high security feature. SDN increase the network visibility of the devices offered, as the control is centralized and it can view both the real and the virtual devices. Full view of the resources facilitates the resource optimization; hence increase the elasticity of the cloud.

OpenFlow defines rules for packet forwarding in OpenFlow switches, describes rules for flow tables and handles the delivery of data packets from one location to another. The statistics about the traffic passing through the OpenFlow switch can be reviewed from flow tables. OFPacketIn,

OFPacketOut and OFFlownod are frequent OpenFlow events to which controller can listen and respond back. The OpenFlow protocol is accepted by many major switches and the routers manufacturing company to support and deliver products compatible with OpenFlow protocol.

B. Redefined Cloud Network with OpenFlow

Open Networking Foundation (ONF) is the group who is working extensively in the field of dynamic networking architecture via SDN technology. Introduction of OpenFlow based SDN changed the way of networking in a cloud environment. SDN redefined the cloud network to meet the price, performance, scalability and dynamic demand of the clients for cloud services. The solution offered by the SDN is the mix of intelligence and flexibility of routing techniques with a higher capacity of integrated application. This concept supports the programmable control interface which decouples and abstracts the control plane from the data plane [29]. With the introduction of SDN, control of the resources gets centralized which exponentially decrease the cost of the hardware infrastructure and cost of management of the network. OpenFlow switch permits selective forwarding of data based on inputs from the controller, which decreases the unwanted traffic in the network. The OpenFlow based SDN architecture allows devices to be programmed according to the need of the client [1], [30]. The cloud service providers can use SDN applications to supervise network conditions, provisioning of network resources and network flow traffic to increase the performance, security and quality of service in the cloud. In the OpenFlow network environment, the functionalities to control the devices are programmed in the control box and data packet forwarding behavior is handled by the central controller for all the devices. SDN control plane supports the traditional feature as well as latest functionalities introduced by the OpenFlow based SDN techniques [30].

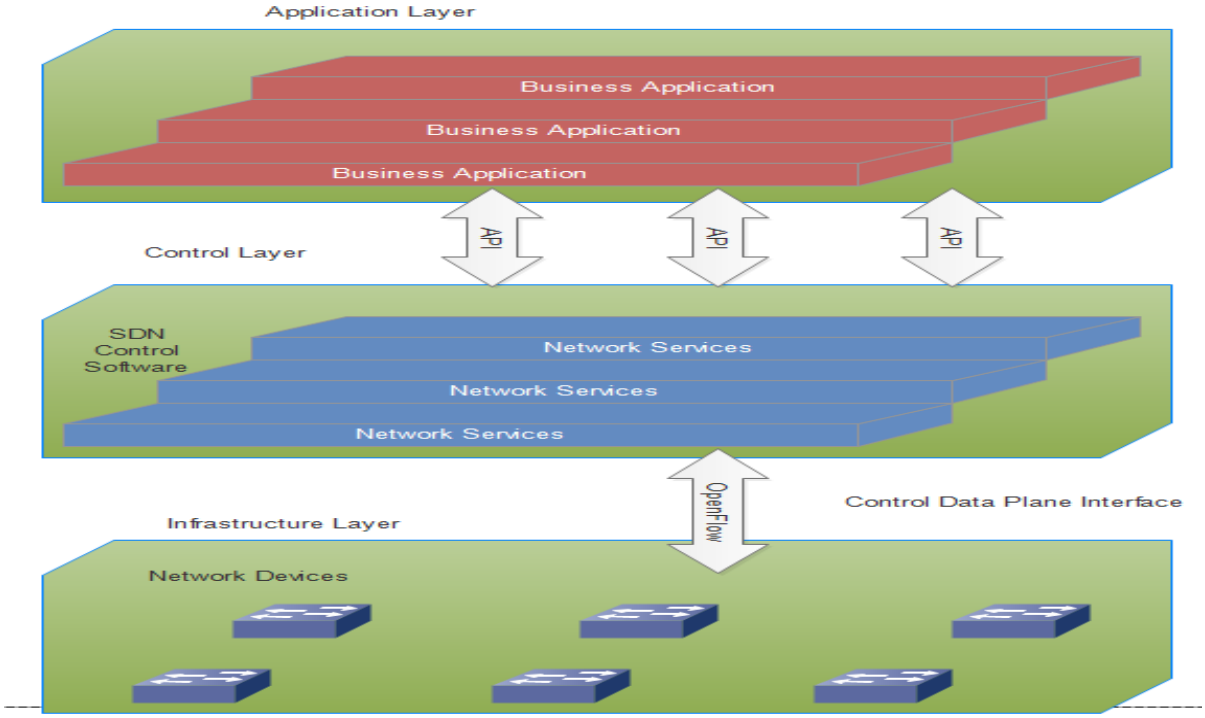

Fig. 1. Openflow based SDN architecture.

II. Dynamic Cloud Network Management

Traditional cloud providers allow user to customize the facilities like, operating systems, hardware specification, storage and execution environment, however, they do not allow them to customize client's network environment. Virtual Private Cloud is an implementation of dynamic networking services. It permits users to develop network topologies to suit their requirements, with dynamic generation IP addresses, which facilitates dynamic IP addresses [5]. SDN supports virtual network services and simplifies data center infrastructure through dynamic connection between VMs and servers with resources.

Introduction of OpenFlow based SDN in cloud networks improved the security, scalability and portability of the resources in the cloud. It gives client exact location of the physical resource shared in the cloud. In OpenFlow based networking environment, networking hardware itself act as a firewall. Network switches are programmed with OpenFlow rules to block the unwanted and malicious traffic in the network. To fulfill the increased demands of customers, scalability feature is improved with the help of dynamic networking [5], [6].

