International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Security and Authentication Scheme for Software Defined Network

Ravindra, S.Shankaraiah

Abstract*: Software-Defined Network (SDN) is regarded as one of the most significant areas for future networking. SDN architecture is a revolutionary new concept that offers more mobility, a high degree of automation and shorter delivery time by pushing the conventional network to be software-based. SDN architecture dynamically separates the control plane from the network data (forwarding) plane, providing a centralized view of the network as a whole and making it easier to manage and monitor the resources of the network. Furthermore, the SDN's initial design, with its centralized control point, does not accurately perceive the security requirements, which poses additional challenges to security issues. Security and authentication scheme in SDN is being surveyed in this paper providing advances in this field to both the research community and the industry. Then start with a list of identified threats to security and SDN breaches. The article analyzes previously outlined security and authentication solutions for SDN. The challenges in securing the network from the attacker are discussed and the holistic security approach required for SDN is described. It will identify future directions for research that will be key to providing network security in SDN.

***Keywords:* Software-Defined Network, Security, Authentication, Authorization, Network Functions Virtualization.**

I. INTRODUCTION

In contrast to network functionality, recent developments in wireless communication address users ' needs in data rate, accessibility support, bandwidth expansion, delays, and much more. The fifth-generation (5 G) network would, in the future or the near future, be promising to meet these user requirements. Security has recently become a public good to integrate into each network, including mobile, digital, 5G and Long Term Evolution (LTE) networks. Security is also a must for all networks.

SDN / NFV is incorporated into 5G infrastructure to serve as a cross-backhaul while cloud computing is integrated to enable the storage of data. Since each model has suffered from some security issues, implementing these three different technologies into the 5G network brings with it a giant threat to security.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Ravindra.S.*, Senior Assistant Professor, Electronics and Communication Engineering, City Engineering College, Bangalore, INDIA. Email: ravindraa.s@gmail.com
Dr. Shankaraiah , Professor and Head, Electronics and Communication Engineering, JSS Science and Technology University (Formerly SJCE), Mysore, INDIA. Email: shankarsjce@gmail.com.

Distributed Denial of Service (DDoS) attack, hijacking attack, IP spoofing attack, flow table overload attack, aircraft command saturation attack, are some attacks that are carried on 5 G networks. Here, as it is involved in all three systems, DDoS attack is considered more disruptive.

Any of these technologies or any combination of these technologies will also be impacted by other attacks. The modern era in human history is identified by the ubiquity of information, often called the Information Age. Since it emerged in the 1960s, the prevalence of the Internet has brought a revolution in economy, social development, communication, and entertainment by almost 40 percent of the population worldwide.

The data revolution has led to a recognition of how the conventional IP-based networks are inflexible and difficult to manage, given their prevalence. In short, this is the motivation for Network Functions Virtualization (NFV) and SDN. Although closely related and often coexisting, NFV and SDN are distinct approaches to imposing meanness to the infrastructure which defines the digital age's bedrock. SDN provides the ability to detach data planes from control planes that cannot be conceived in conventional networks.

Data plane and control plane decoupling enables control of forwarding hardware in a network as opened and controlled by both the user. OpenFlow is the standard SDN protocol, with OpenFlow switches, controller and flow entries in the architecture. Software-Defined Networking (SDN) provides a new centralized network control and management structure; an SDN controller monitors and manages all network elements and globally and seamlessly enforces the management and supervision functions. [2]

The rest of the paper is sorted as follows: Section II presents System Architecture of Typical Software-Defined Networks; Section III presents SDN Security Overview; Section IV describes details of SDN Security Analysis; Section V presents SDN Authentication Systems Overview; Section VI explains SDN Authentication Analysis; and finally, Section VII presents the ends and future directions.

II. SOFTWARE-DEFINED NETWORKS

The Software-Defined Networks (SDN) approach is based on the premise that splitting network function control from the network devices themselves (switches, routers, firewalls, etc.) will overcome many drawbacks associated with the vertically integrated, closed, and proprietary networking infrastructure of today. The implementation of software-based virtualization systems and the convergence of voice, video and information communication to IP networks increased the need for such a change in networking standards.

Figure 1 illustrates a typical network in a data center environment that is deployed using SDN. Four users have virtual machines (VMs) operating on the same physical host with the same Open Virtual Switch (OVS) attached to each VM. Data frames from the VMs are tagged with a VLAN ID or some other ID depending on the tunneling protocol in use, distinguishing logically each of the four users.

The OVS then uses flow rules to determine how to handle the traffic from the SDN controller. Separating control and data planes leads to dumb forwarding devices being made by network switches, with control logic being implemented in a centralized controller. This not only enables the network administrators to regulate the traffic flow much more effectively but also enables them to respond much more effectively to evolving network needs in a dynamic environment. The SDN architecture is shown in Figure 2.

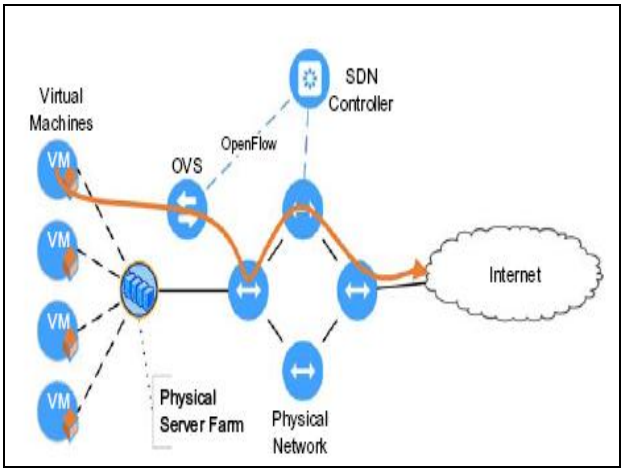

Figure 1 Typical Network Implemented Using SDN.