The main drivers for dynamic network virtualization are fast network, higher efficiency in utilizing the network resources and cost reduction. In dynamic network first requirement is the virtualization of the data center networks (DCN). Hence, the network virtual layer which is also called hypervisor is developed to virtualize the network resources to make a pool of network devices like, switches and routers

[7]. The hypervisor provides an actual mechanism to implement the functional network virtualization. The hypervisor's job is to fulfill the demands of clients by managing resources effectively. A multiple module virtual environment can have multiple hypervisors that can be used to provision and manage the resources available in the cloud [8].

A. Virtualization: Network of Virtual Machine Instances

Virtualization has a great impact on IaaS solutions of cloud service providers. Some examples of IaaS solutions are Nimbus, Open Nebula, Eucalyptus and Open stack [8]. Infrastructure virtualization separates the data plane from the control plane. A virtual infrastructure is defined by virtualizing the various physical resources and control programs on the data plane for provisioning. Each virtual infrastructure has its private set of control application programs within the control server. The users can choose the programmed control modules to prepare their customize environment, which includes, routing, network management, virtual machine migration control and so on [9].

OpenFlow, Open vSwitch, OpenNebula and One Cloud are the SDN based technologies used to implement the virtualization in the cloud. Open vSwitch is implemented through standard management interfaces such as, sFlow, NetFlow and can be customized programmatically. It is used to manage the network traffic between physical hosts and VMs [10]. OpenNebula frameworks are specially designed to manage the virtualized infrastructure which provides private, public and hybrid IaaS. The hypervisor supported by OpenNebula are KVM, VMware and Xen. This provides a centralized management interface for virtual and physical resources. It also supports high extensible plug-in framework management tools like, VM schedulers, virtual image managers to increase the capability of the resources offered [11]. One Cloud allows users to provision virtual machine instances using KVM hypervisor. It is an IaaS system. OpenFlow network and Open vSwitch are used as a virtual bridge to connect all the hypervisors physically.

B. Cloud Services Feasible in Virtualized Network

To improve the performance of the cloud we required to implement the virtualization of DCNs. This makes the cloud services feasible for almost all types of clients. The virtualization of DCNs optimizes the cloud service to its maximum extent. As we discussed above also that the maximum impact of virtualization of network is on the IaaS services. DCNs list all the VMs on DCNs servers so as all the available resources can be utilized at the maximum optimization. The DCNs are also responsible for the maintenance, repairs and addition and deletion of resources into the resource pool on DCN servers [12]. DCN provides connection of hundreds of data centers in such an efficient way, so that cloud computing services can expand easily. It helps to implement the reliable and secure communication between the various services.

III. Security Consideration in SDN

Security is one of the major concerns in computer science as companies, government services and individuals rely on computer networks for their day to day activities. The amount and sensitivity of data stored on network has considerably increased over the time. Viruses, Worms, Distributed Denial of Service (DDoS), Spyware and Trojan Horses the common heard jargons are generally considered as the common types of threats and attacks to network security. DDoS attacks overload the network with too much traffic by sending lots of information on the network. Thus it affects network bandwidth, memory, CPU and so on. If the network goes offline it can cause money and time loss to companies. Most importantly if DDoS takes down servers meant for network security, the whole network is open to the threats and attacks. Attackers try to steal data, they want to ruin the network, or try to use network for unlawful activities. Therefore every connection in network could be an opportunity for attackers. Strong security measures are required that not only protect network users and infrastructure from threats, but also evolve as networks evolve. Effective security not just creates a shield on network, it helps each entity associated with network to thrive and focus with freedom. In the light of given context, this topic elaborated how security has enhanced with SDN platform and cover the security challenges with SDN. SDN that was developed to obtain simplified and secure networking [13]-[18], attain security with dynamic access control, detection and mitigation of attacks and robust traffic monitoring.

A. Security Threats to SDN

SDN is an emerging network technology with flexible and agile environment for network traffic control proposed by many companies and researchers such as [19]-[21]. This novel approach comes across significant issues in availability, scalability and security [22]-[23]. Whenever there is new platform, service or infrastructure hackers try to go into that new option. Since SDN is based on programmable control interface, in SDN how the operators deal with the software has major impact on security. If the administrators and software developers not properly deal with security folks, it could have negative impact on security and result in security gap. If there is any compromise in controller and applications, whole network is affected. Fig. 2 represents the points in different layers that could be target of security attacks in SDN. The attacks on threat points cause forge traffic flow between switches, affect communication between controller and switch.

A physical damage, link failure, or attacks on a vulnerable controller [24]-[25] in worst cases results in paralysis of whole network. With the compromised controller, traffic could transfer to compromised nodes, and hacker could insert malware, monitor traffic and could even modify the packet contents. As in SDN route flows among security devices, the consequence of an affected controller could be very catastrophic. In case the communication between data plane and control plane is not appropriately secured entire network security is compromised. Man in the middle attack (with DNS spoofing, ARP Spoofing, session hijacking etc.) between controller and switch, DoS attacks, reply attacks, dodged network access policy by malicious users and unclear management of encrypted packets are threats to data forwarding plane layer [22], [26]. Whereas DDoS is a threat for control layer [22], [26] and illegal access affects application layer [22]. Effective diagnosis of faults and assurance of speedy recovery in SDN remains a security issue if trusted

resources are not incorporated in infrastructure [27]. A thorough analysis of SDN challenges and threats reveals that still lots of research, investigations and efforts required for transforming this novel techniques into more reliable and secure infrastructure [28].