SDN Benefits and Challenges

According to the following benefits, the use of SDN has carried on steam:

- The traffic patterns that culminate in the implementation of cloud services and big data analytics do not follow the traditional model of a north-south network.
- Separating network control from hardware devices removes the need for the individual configuration of each device. Having a central network policy that can be delivered to the SDN devices reduces deployment time, thereby increasing profits for the data center or service providers.
- As control is isolated from network devices, administrators may adjust the device's actions by forcing software updates to the system instead of fork-lift upgrades-again improving the data center provider's income.
- The functionalities performed by multiple conventional network devices can be handled by a single device. For example, switching, routing, load balancing, and security functions could be done by a single device. In contrast, SDN is an agnostic product, allowing companies to be more versatile.
- Organically, SDN can form traffic and manage QoS. Providing various QoS rates for different applications in current networks is a highly manual process and is unable to adjust rapidly to changing network conditions.
- SDN provides an abstraction layer that allows application managers and administrators to distance themselves from physical hardware management. While having access to virtual disk and memory, SDN virtualizes a Network Operating System (NOS), abstracting from the applications the physical topology of the network. Many applications running on the same physical hardware could have different network views, as shown in Figure 2

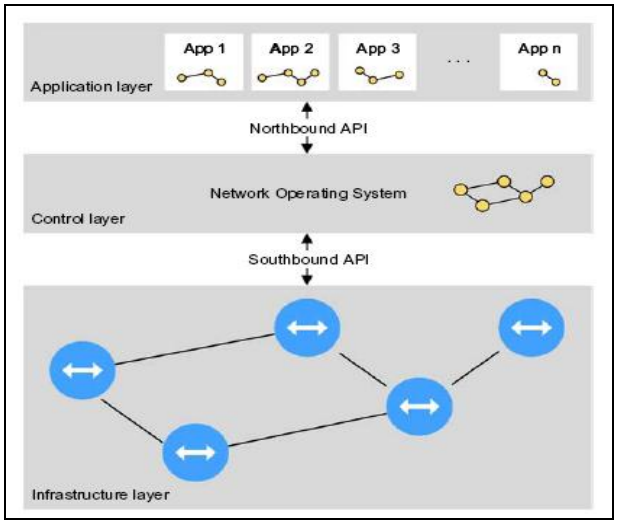

Figure 2 Abstractions in SDN.

Besides being deployed for a variety of traditional features such as routing, security, and load balancing, SDN can be used for traffic engineering, end-to-end QoS enforcement, mobility management, data center implementation, and power consumption reduction. All of these applications are grouped into five categories: 1) traffic engineering; 2) connectivity and wireless; 3) measurement and monitoring; 4) security; and 5) networking of data centers.

SDN CONTROL PLANE An SDN setup's centralized control plane consists of one or more SDN controllers that use open APIs to manage the vSwitches or forwarding devices underlying it. Besides pushing forwarding rules to the vSwitches, the controllers also monitor the environment, giving the controllers the ability to integrate forwarding decisions with real-time traffic management. The controllers interact with the rest of the SDN infrastructure using three communication interfaces, commonly referred to as the interfaces southbound, northbound and east/westbound. Our roles are divided as follows:

- The Southbound interface allows the operator to communicate, connect and monitor the elements of the forwarding. While there are other proprietary implementations, OpenFlow is by far the southbound interface's most popular implementation. OnePK (Cisco) and Contrail (Juniper Networks) are among the proprietary technologies with non-trivial market share.

ForCES have failed to gain much popularity or acceptance as an alternative IETF standard.

- The northbound interface allows applications to program controllers in the application layer by making available to them abstract data models and other functionalities. Additionally, the northbound interface in the network devices can be called an API.
  There is no dominant market leader or agreed standard for northbound interfaces unlike Open-Flow for southbound interfaces.
- East / Westbound interfaces are intended to communicate between controller groups or federations. Similar to the northbound interfaces, a universally accepted standard is yet to be developed.

SDN DATA PLANE The SDN architecture data plane is responsible for enabling data transfer from the sender to the receiver(s). They are agnostic to the protocol used for end-point communication. Except for communicating with the controller, data plane devices themselves do not generate or receive data, but rather function as data conduits. To communicate with controllers, data plane devices need to adopt a southbound API. Data plane devices come in two ways: 1) software-based devices such as Open vSwitch, and 2) hardware-based devices such as OpenFlow support HP switching. Software-based devices, as can be predicted, have a more full set of features, but are generally slower.

OPENFLOW OpenFlow, identified by the ONF, is a protocol between SDN architecture's control and forwarding layers and is by far the most widespread SDN implementation. A basic architecture for OpenFlow consists of end hosts, a controller and switches enabled for OpenFlow. Remember that an OpenFlow switch is not limited to being a layer-2 system, contrary to the conventional nomenclature of the network. Using an Open-Flow API, the controller communicates with the switches. When a packet enters an OpenFlow switch, it handles the packets as follows:

1. A flow table search is done to match the packet's header fields to the local flow table. If there is no compatible entry, the packet will be sent for processing to the controller. When there are several entries in the flow table that suit the incoming packet, the packet with the highest priority will be picked.
2. Byte counters and packets are updated.
3. The action set is accompanied by the action(s) corresponding to the matching flow rule. If the execution chain is part of a different flow table, processing will continue.
4. The action set will be executed once all flow tables have been processed.

SDN CONTROLLERS The controller is the SDN operation's brains. This lies between the machines of the data plane on one side and applications of high level on the other. By installing flow entries on switch devices, an SDN controller assumes the responsibility of establishing every flow in the network. Flow entries can be applied to a data plane system in either (1) proactive mode where the flow rules are sent to the data plane devices as soon as the controller knows about them, or (2) reactive mode where the controller sends flow entries to the data plane devices only as required. When data plane devices send flow setup requests to the controller in reactive mode, it first checks this flow against the application layer policies and decides what actions to take. First, it defines a path to traverse the packets (based on other application-layer policies) and installs new flow entries along the path in each system. Added flow entries have specific timeout values that indicate how long they should be stored in their forwarding tables in the event of inactivity before deleting the entry to the data plane devices. The network administrator choice is decided by the tradeoff between setup delay and memory required to maintain the forwarding table in your system. Also, the opportunity to be adaptive depending on the current network requirements is provided to the administrators in reactive mode.

OPEN VIRTUAL SWITCH OVS is the open-source implementation of a multi-layer virtual programmable switch distributed. OVS implementations generally consist of flow tables with matching conditions and related actions for each flow entry. OVS uses a secure channel to communicate with the controller and uses the OpenFlow protocol in general. Instead of the conventional Linux Bridge, OVS was commonly incorporated into big cloud orchestration frameworks such as OpenStack, CloudStack, etc. Figure 3 is the core OVS elements. A NIC (physical or virtual) receives the packets from the kernel module. If the packet is handled by the kernel module, it simply follows the instructions. If not, the packet will be sent in user space to the ovs-vswitchd using NetLink. It defines how to use the OpenFlow protocol to manage the packet. The ovs-vswitchd interacts through a socket with an ovsdb-server. The ovsdb-server store's JavaScript Object Notation (JSON) format for OVS configuration and change management information. Using Command Line Interface (CLI) commands to execute all functions in the userspace. In the rest of this text, OVS and vSwitch are used interchangeably.

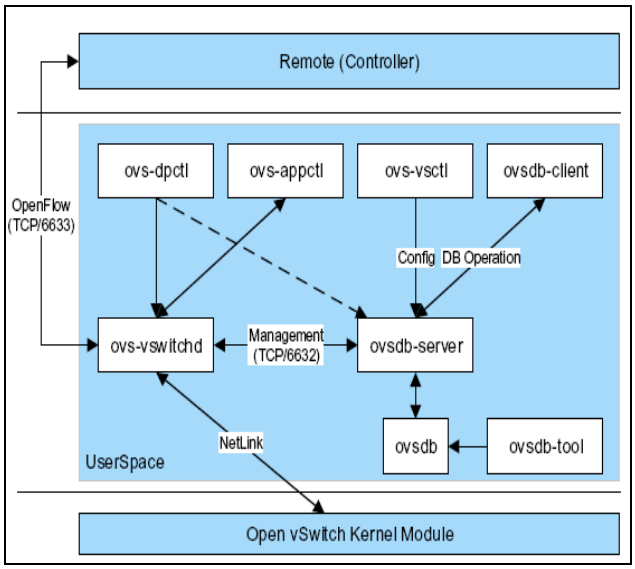

Figure 3 Open vSwitch Architecture

III. SDN SECURITY OVERVIEW

Incorporate cloud and data-center network SDN finds most implementations. SDN can offer advantages not only for data management and orchestration but also for the protection of the server. The security of SDN itself is, therefore, a very significant field of research.

With the hierarchical nature of SDN, security issues such as distributed denial of services (DDoS) attacks on the SDN controller can be implemented. The operational SDN architecture can be divided into the application, the control, and the data layers. Multiple attack vectors can be found in every layer. Also, the communication channel between layers, for example, can be used to modify traffic and eavesdropping attacks through an application control interface.

A. SDN SECURITY CLASSIFICATION

The relationships between SDN components can introduce new, conventional network vulnerabilities. For example, the use of a secure transport layer on the Open Flow network is optional. Thus, safety issues, such as DoS, fraudulent flow rules and alters of the rules, may arise from the nature of the communication protocol. The various components in the SDN are shown in Figure 4: (1) application plane, (2) control plane and (3) data plane subject to attack. Figure 4 shows: In SDN controllers (Opendaylight, ONOS, Floodlight), for example, application vulnerability may be possible. Also, security threats can be encountered through the communications paths between three levels: northbound APIs (4) and southbound APIs (5). Some of the attack vectors for target components are discussed in detail below:

Application Plane: Security vulnerabilities can be present in applications designed for telemetry, orchestration and other SDN operations. The Cross-Site Request Forgery (CSRF) also extends to SDN all security issues that can occur in a typical web application, like the Cross-Site Scripting (XSS). The malicious/committed applications will spread attacks throughout the network.

Control Plane: This control unit consists of one or more controllers for the handling of various types of protocol, such as OpenDaylight, POX, ONOS and other applications and plugins. The attacker will produce traffic from the IP address and give the controller an immense amount of traffic. This attack will saturate the interaction between the switch and the controller, thus increasing the latency of the network.

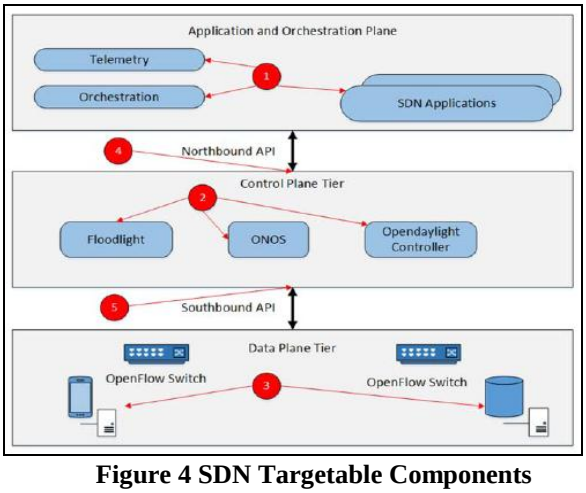

Figure 4 SDN Targetable Components

Data Plane: By forging the Link Layer Discovery Protocol (LLDP) packets, the attackers will poison the network's global view. Attackers can also observe the delay in contact with specially created packets between the control plane and the data plane applications. This can help identify the system logic of the controller. The attackers will target the switches as well. The data flow control switch often has limited memory and can be overflowed by a large number of flood controls.

Communication Channels: A Man in - the -Middle (MITM) attack may be carried out on a channel of communication between switches and managed devices (Southbound API), controllers and Northbound APIs (Northbound API). Authors who target the communication channel have posed attacks by eavesdropping traffic between hosts and gradually shifting traffic between hosts.

B. SDN SECURITY THREAT VECTORS

In this section, some key Threats Vectors (TVs) in SDN is examined in detail, and investigate if a superior SDN stage configuration can help in managing security threats inborn and extraneous to the SDN.

TV1 Fake Traffic Flows: Faulty devices or noxious clients can utilize DoS assaults to focus on the TCAM (ternary content-addressable memory) switches in the SDN foundation, to debilitate the limit of the TCAM switches. The issue can be relieved by utilizing a straightforward authentication mechanism, yet on the off chance that the assailant can bargain the application server comprising of subtleties of clients, an aggressor can utilize the equivalent confirmed ports and source MAC delivers to infuse fashioned approved streams into the network.

TV2 Switch Specific Vulnerabilities: The switches present in the SDN condition can have drawbacks. For example, a drawbacks in Juniper OS (CVE-2018-0019) SNMP MIB-II subagent daemon (mib2d) permits a remote network-based assailant to cause the mib2d procedure to crash bringing about a denial of service condition (DoS) for the SNMP subsystem. A switch can be utilized to hinder the traffic in SDN condition, go amiss the network traffic to take data, or can be utilized to embed manufactured traffic demands with the objective of over-burdening the controller or the neighboring switches.