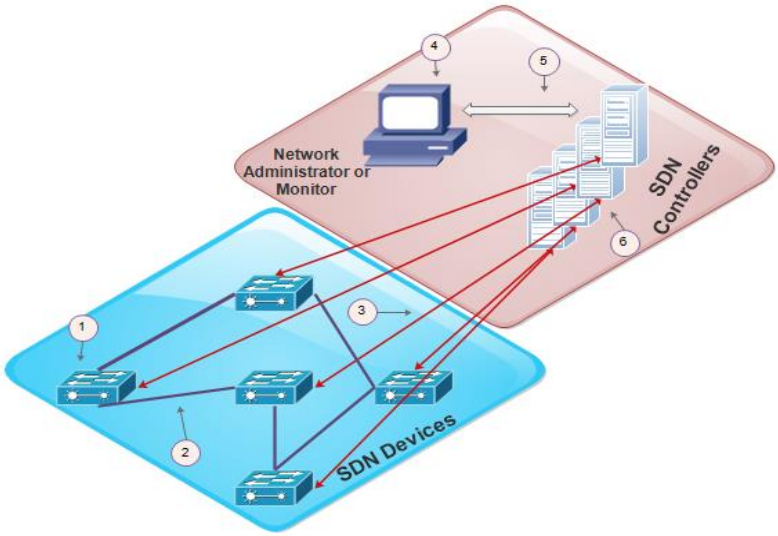

Fig. 2. Threat points in SDN infrastructure.

B. Enforcing Network wide Security Policies

So far, brief introduction of SDN in context of cloud and the concerns regarding the security around SDN is given. The intense research and development in SDN has resulted in dramatically evolving technology with varied security solutions to threats and attacks. The different ways to define and enforce security policies are summarized in this section. The security policy in network is generally defined as the routing rules, or the actions that are allowed or forbidden in the network. Effective security policy improves quality of service (QoS), and filters the traffic. The security policy for information shared in network could be based on measurable documented standards, and procedure for policy enforcement and disaster recovery. Security policies in SDN spread security in the network with better visibility to network traffic, segregation of services in infrastructure, rigorous monitoring of sensitive data and through inspection of suspicious devices.

Careful design and implementation of SDN controllers and their access control policy is strongly required for network security. Dynamic access control framework implemented in Resonance [29], where controller implements policies with programmable switches. In this research controller provide central authentication and compromised host is segregated. A four state architecture that resembles framework elaborated in [29] was presented with high level policy language in [30]. Access control list and polices for NOX controller as core component of flow based policy enforcement discussed in [31]. The issues between access control and high level policies in switch and firewall are tackled in [32]. Security enforcement kernel FORT-NOX designed for role based authentication, conflict detection and resolution and rule based authorization covered in [33]. An interesting feature of [33] is OpenFlow switches are prevented from packet header modification to bypass firewall. Enforcement of security policy support QoS, network monitoring in real-time environment and problem detection [34]-[35]. SDN utilized in [36] for better performance and to resolve traditional network security threats. Network services and security improved in this architecture with validation of sources addresses. Flexible, secure and scalable network management architecture for large scale networks [16] enforces security policy and dynamic load balancing in hybrid network with programmable devices. In FLOWGUARD (a centralized firewall) violations in firewall security policy are detected and resolved with policy enforcement on top of the controller [37]. SIMPLE, the work in [38] introduces resource management, flow correlation and policy manager for sending packets through various middle boxes. Load balancing ensured in SIMPLE while installing the rules (translated middleboxes specific policies) in SDN switches.

The scripting language to add security policy to SDN in conjunction with NOX controller incorporated in FRESCO security framework [39]. Scripting language used in development of security applications. Controller program for monitoring and configuration of policies [40], an advance language for network policies for control architecture Procera [41], and network security policy in human readable language for responding to alerts in OpenSec framework [42] represent few of the research work in policy language.

C. Security Control in Multiple Layers

A review of techniques used to secure network by implementing security policies reveals that security studies are generally layer oriented. Each security solution pays more attention to threats and attacks on some specific layer. In SDN architecture, the three layer architecture is represented as application layer, control layer, and infrastructure layer as shown in Fig. 1. FlowNAC [15] support user authentication and grant rights to the users for network access. Frameworks in [15] and [42], OpenSec designed to deal with the security issues of switches. Switch level security in [42] is improved with spam detection, packet inspection and intrusion detection.

Research work in [16]-[17], [33], [41] provide countermeasures to security issues with control layer. They have more impact on security with automatic user authentication [16], virtual IP allocated to host [17], monitoring with varied granularity [18], avoidance of conflicts in rules [33], and with detection and tracking capabilities [37]. The security of both infrastructure layer and control layer are considered in [13], [29], [36] with DDoS detection, access control and unwanted traffic control respectively. Authors in [39] elaborate security mechanism for control and application layer with threat detection and mitigation.

D. How OpenFlow Enhance SDN Security

OpenFlow as one of the most popular specification of SDN significantly improved network security and reliability. Many of the switches in SDN are now adopted with OpenFlow interface. OpenFlow protocol provides secure communication between switches and controller with SSL and TLS encryption. SDN based on OpenFlow delivers better performance in terms of load balancing, routing, firewall configuration and traffic management [43]. In OpenFlow based SDN it's easy to alter packet flow rules, and now many researchers have introduced it in intrusion detection systems, mobile networks, and wireless sensor networks [44]. With the survey of security solutions for SDN, few research efforts that enhance security of OpenFlow based SDN architecture is being identified.

DDoS attacks detection with NOX controller and OpenFlow switches covered in [13]. OpenFlow Random host mutation [16] uses OpenFlow for IP mutation in SDN. In this approach [24] end host is protected from adversaries through unpredictable and random mutation of host IP. Resonance [29] for dynamic access control and distributed network monitoring uses OpenFlow switches and controllers. FORT-NOX [33] directly implemented on NOX as C++ extension is security enforcement kernel. Prioritization of security rules covered in [33] with southbound API. VAVE platform [36] was presented for OpenFlow architecture and engaged OpenFlow protocol for effective validation of source address. VAVE ensures information privacy and prevents spoofed and forged attack on data that pass through OpenFlow interface. FRESCO [39] a development framework for SDN based security applications incorporate security enforcement kernel that is integrated with OpenFlow controller. Research efforts in [42] provide solution to security challenges in switches with OpenFlow enabled framework.

E. Threats and Vulnerabilities with SDN utilization in Cloud

As discussed in Sections 1 and 2 that SDN and OpenFlow align well with cloud computing due to the scaling and dynamic nature of cloud. Since SDN is a step towards offering dynamic virtualization services to clouds, and fully virtualized data centers, therefore extensive research and development required to have a clear understanding of its security implications. SDN has some related threats and attacks that are either similar to challenges in traditional networks or specific for SDN. The different aspects of security and vulnerabilities with SDN based cloud briefly covered in this section. A detailed discussion on mechanisms elaborated in researches for development of secure OpenFlow based cloud environment covered in Section 4. The opportunities and vulnerabilities related to cloud security with SDN are thoroughly discussed in [45].

A centralized and global view of SDN when employed in cloud environment with multiple tenants and shared resources require well defined boundaries for user privileges and limited functionalities passed on to users. SDN provide better control of VLAN and firewall implementation. In dynamic cloud environment quick response to attacks is very important. Though evolution of SDN evolves virtual machine migration, but appropriate security measures are required to avoid attacks on VM traffic. Reliability of cloud could be a major issue if numbers of SDN controllers are limited. As failure of controller has drastic impact on whole network. Problems of inaccuracy and unreliability in network management problem extend to control plane. SDN with central controller and network switches can enforce policy, but it is not as simple as it seems to be. Defining policies on high level such as in cloud require refined frameworks that ensure security with performance. Any negligence in configuration of security policies may cause data leakage, unauthorized access of controller, modification of flow rules, and data modification [55]. How SDN could help to decrease security risks, or worsens the security risk in cloud environment covered in [55].

IV. CLOUD SECURITY AND OPENFLOW

Though, potentials of SDN for on demand services and applications for the user community cannot be denied. This advancement can induce unpredictable traffic across Cloud network which cannot be eluded by means of traditional approaches. Hence, SDN should equipped with centralized tools to monitor traffic flows so as the security modules of the SDN networks. In this section, the plethora of research work suggested for SDN will be elaborated.

A. Security Frameworks of SDN

In [46], researchers proved that, adversaries passively and actively can fingerprint SDN networks. They have showed probability of fingerprinting of SDN network by means of RTT and packet pair dispersion. SDN never considered impairment confinement policy with respective damage recovery as mentioned by [47].

Control plane guides traffic rules whenever the data plane requires to control network. However, these kinds of scripting policies can harm SDN seriously when the data plane floods the request flow change to the control plane. Furthermore, Cloud computing techniques hide resources, such as physical servers, used processors, and OS from users. This technique enables network admin to divide a single processor into many independent servers. This flexibility also allows migrating server into other machine in case of failure. However, this migration should consider network topology of the failure machine. Because physical sever is connected to the network which won't be moved, moving virtual LAN from one network to other network creates networking issues. However, SDN is relatively new technology and creates new risks. Specifically, compromised network elements can affect the whole SDN architecture because of its centralized approach [47].

Static address assignment to the network always allows the remote users to scan and send the probe to the remote network.

However, because of limitation of DHCP and NAT protocols, yet IP address change is required at random pace and frequently so as to avoid scanning [27]. Nevertheless, this method is not effective for the DDoS and application layer attacks. However, to distinguish between normal traffic and abnormal traffic of huge size is very difficult in a distributed network environment. These challenges are addressed in [13]. They have implemented self-organizing Maps, which are traffic aware unsupervised artificial neural network. These Maps are used to distinguish normal and abnormal traffic flow.

One more daunting task is security monitoring of large scaled network. In [48], they have focused on how to route network traffic for network equipment's than analyzing the network traffic. Yet another, approach in monitoring traffic is Cloud Watchers[39], in this approach, network traffic bypasses to the network security devices by using programing scripts. In [Resonance], they have delegated traffic management to the network devices. Researchers [Resonance] have used programmable network elements to control network traffic. These lower level network switches are programmed to drop and redirect traffic whenever they sense real-time alerts in the traffic. In [49], middle boxes are used to induce network-wide policy enforcement on the outgoing to packets to provide useful information on host and source states.

Scripting network policies on vendor specific network devices is rigorous. Furthermore, these network policies induce configuration complexity apart from latency to adopt dynamic nature of the network traffic. Hence, network policy scripting is challenging process for the dynamic environment of SDN. In [42], an OpenFlow-based security framework is proposed and it allows a network security administrator to generate and apply security policies scripted in English like languages.