TV3 Control Plane Communication Attack: The control-data plane correspondence doesn't require the nearness of TLS/SSL security. Regardless of whether Public Key Infrastructure (PKI) is available in an SDN situation, complete security isn't ensured for the channel correspondence. Research works feature security issues with TLS/SSL. An undermined Certificate Authority (CA), defenseless application can prompt an assailant getting entrance in charge plane channel of the SDN. The assailant can dispatch DDoS by utilizing switches that are constrained by the control plane.

TV4 Controller Vulnerabilities: The controller is the most significant segment in the SDN condition. An undermined controller can cut down the whole network.

For instance, an old variant of SDN controller ONOS experiences remote denial of service attack (CVE-2015-7516). The aggressor can cause a NULL pointer to dereference and switch detach by sending two Ethernet outlines with ether type Jumbo Frame (0x8870) to ONOS controller v1.5.0. A blend of mark based interruption location devices will be unable to locate the definite mix of occasions that set off specific conduct and esteem it pernicious or benign.

TV5 Lack of Trust between Controller and Management Applications: Controller and the executive's plane applications come up short on an inherent system to set up trust. The endorsement creation and trust confirmation between organizing gadgets in the SDN condition can be not quite the same as the trust system between ordinary applications.

C. DESIGN OF SECURE AND DEPENDABLE SDN PLATFORM

As illustrated in Figure 5, secure and reliable SDN architecture can be used to address the threat vectors with features such as defect tolerance, self-healing, trusting framework, and dynamic service provisioning capabilities. In this section, we complain about each of the security mechanisms integrated into the SDN framework design.

1. Replication: Apart from a large amount of traffic or software vulnerabilities, application and controller replication can help with the handling of controllers or application failures. As shown in Figure 4, replication is provided by three variants of the SDN controller. Furthermore, each controller has been replicated with application B. This approach may help to address both hardware and software (accidental or malicious) failure issues. The isolation of malicious code while ensuring the quality of service provides another benefit for replication.

2. Diversity: The use of only one form of operating system or code enables the manipulation of a target for attackers. Diversity improves the strength and tolerance of intrusion. Diversity helps to avoid increasing defects and vulnerabilities as only a few intersecting vulnerabilities occur between different software and OS. Using diverse controllers can help to reduce lateral attacker movement and cascade system faults caused by common vulnerabilities in the SDN management plane.

3. Automated Recovery: On account of security assaults, prompting administration disturbance, the proactive and responsive security recuperation systems can help in keeping up with ideal assistance accessibility. When supplanting software, e.g., SDN controller, it is important to play out the supplanting with new and assorted adaptations of the segment. For instance, if we intend to switch SDN controller Open Daylight, we can consider a substitute form of controller software, for example, Floodlight, ONOS or Ryu giving comparable usefulness.

4. Dynamic Device Association: The relationship between the controller and gadgets, for example, OpenFlow switch ought to be dynamic. For example, on the off chance that one occurrence of the controller comes up short, the switch ought to have the option to powerfully connect with the backup controller in a verified manner (appropriate validation system to distinguish great controller from malicious controller software). Dynamic Device affiliation highlight helps in managing deficiencies (crash or Byzantine). Different points of interest incorporate the burden adjusting highlight gave by assorted controllers (reduced service latency).

5. Controller-Switch Trust: A trust establishment system between the controller and switch is critical to manage instances of phony streams being embedded by malicious switches. The controller can in fundamental trust establishment situation keep up a whitelist of switch devices that are permitted to send control plane explicit messages to the controller. In an increasingly intricate situation, Public Key Infrastructure (PKI) can be utilized to set up trust between the control plane and data plane devices. The conduct devices constrained by the controller can likewise be utilized to make a trust system. The devices displaying strange conduct can be placed in isolate mode by the controller

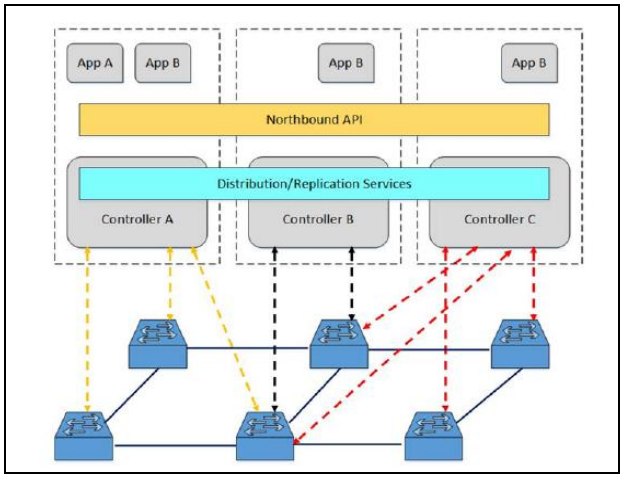

Figure 5 Design Of Secure And Dependable SDN.

.6. Controller-App Plane Trust: The software segments change conduct due to change in the earth. Also, software maturing can present security vulnerabilities. Controller and application plane segments should utilize autonomic trust the executive's systems dependent on common trust and assigned trust (third part, for example, the Certificate Authority to set up trust). The controller can use autonomic trust the board for part based software frameworks. Subjective measurements, for example, privacy, uprightness, and accessibility can likewise be utilized to set up the dependability of an application in the SDN framework.

7. Security Domains: Security spaces help in fragmenting the system into various degrees of trust, and control of the dangers to just the influenced area in the SDN structure. A security space-based detachment can be consolidated to give resistance inside and out to the SDN condition. For instance, the web-server application on one physical server should just connect with database back-end applications, and no other application running in a similar system. A whitelist-based security approach creation with a suitable strategy strife checking component can be used to accomplish such security objectives.

D. SDN-SPECIFIC SECURITY CHALLENGES

In addition to the threat vectors discussed in earlier paragraphs, certain SDN-specific safety issues do not exist inherently in conventional networks. We highlight these challenges and best practices of security in this subsection to avoid them in SDN.

1. Programmability: SDN provides programmatic capabilities to consumers from various corporations and organizations. Modern companies follow the organizational model of a closed domain. The SDN business model thus makes it necessary, across a variety of business and administrative areas, to safeguard system integrity, open interfaces and data from third parties.

Traffic and Resource Isolation: Corporate planning and real-time information of one program must be completely isolated from other applications. In the SDN setting, traffic and resource isolation must be guaranteed among the tenants. Complex interactions can result in more fine-grain isolation because of the SLA requirements and private addressing scheme.

Trust between third-party applications and controller: Authentication and authorization mechanisms should be implemented to limit the exposure of the controller at the application registration point for the controller.