However, scripting network policies, such as enforcing RPKI-Based Routing Policy on the Data Plane at an Internet Exchange [50], will remain main concern for the network operators till SDN adopts new patches of security policies. To mention few, IDS is the choice for the network administrator to identify abnormal rate bounds at the control panel. Another set of solution in line with new security policies is to use autonomic trust management solution for SDN [51]. This policy is built on the adaptive trust model which enables requirement, assessment, instituting, and guaranteeing the trust of network elements according to observation measured at the runtime. Network operators can make use of cryptographic models of multiple certification environments between various network subdomains. In [46], they have proposed solution for the adversary attack (injecting probe) on the SDN network by passively or actively collecting traffic exchanged with the SDN network.

In [52], they have proposed API for packet generation for OpenFlow switches. The API for packet generation allows partition between controller's switch and functions, hence allowing the controller to bypass assigned tasks. However, these methods are not tested well for the security concern. In view of this discussion topics has been summarized few SDN security use cases that are essential to conquer security breaches. SDN vulnerable to attacks but these use cases if implemented to some extent harden the security attacks.

- Traffic filtering, the major network elements such as SDN switches can act as firewall so the content that is not permitted is denied.
- DDoS Mitigation, communication between DDoS controller system and northbound API configures controller for a clean traffic pass to destination.
- Network Slicing, logical separation in network by addition of slicing layer between control and data plane with strong isolation.
- Network Access Control, unauthorized access prevented through security checks. Nodes that pass checks can only join network and send /receive data.
- Security Traffic Monitoring, packet monitoring tap to assess the data flow improve security.

B. Security in Future Networks

The rapid progress in networks reveals that in the years 2020 to 2030 almost 100 billion things will be connected with 5G [56]. It means that new approaches are needed while defining the security for 5G to gain the user trust. The features of SDN such as network management and applications management are supportive in getting dynamic nature of 5G. Therefore dynamic and flexible security mechanisms with new trust and delivery models are required. Evolving 5G network architecture is based on SDN for communication between clouds, satellite systems, gateways and other devices. Security, resilience, robustness, privacy, trust and data integrity are main focus of these diverse and functional network environments [57].

The common attacks related to 5G are data manipulation, equipment cloning, rogue devices, unprotected endpoint entry, man-in-the-middle attack, spoofing, and premium content privacy. Most of the attacks can affect all 5G segments and a multilayer security model applicable from network to user guarantee basic security requirements. General 5G network architecture and its layered security vision are depicted in Fig. 3 and 4 respectively.

The ongoing advances and future of cloud computing make it a favorable enabling technique for flexible 5G network. In this exploitation of advanced techniques spectrum, infrastructure, high performance computing will be available as services (anything as a service). In ANYaaS traditional data center services move to mobile connectivity [58], as mobile devices can function as resource providers [59]. OpenFlow operate as standard in SDN enabled mobile networks. But the traditional OpenFlow mechanism is not suitable in mobile networks in terms of security. The impact of attacks on OpenFlow control on SDN based mobile networks are covered in [61]. Proscribed use of frequency, snooping by attackers and privacy issues are the security issues that need to be explored for improved security in 5G networks [53]. The reduced client latency effects users' control over the data and it leads to privacy, authentication and traceability issues.

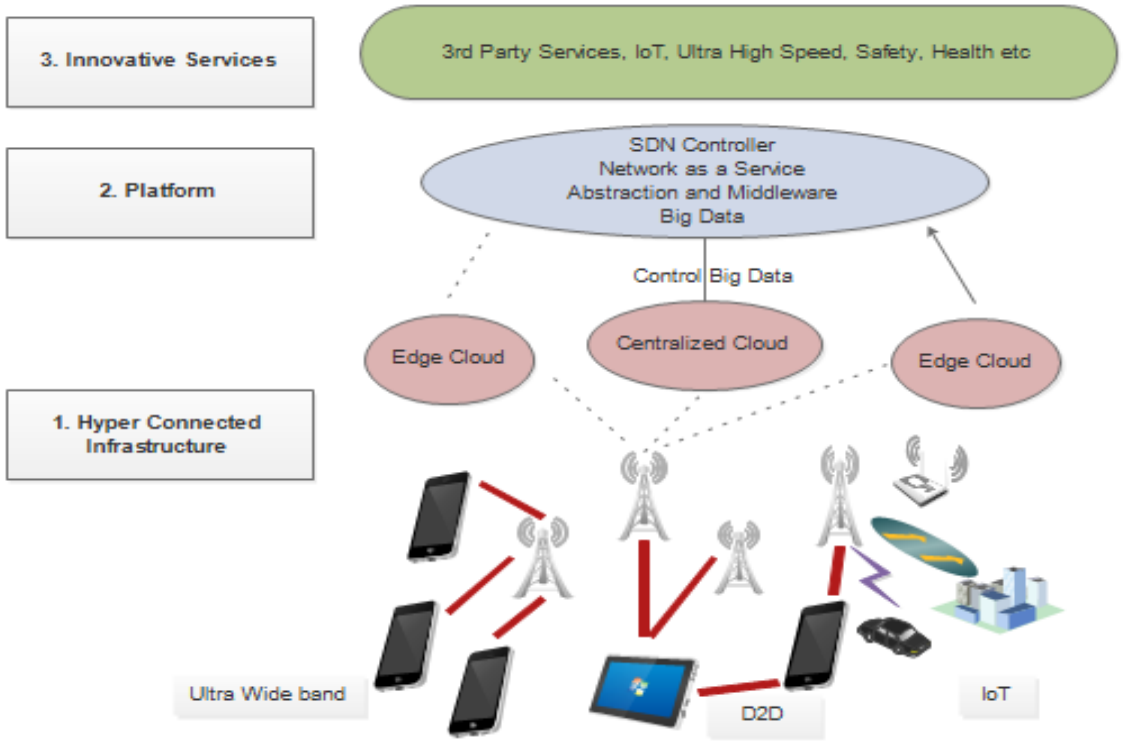

Fig. 3. 5G network architecture.

Intelligent security management, virtual security functions, authentication, authorization and residents isolation build up the concept of virtualized security (v-security) in 5G networks [60]. CHARISMA [60] with extension in OpenFlow protocol, intrusion detection, authentication, cluster encryption at physical layer, virtualization of network layer, and packet inspection defined a security protocol suitable in 5G network architecture. Comprehensive study in [61] on security of mobile networks revealed concerns and possible options to handle these concerns. These both are really important to consider while adopting future network technologies that are evolution of mobile communication. Authors in [62] uncover security breaches that could occur due to DoS/DDoS attacks on control plane, system error or malicious software. The proposed security model in [62] is designed for telecommunication network where security of control and data plane, and the control- data interface is the major focus.

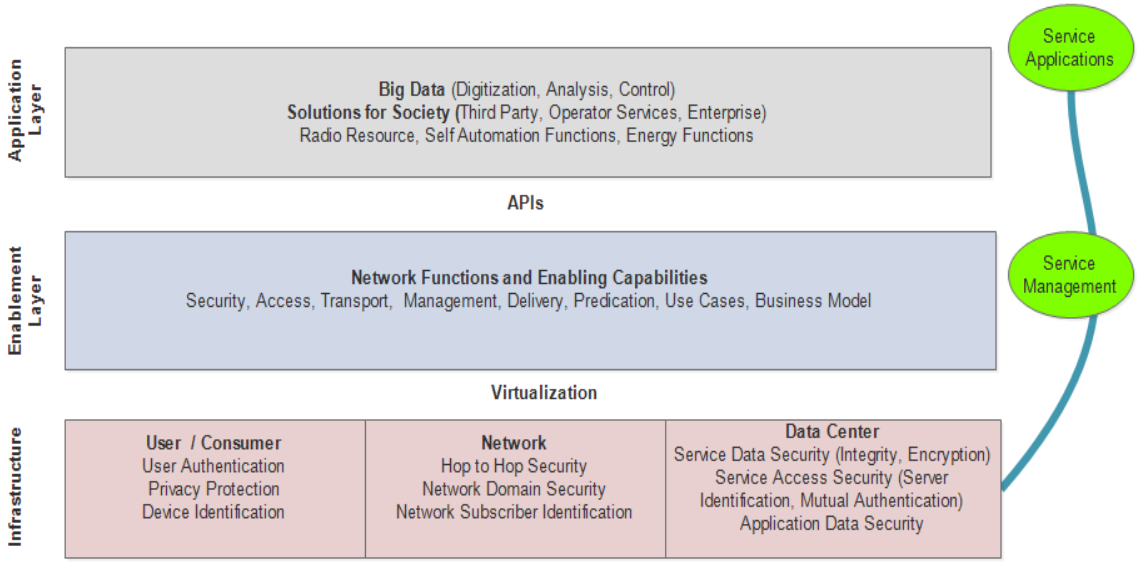

Fig. 4. 5G layered security vision.

V. CONCLUSION

OpenFlow is considered in full scale deployments. Big giant such as Google, Cisco and many more cloud computing service providers are delivering services to their customers with SDN. Hence, security concern is considered to be important aspect of the technology. Very recently, plethora of research on this technology is suggested. Furthermore, number of researchers proved that, vulnerabilities do exist in the OpenFlow technology, namely, spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges. These vulnerabilities can be had with adversary having access to single machine, group of machines and eventually taking control over complete network. Most of the suggested security modules with respect to OpenFlow are based on simulations of small scaled network. Undeniable, some of the methods considered here in the survey have considered lab based simulations involving very few processors. Hence, threats related to distributed attack such as DDoS is not full evaluated. Furthermore, latency sensitive applications running under SDN network with security enabled network elements is also not studied. Hence, before deployment of OpenFlow in a large scale requires through study of its vulnerabilities under the deliberation of Cloud benefits such as elasticity, on demand applications and smooth running of latency sensitive applications. The network is now moving from 3G, 4G to 5G. Cloud will help users to attain access to the capabilities of 5G. The evolution in network suggests modification in security models to gain user trust on network and services.

REFERENCES

[1] Alsmadi, Izzat, and Dianxiang Xu. Security of software defined networks: A survey, Computers & Security 53 (2015): 79-108.

[2] Armbrust, Michael, and Armando Fox. Rean riffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia: Above the Clouds: A Berkeley View of Cloud Computing. Techinical Report No. UCB/EECS-2009-28, 2009.

[3] Bailey J, Pemberton D, Linton A, Pelsser C, Bush R. Enforcing rpki-based routing policy on the data plane at an internet exchange, In Proceedings of the third workshop on Hot topics in software defined networking 2014 Aug 22 (pp. 211-212). ACM.

[4] Ballard, Jeffrey R., Ian Rae, and Aditya Akella. Extensible and Scalable Network Monitoring Using OpenSAFE. INM/WREN. 2008.

[5] Benson, Theophilus, Aditya Akella, Anees Shaikh, and Sambit Sahu. CloudNaaS: a cloud networking platform for enterprise applications. In Proceedings of the 2nd ACM Symposium on Cloud Computing, p. 8. ACM, 2011.