2. Integration with Legacy Protocols: Some technical and process deficiencies in the legacy protocols were resolved by the advent of SDN. Nevertheless, updating security features for existing technologies, such as DNS and BGP may not be easy. Until integrating into SDN, it is important to test the functionality of the existing protocols.

3. Cross-Domain Connection: The SDN infrastructure provides connectivity between various physical servers, clusters and data centers. Each security domain can be managed by one or several controllers. SDN design should include an adequate mechanism for establishing a relationship of trust between controllers. The confidence framework should be capable of preventing abuse and of building a safe channel.

E. OPENFLOW PROTOCOL AND OPENFLOW SWITCH SECURITY ANALYSIS

1. Attack Model

Actors

The OpenFlow attacks can be implemented internally or externally. A trusted insider may attempt to enhance privilege by altering OpenFlow protocol implementation or request unauthorized access to reference data relating to OpenFlow. An external assailant, on the other hand, may control devices attached directly to the OpenFlow switches and attempt to generate malicious traffic requests to disrupt the communication and gain privileges remotely from OpenFlow devices.

Attack Vectors

External and internal attackers can use the following vectors, which aim for components of OpenFlow: passive eavesdropping on messages in the data/control plane. This can help the perpetrator obtain the information necessary for further attacks. Replay Non-authentic Data Control, Man-in-the-Middle (MITM), DoS / DDoS or side-channel attacks on SDN Network attacks.

Target/Goal

OpenFlow protocol assets/properties can be accessed by the attacker:

- Protocol messages with sensitive information.
- Locate, network topology, accessibility of the SDN network or related performance information. The device data for OpenFlow switch flow table entries are referenced.
- Monitor and data plane data and asset information (e.g. bandwidth, latency, timeout flow).

2. Protocol-Specific Analysis

The following entities, elements, and subcomponents, as indicated in Table 1, should be considered in the protocol analysis. The study assumes that each OpenFlow switch can be connected to one or more of the cloud service provider's trust limits. TLS security can also be used to handle message manipulation and to carry out mutual authentication between the switches and the controllers.

Table 1 OpenFlow Protocol Analysis Breakdown

Entity	Component	Sub-components/Scenarios
Switch	Ports	Physical Ports
		Logical Ports
		Reserved Ports
	Tables	Counters
OpenFlow Channel and Control Channel	Channel Connections	Connection Setup
		Encryption
		Multiple Controllers
		Auxiliary Connections

IV. SDN SECURITY ANALYSIS

Ihsan H. Abdulqadder et al [1] proposes an improved assault mindful security provisioning plan to give protection from significant assaults in SDN and NFV empowered 5G to organize. In this work, security is given by the following procedure: (I) Initial Authentication process, (ii) Classification of bundles, and (iii) Switch movement process. Introductory Authentication is performed at Access Point (AP) for every client by Secure ID-based Authentication (SIA) conspires. The presumed bundles are distinguished in the controller and arranged at Virtual Network Function (VNF). For parcel characterization, the ideal bundle highlights are chosen to utilize the Genetic Algorithm with Correlation (GAC) based element determination calculation. We have proposed a Radial Basis Function with the Extreme Learning Machine (RBF-ELM) classifier. At that point, the malignant parcels are dropped at VNF and ordinary bundles are diverted to goal address through controller. To relieve stream table over-burdening assault, we have displayed an Enhanced Artificial Bee Colony (EABC) calculation in the controller. The test result shows that our proposed security provisioning plan shows better execution as far as deferral, a measure of diverted parcels, location precision, bundle transmission rate, and parcel misfortune proportion.

Ihsan Abdulqadder et al [2] presents a strong security plan to furnish stronghold against significant dangers alongside client protection in 5G network, two extra elements are presented.

For versatile clients, starting authentication is given at passages by an innovative Highly Secured Authentication and Handover Mechanism (HSAOHM) plot. Which limit handover inactivity without loss of client security. At that point, the approved client bundles are landed at dispatcher in which a novel Tree-Based Switch Assignment (TBSA) algorithm is consolidated. TBSA mitigates the stream table over-burdening assault by doling out bundles to underloaded switches. In controller, DDoS assault is distinguished with the help of entropy examination. At that point, the suspicious parcels are diverted to scrubbing Virtual Network Function (sVNF) in the cloud. In sVNF, suspicious bundles are ordered into typical parcels and malevolent bundles by utilizing Hybrid Fuzzy with Artificial Neural Network (HF-ANN) classifier dependent on bundle highlights. Ordinary parcels are permitted to get to applications while pernicious bundles are dropped at sVNF. Broad reenactment shows security improvement in the 5G network as far as handover inertness, holding time, switch disappointment rate, identification exactness, and postponement.

Sahil Garg et al [3] propose a software-defined network (SDN)- based solidified system giving start to finish security and protection in 5G empowered vehicular systems. The system improves organize the board through SDN while accomplishing enhanced system interchanges. It works in two stages: initial, an elliptic bend cryptographic based authentication protocol is proposed to commonly validate the bunch heads and endorsement expert in SDN-based vehicular arrangements, and, second, an interruption discovery module upheld by tensor-based dimensionality decrease is intended to lessen the computational unpredictability and distinguish the potential interruptions in the system. To survey the exhibition of the proposed structure, a broad assessment is performed on three test systems; NS3, SUMO, and SPAN. To saddle the potential advantages of the proposed model, the primary module is assessed based on security highlights, though the subsequent module is assessed and contrasted and the current best in class models, based on location rate, bogus positive rate, precision, identification time, and correspondence overhead. The recreation results show the predominance of the proposed system when contrasted with the current models.

Jun Wu et al [4] proposes large information examination based secure cluster management architecture for the improved control plane. A security confirmation plot is proposed for cluster management. Besides, we propose a colony optimization enhancement approach that empowers an enormous information examination plot and the usage framework that streamlines the control plane. Recreations and correlations show the possibility and proficiency of the proposed plan. The proposed plan is critical in improving the security and effectiveness SDN control plane.

Gengshen Lin et al [5] propose a security function virtualization (SFV) based moving objective guard of SDSG which makes the assault surface continually evolving. In the first place, we structure a unique barrier system by relocating virtual security function (VSF) occasions as the traffic state changes. The brought together SDN controller is re-intended for worldwide status checking and relocation of the executives. Also, we formalize the VSF examples movement issue as a whole number nonlinear programming issue with numerous requirements and plan a pre-relocation calculation to avoid VSF occurrences' assets from being depleted. Reproduction results demonstrate the attainability of the proposed plan.