[6] Bernardos, Carlos J., Antonio De La Oliva, Pablo Serrano, Albert Banchs, Luis M. Contreras, Hao Jin, and Juan Carlos Zúñiga. An architecture for software defined wireless networking. IEEE Wireless Communications 21, no. 3 (2014): 52-61.

[7] Blenk, Andreas, Arsany Basta, and Wolfgang Kellerer. HyperFlex: An SDN virtualization architecture with flexible hypervisor function allocation. In Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, pp. 397-405. IEEE, 2015.

[8] Braga, Rodrigo, Edjard Mota, and Alexandre Passito. Lightweight DDoS flooding attack detection using NOX/OpenFlow." In Local Computer Networks (LCN), 2010 IEEE 35th Conference on, pp. 408-415. IEEE, 2010.

[9] Casado, Martin, Michael J. Freedman, Justin Pettit, Jianying Luo, Nick McKeown, and Scott Shenker. Ethane: taking control of the enterprise. In ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 1- 12. ACM, 2007.

[10] Cho, Hsin-Hung, Chin-Feng Lai, Timothy K. Shih, and Han-Chieh Chao. Integration of SDR and SDN for 5G. IEEE Access 2 (2014): 1196-1204.

[11] Dabbagh, Mehiar, Bechir Hamdaoui, Mohsen Guizani, and Ammar Rayes. Software-defined networking security: pros and cons. Communications Magazine, IEEE 53, no. 6 (2015): 73-79.

[12] Dejan Miloji andi and, Ignacio M. Llorente, and Ruben S. Montero. Opennebula: A cloud management tool. Internet Computing, IEEE, 15(2):11 –14, March-April 2011.

[13] Fayazbakhsh, Seyed Kaveh, et al. FlowTags: enforcing network-wide policies in the presence of dynamic middlebox actions, Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013.

[14] Feamster, Nick, Ankur Nayak, Hyojoon Kim, Russell Clark, Yogesh Mundada, Anirudh Ramachandran, and Mukarram Bin Tariq. Decoupling policy from configuration in campus and enterprise networks. In Local and Metropolitan Area Networks (LANMAN), 2010 17th IEEE Workshop on, pp. 1-6. IEEE, 2010.

[15] Giotis, Kostas, Christos Argyropoulos, Georgios Androulidakis, Dimitrios Kalogeras, and Vasilis Maglaris. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer Networks 62 (2014): 122-136.

[16] H. Cui, G. O. Karame, F. Klaedtke and R. Bifulco, On the Fingerprinting of Software-Defined Networks, In IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2160-2173, Oct. 2016.

[17] He, Daojing, Sammy Chan, and Mohsen Guizani. Securing software defined wireless networks. Communications Magazine, IEEE 54, no. 1 (2016): 20-25.

[18] Hinrichs, Timothy, Natasha Gude, Martın Casado, John Mitchell, and Scott Shenker. Expressing and enforcing flow-based network security policies. University of Chicago, Tech. Rep (2008).

[19] Hu, Hongxin, Wonkyu Han, Gail-Joon Ahn, and Ziming Zhao. FLOWGUARD: building robust firewalls for software-defined networks. In Proceedings of the third workshop on Hot topics in software defined networking, pp. 97-102. ACM, 2014.

[20] Jafarian, Jafar Haadi, Ehab Al-Shaer, and Qi Duan. Openflow random host mutation: transparent moving target defense using software defined networking. In Proceedings of the first workshop on Hot topics in software defined networks, pp. 127-132. ACM, 2012.

[21] Kim, Hyojoon, and Nick Feamster. Improving network management with software defined networking. Communications Magazine, IEEE 51, no. 2 (2013): 114-119.

[22] Kreutz, Diego, Fernando Ramos, and Paulo Verissimo. Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, pp. 55-60. ACM, 2013.

[23] Lara, Adrian, and Byrav Ramamurthy. Opensec: A framework for implementing security policies using openflow. In Global Communications Conference (GLOBECOM), 2014 IEEE, pp. 781-786. IEEE, 2014.

[24] Li, Wenjuan, Weizhi Meng, and Lam For Kwok. A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. Journal of Network and Computer Applications 68 (2016): 126-139.

[25] Liyanage, Madhusanka, Ahmed Abro, Mika Ylianttila, and Andrei Gurtov. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective. IEEE Security and Privacy Magazine (2015).

[26] Liyanage, Madhusanka, et al. Security for future software defined mobile networks. Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on. IEEE, 2015.

[27] Ma, Duohe, Zhen Xu, and Dongdai Lin. Defending Blind DDoS Attack on SDN Based on Moving Target Defense. In International Conference on Security and Privacy in Communication Networks, pp. 463-480. Springer International Publishing, 2014.

[28] Marinelli, Eugene E. Hyrax: cloud computing on mobile devices using MapReduce. No. CMU-CS-09-164. Carnegie-mellon univ Pittsburgh PA school of computer science, 2009.

[29] Masoudi, Rahim, and Ali Ghaffari. Software defined networks: A survey, Journal of Network and Computer Applications 67 (2016): 1-25.

[30] Matias, Jon, Eduardo Jacob, David Sanchez, and Yuri Demchenko. An OpenFlow based network virtualization framework for the cloud. In Cloud computing technology and science (CloudCom), 2011 IEEE Third International Conference on, pp. 672-678. IEEE, 2011.

[31] McKeown, Nick, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review 38, no. 2 (2008): 69-74.

[32] Nayak, Ankur Kumar, Alex Reimers, Nick Feamster, and Russ Clark. Resonance: dynamic access control for enterprise networks. In Proceedings of the 1st ACM workshop on Research on enterprise networking, pp. 11- 18. ACM, 2009.

[33] Paim de Jesus, Wanderson, Daniel Alves da Silva, Rafael T. de Sousa, and Francisco Vitor Lopes Da Frota. Analysis of SDN Contributions for Cloud Computing Security. In Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 922-927. IEEE, 2014.

[34] Parker, M. C., G. Koczian, F. Adeyemi-Ejeye, T. Quinlan, S. D. Walker, A. Legarrea, M. S. Siddiqui et al. CHARISMA: Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access.

[35] Porras, Philip, Seungwon Shin, Vinod Yegneswaran, Martin Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for OpenFlow networks. In Proceedings of the first workshop on Hot topics in software defined networks, pp. 121-126. ACM, 2012.

[36] Qazi, Zafar Ayyub, Cheng-Chun Tu, Luis Chiang, Rui Miao, Vyas Sekar, and Minlan Yu. SIMPLE-fying middlebox policy enforcement using SDN. In ACM SIGCOMM computer communication review, vol. 43, no. 4, pp. 27-38. ACM, 2013.

[37] Raghavendra, Ramya, Jorge Lobo, and Kang-Won Lee. Dynamic graph query primitives for sdn-based cloud network management. In Proceedings of the first workshop on Hot topics in software defined networks, pp. 97-102. ACM, 2012.

[38] Rekha, P. M., and M. Dakshayini. Dynamic network configuration and Virtual management protocol for open switch in cloud environment. In Advance Computing Conference (IACC), 2015 IEEE International, pp. 143- 148. IEEE, 2015.

[39] Roberto Bifulco, Julien Boite, Mathieu Bouet, and Fabian Schneider. 2016. Improving SDN with InSPired Switches. In Proceedings of the Symposium on SDN Research (SOSR '16). ACM, New York, NY, USA,

[40] Sasaki T, Perrig A, Asoni DE. Control-plane isolation and recovery for a secure SDN architecture. InNetSoft Conference and Workshops (NetSoft), 2016 IEEE 2016 Jun (pp. 459-464). IEEE.

[41] Schehlmann, Lisa, Sebastian Abt, and Harald Baier. Blessing or curse? Revisiting security aspects of Software- Defined Networking. In Network and Service Management (CNSM), 2014 10th International Conference on, pp. 382-387. IEEE, 2014.

[42] Shalinie, S. Mercy, and R. Nagarathna. An Intelligent Prototype to Lay the Road to Secure Next Generation Networks. Cover Story (2012): 29.

[43] Shimonishi, Hideyuki, and Shuji Ishii. Virtualized network infrastructure using OpenFlow. In Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, pp. 74-79. IEEE, 2010.

[44] Shin, Seungwon, Phillip A. Porras, Vinod Yegneswaran, Martin W. Fong, Guofei Gu, and Mabry Tyson. FRESCO: Modular Compassable Security Services for Software-Defined Networks. In NDSS. 2013.

[45] Shu, Zhaogang, Jiafu Wan, Di Li, Jiaxiang Lin, Athanasios V. Vasilakos, and Muhammad Imran. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications: 1-13.

[46] Stabler, Greg, Aaron Rosen, Sebastien Goasguen, and Kuang-Ching Wang. Elastic IP and security groups implementation using OpenFlow. In Proceedings of the 6th international workshop on Virtualization Technologies in Distributed Computing Date, pp. 53-60. ACM, 2012.

[47] Tsugawa, Maurício, Andréa Matsunaga, and José AB Fortes. Cloud Computing Security: What Changes with Software-Defined Networking?. In Secure Cloud Computing, pp. 77-93. Springer New York, 2014.

[48] Voellmy, Andreas, Hyojoon Kim, and Nick Feamster. Procera: a language for high-level reactive network control. In Proceedings of the first workshop on Hot topics in software defined networks, pp. 43-48. ACM, 2012.

[49] Wang, Bin, Zhengwei Qi, Ruhui Ma, Haibing Guan, and Athanasios V. Vasilakos. A survey on data center networking for cloud computing. Computer Networks 91 (2015): 528-547.

[50] Wang, Kai, Yaxuan Qi, Baohua Yang, Yibo Xue, and Jun Li. LiveSec: Towards effective security management in large-scale production networks. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, pp. 451-460. IEEE, 2012.

[51] Y. Pu, Y. Deng, and A. Nakao, Cloud rack: Enhanced virtual topology migration approach with open vswitch, in Information Networking (ICOIN), 2011 International Conference on, jan. 2011, pp. 160 –164.

[52] Yan Z, Prehofer C. Autonomic trust management for a component-based software system. IEEE Transactions on Dependable and Secure Computing. 2011 Nov; 8(6):810-23.

[53] Yang, Fengyi, Haining Wang, Chengli Mei, Jianmin Zhang, and Min Wang. A flexible three clouds 5G mobile network architecture based on NFV & SDN. China Communications 12, no. Supplement (2015): 121-131.

[54] Yao, Guang, Jun Bi, and Peiyao Xiao. Source address validation solution with OpenFlow/NOX architecture. In Network Protocols (ICNP), 2011 19th IEEE International Conference on, pp. 7-12. IEEE, 2011.

[55] Zaalouk, Adel, Rahamatullah Khondoker, Ronald Marx, and Kpatcha Bayarou. OrchSec: An orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions. In Network Operations and Management Symposium (NOMS), 2014 IEEE, pp. 1-9. IEEE, 2014.