Rajat Chaudhary et al [6] planned a software-defined network (SDN) empowered multi-characteristic secure correspondence model for an IIoT situation. The proposed plan works in three stages: 1) an SDN-IIoT correspondence model is structured utilizing a cuckoo-filter-based fast-forwarding scheme, 2) a property based encryption conspire is displayed for secure information correspondence, and 3) a companion entity authentication plot utilizing an outsider authenticator, Kerberos, is additionally introduced. The proposed plan has been assessed utilizing various parameters where the outcomes acquired demonstrate its adequacy in contrast with the current arrangements.

Reem Melki et al [7] propose a plan for verifying MP-TCP. This is accomplished with the help of SDN, in which another security module living in the SDN controller goes about as an outsider session-key dispersion authority. After the recovery of session keys, a lightweight data concealing component to verify the keys traded during the underlying handshake is proposed.

Jingjing Xu et al [8] propose another savvy framework dependent on SDN. It likewise furnishes with the elements of fine-grained get to control and accessible encryption work, which consolidates a novel attribute-based searchable encryption scheme (ABSES) with SDN architecture. Our development acknowledges between area data sharing, fine-grained get to control, and ciphertext accessible capacity. The proposed ABSES adequately guarantees the security of ciphertext put away in server farm, and that clients can't acquire unapproved data or unlawful system assets with no confirmation. It decreases arrange data transmission and nearby assets while improving the versatility and adaptability of SDN get to control at the interim. At last, our ABSES is demonstrated to be right and verify under picked watchword assault. The correlation with other delegate quality based accessible encryption plans shows that our ABSES has to some degree better execution. The proposed new brilliant framework can be utilized in human life and add more comfort to our day by day life.

Sugandhi Midha et al [9] centers around making SDN OpenFlow correspondence increasingly secure by following broadened TLS backing and guarded calculation.

Jean Claude Nikoue et al [10] proposes an exhaustive methodology for associations to assess security-related highlights accessible in SDN controllers. The procedure can fill in as a rule in the choices identified with SDN decision. The proposed security appraisal pursues an organized way to deal with assess each layer of the SDN design and every measurement characterized in exhibited examine has been coordinated with the security controls characterized in NIST 800-53. Through the tests on genuine controllers the paper gives a model on how the proposed methodology can be utilized to assess existing SDN arrangements.

Haifeng Zhou et al [11] propose an ongoing strategy to distinguish traded off SDN gadgets in a solid manner. The proposed strategy targets taking care of the identification issue of bargained SDN gadgets when both the controller and the switch are trustless, and it is integral with existing recognition techniques. Our essential thought is to utilize backup controllers to review the taking care of data of system update occasions gathered from the essential controller and its switches, and to distinguish bargained gadgets by perceiving conflicting or sudden dealing with practices among the essential controller, reinforcement controllers, and switches. Following this thought, we first catch each system update solicitation and its execution bring about the essential controller, gather each got system update guidance and the data of any state update in switches, and convey these four sorts of data to those backup controllers in an auditor role. An examiner controller is intended to make a review record for each got system update demand and to include its execution aftereffect of this system update demand just as they got four sorts of coordinating data to the review record. Specifically,

heterogeneous auditor controllers are proposed to stay away from a similar defenselessness with the essential controller. The review calculation and hypothetical confirmation of its viability for security upgrade are then introduced. At long last, in light of our model execution, our exploratory outcomes further approve the proposed technique and its low expenses.

Yanbing Liu et al [12] plan a SDN-based information move security model middle box-guard (M-G). M-G targets diminishing system inactivity, and appropriately oversees dataflow to guarantee the system run securely. To begin with, as per diverse security arrangements, middle boxes identified with the characterized secure approaches, are put at the most proper areas, utilizing dataflow reflection and a heuristic calculation. Next, to maintain a strategic distance from any middle box turning into a hotspot, a disconnected whole integer linear program (ILP) pruning algorithm is proposed in M-G, to handle switch volume imperatives. What's more, an online linear program (LP) plan is come up to deal with load balance. At last, secure instruments are proposed to deal with various assaults. Furthermore, arrange steering is fathomed deftly, through dataflow the executive's convention, which is figured by means of joining passages and labels. Test results show that this model can improve security execution and oversee dataflow viably in SDN-based IoT framework.

Ying Qian et al [13] investigates significant conceivable security threats and assaults in SDN switch and proposes new way to deal with powerfully recognize and screen noxious practices on stream message passing and protect such assaults to militate the security threats to switch stream table the channel among switch and controller.

Ramissa Djouani et al [14] discuss about Internet of things (IoT) is another rising innovation with no human control, another period where it's tied in with making esteems in an associated society with upgraded administrations and sharing information like never before to improve our way of life. The enormous development of IoT associated gadgets produces colossal measure of information which makes various difficulties as far as capacity and preparing limit, arrange the executives and particularly information security and protection as a security breaks may have serious outcomes, for example, hazardous. Joining IoT with other inclining advances, for example, Software Defined Network (SDN) and Cloud uncovers so significant in view of the advantages they are offering to beat these difficulties. Authors present a security proposition for IoT dependent on SDN and Cloud integration.

V. SDN AUTHENTICATION SYSTEMS OVERVIEW

In the present world, network administrators are making an enormous effort to secure corporate networks that often contain important data and resources. Regrettably, these networks are vulnerable because of accidental applications ' bugs, misuse or even insider threats, regardless of policies and measures used. Network access should be easy, but uncontrolled and network linked is vital to the security of the network; this is called the Network Access Control, also called the Port Access Control. There is a Standard IEEE 802.1x technology that defines a port-based Ethernet network access control system. IEEE 802.1x is a specification that specifies a method of enclosing messages to be sent via a Local Area Network (LAN) EAP. (Extensible Authentication Protocol).

This encapsulation is termed EAP over LAN (EAPOL). The concept of such a solution is that the network must be authenticated first using your credentials, before you have access to it via a switch port. No one can access the network directly. For authentication, IEEE 802.1x relies on the EAP protocol which allows the use of EAP-MD5, EAP-IKE v2, EAP-TLS and many others. The 802.1x standard specification comprises three aspects: the source (host), the authenticator and the authentication server.

AUTHENTICATION PROCESS When a new 802.1x-ware client (supplier) links to the networking, the authentication process will start. The authentication messages between the suppliers and Authenticator begin when they send the EAPOL-Start frame to the edge switch or if the Authenticator detects changes to their ports, and if it receives a packet on a particular port, with an origin MAC address not included in its flow table, see Figure. 6.

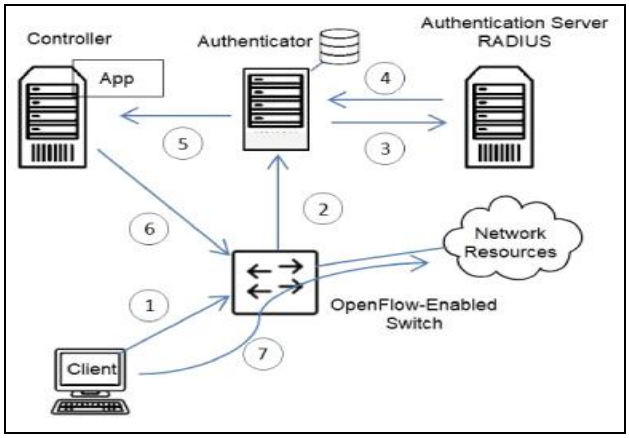

Figure 6 Authentication Process.

The Switch is told proactively to forward the EAPOL initialization frames to Centralized Authenticator. With EAPRequest / identity the Authenticator replies and asks for the credentials of the applicant. The Supplier responds by supplying its credentials with an EAP Answer / Identity kit (user name that determines this customer request solely). The Authenticator then decapsulates the email and compares it to a local user database. If a match occurs, the Controller request will be informed by Authenticator. Otherwise the message will be encapsulated and sent to the Authentication Server. The RADIUS Access / Challenge authentication server is sent to the client. The applicant then offers the EAP response / identity credentials. After that, the RADIUS server checks the received credentials and either transmits an EAP Success (Access-Accept) packet to the extent that the client is successfully authenticated and authorized to acquire access to the network, or a EAP-Reject (Access-Accept) packet to block the access. The authenticator updates the active user registry and gives the Controller the final decision to install new information on the relevant flow table and the rule class for that customer can be implemented.

AUTHORIZATION PROCESS Authentication and authorization are usually paired. We know "whom you can reach" after successful authentication, while authorization means "those who can access what" in a network. This is for users, devices and network services. Therefore, the Authentication Server returns an EAP Success (access-acceptation) Packet, when the supplier is correctly authenticated, that includes a list of user permissions (attribute value couples) that specifies the parameters to be used for the current session. The modified authenticator then sends these messages to the app running at the top of the controller to notify the Supplier's authentication success and identity (its MAC address). The service type, the model, the access list or only the static path to be implemented in the open flow table can be used in these parameters. Finally, the Controller software converts this parameter into the flow rules to be mounted on the relevant switch and applied to the relevant port. This enables the switch to find a link between the supplier and its stream easily.

VI. SDN AUTHENTICATION ANALYSIS

Xiao Liang et al [15] propose a hierarchical authentication system for the IPv6 source address with the innovation of software defined network (SDN). This instrument consolidates the validation of three sections, to be specific the entrance organize, the intra-area and the between space. What's more, it can give a fine-grained security assurance for the gadgets utilizing IPv6 addresses.

Jin Cao et al [16] coordinate client ability and Software Defined Network (SDN) procedure, and propose a capacity based security assurance handover verification system in SDN-based 5G HetNets. Our proposed plan can accomplish the shared validation and key understanding between User Equipments (UEs) and BSs in 5G HetNets simultaneously to a great extent decrease the verification handover cost. We show that our proposed plan without a doubt can give powerful security assurance by utilizing a few security examination strategies including the BAN rationale and the proper confirmation device Scyther. What's more, the presentation assessment results show that our plan outflanks other existing plans.

Hui Yang et al [17] propose a blockchain-based trusted authentication (BTA) design for 5G with blockchain-based anonymous access (BAA) plot in cloud radio over fiber arrange. The possibility and productivity are checked on improved SDN testbed to empower blockchain as assistance.

Ting Ma et al [18] present a quick and proficient physical layer authentication plot for software-defined-radio (SDN) empowered 5G heterogeneous network (HetNet). In the plan, we propose to play out the handover authentication with Kolmogorov-Smirnov (K-S) theory test. The K-S based authentication is quick, productive, and progressively appropriate for physical layer traits with differing dissemination structures.

Cong Wang et al [19] speak to the related research and propose a novel and productive software-defined networking (SDN) - based handover authentication conspires for MEC in CPS (SHAS). An authentication handover module (AHM) in the SDN controller is applied for key circulation and confirmation the board. Before ECN handovers, the AHM appropriates a key to the present serving AP for ECN further handover. At whatever point a handover occurs, target AP demands the AHM for the one-time session key (OSK) to authenticate the ECN. The objective AP and ECN can continue with the 3-way handshake convention by the OSK to accomplish common authentication and mystery key privacy. Utilizing the intelligent deduction of Burrows, Abadi, and Needham and formal check via automated validation of Internet security protocols and applications (AVISPAs), proposed SHAS plan can get common validation and mystery key privacy with a solid enemy of assault capacity. The recreation results show that the SHAS conspire has the attributes of lower computational postponement and less correspondence assets. At long last, the commonsense exhibit of our plan is finished utilizing the generally acknowledged NS-3 reproduction.

Osamah Ibrahiem Abdullaziz et al [20] present a lightweight authentication arrangement, called hidden authentication (HiAuth), to ensure the SDN controller by concealing the characters of the sending gadgets into the control parcels utilizing effective bitwise tasks. HiAuth is the first to consolidate data concealing systems into OpenFlow to give protection from DoS assaults. HiAuth misuses the IP ID field of IPv4 and the exchange distinguishing proof field of OpenFlow in two confirmation plans. The test results show that HiAuth can viably relieve interloper DoS assaults and give high imperceptibility to aggressors.

Liming Fang et al [21] configuration, actualize and assess another confirmation conspire called The Hidden Pattern (THP), which consolidates illustrations secret key and advanced test an incentive to avoid different sorts of validation assaults simultaneously. We analyzed THP in the points of view of both security and ease of use, with a complete number of 694 members in 63 days.

Our assessment shows that THP can give preferred execution over the current plans regarding security and ease of use.

Ju-Ho Choi et al [22] propose another MACsec expansion over the Software-Defined Networks (SDN) for an in-vehicle secure communication, which depends on IEEE 802.1X authentication mechanism. The proposed plan broadens the security extent of MACsec from point-to-point to start to finish by assigning AKM procedure of ECUs and changes to the SDN controller. It could limit the cryptographic procedures of the ECUs and switches with no change of the current MACsec standard and could shield a car framework from any control by unapproved outsiders. The exploratory outcomes show that the proposed plan is relevant for in-vehicle secure communication.

Yongli Tang et al [23] propose a lightweight identity two-way authentication conspire (LTWA) because of the cryptographically generated address (CGA) algorithm joined with the hash generated address (HGA) algorithm. The plan presents the CGA algorithm and the HGA algorithm without outsider support, in order to finish the main authentication official and the non-first authentication authoritative between the correspondence hubs separately, which adequately keeps an aggressor from fashioning or altering confirmation cooperation messages, in this way setting up a start to finish believed association in the entrance arrange. We tentatively confirm the proposed LTWA conspire. The recreation results show that the plan ensures the security cooperation between correspondence hubs, and diminishes the normal computational overhead and the blocking rate brought about by vindictive assaults.

Tahira Mahboob et al [24] presents a straightforward authentication mechanism utilizing the hash table, cryptographic hash capacity and REST API for passages (APs) and applications to verify the correspondences. The unapproved applications are not permitted to get to organize assets. Furthermore, unapproved passages are not permitted to speak with other system components. The remote topology is imitated and tje proposed application is tried to approve the outcomes. The application produces the report about all-out approved and unapproved passageways in the topology. The application is permitted to run consistently in the system and caution the chairman about vindictive gadget. This pernicious gadget and application aren't permitted to speak with other system component or access organizes assets. Execution assessment has been done by measuring the time required to run the application for a shifting number of Access Points (APs).

Hongyan Cui et al [25] talk about the authentication mechanism of the system application. Simultaneously, it actualizes the application authentication framework which tends to the key difficulties: how to securely resolve clashes between untrusted organize applications and solicitations. The paper experiences framework testing in testbed built Floodlight design. The test outcomes show that the framework functions admirably to successfully safeguard against unapproved get to and give log history, which checks the adequacy of the proposed technique to verify the northbound interface by presenting the application authentication framework.

Ke Ding et al [26] an authentication handover mechanism under a multi-SDN domain (AHMMD) is proposed, to comprehend the long confirmation handover delay in multi-space SDN condition. In AHMMD, right off the bat, when the versatility substance gets to the system just because, its personality and administration characteristics are verified by the stream validation convention, which is structured dependent on the unbalanced encryption key; besides, when the portability element moves to the neighbor area, the verification data will be conveyed from the present controller to the local controller through a security correspondence channel. To advance the productivity, a handover time forecast calculation is received in AHMMD. Exploratory outcomes dependent on our AHMMD model have demonstrated that the handover defer diminishes by half while the handover cost diminishes by 60%.

Yanling Zhao et al [27] a numerous course count strategy is proposed by altering the Dijkstra algorithm. The strategy gives dependable transmit courses to the higher quality of service (QoS). To test the proposed techniques, the model framework was structured with an ODL controller and switches. Also, the framework actualizes the verification and various leveled transmit capacities.

Jing Yang et al [28] propose to present remote connection marks chose by clients' areas as handover validation information to accomplish bound together and quick handover confirmation at the physical layer in 5G programming characterized organizing based HetNet. In particular, the one of kind remote channel qualities between a client and the access point (AP) are separated as the security context information (SCI) and moved to the objective AP. The last decides if the client is the genuine one who has just been verified by the got SCI. They at that point dissect the verification execution identifying with various properties and results show that the validation quality can be adaptively balanced. Besides, they locate that ideal execution can be accomplished by setting an appropriate choice limit and determine the problematic exhibition by iterative inquiry. Ultimately, examination and reproductions on inactivity and overhead contrasted and existing ones are directed and results demonstrate the adequacy of the proposed plan.

Table 2. Representative Summary of above Survey

Sl. No	Author & Year	Method	Work	Conclusion	Comments/Observations
1	Ihsan Abdulqadder et al [2]-2018	Highly Secured Authentication and Handover Mechanism (HSAOHM) Scheme. Tree-Based Switch Assignment (TBSA) algorithm.	A robust security scheme is presented in the 5G network to resolve major security threats such as authentication handover, flow table overloading attack, and DDoS attack in the network.	HS-AHOM scheme is not only highly secure but also preserves user privacy.	Resolve control plane saturation attack in to strengthen the proposed security scheme.
2	Jun Wu et al [4]-2018	Secure Authentication for Cluster Control	Big data analysis-based secure cluster management architecture for the optimized control plane is proposed. A secure authentication scheme was proposed to ensure the legality of the data sources.	Work is significant in improving the performance and efficiency of applications running in SDN	A distributed security data storage scheme for the SDN controller cluster will be proposed
3	Gengshen Lin et al [5]-2019	VSF instances premigration algorithm	Focus on the resource-exhausted attacks to virtual security functions in the SDN-enabled smart grid and proposed a moving target defense mechanism by migrating VSF instances dynamically	Proposed a premigration algorithm to migrate VSF instances before their resources are exhausted.	Research would be conducted to discuss practical deployment and design more lightweight algorithms for the smart grid.
4	Jingjing Xu et al [8]-2018	Attribute-Based Searchable Encryption Scheme	ABSES effectively ensures the security of ciphertext stored in the data centre, and that users cannot obtain unauthorized information or illegal network resources without any certification.	It reduces network bandwidth and local resources, while improving the scalability and flexibility of SDN access control at the meantime.	Future work, we will focus our work on a smarter system that is more flexible for users in SDN.
5	Sugandhi Midha et al [9]-2019	TLS Extension and Defensive Algorithm	Focuses on making SDN OpenFlow communication more secure by following extended TLS support and defensive algorithm.	The enhancement of TLS algorithm has made the authentication stricter and SDN more secure	The security is improved in the authentication process for generating and verifying the identity of either client or server.
6	Jin Cao et al [16]-2019	Capability-Based Privacy Protection Handover Authentication Mechanism	Integrate user capability and Software Defined Network (SDN) technique, and propose a Capability-Based Privacy Protection Handover Authentication Mechanism in SDN-based 5G HetNets.	The proposed scheme has much better performance in security and efficiency compared with the standard handover scheme and other related schemes even if there is an unknown attack.	Achieve the mutual authentication and key agreement between User Equipments (UEs) and BSs in 5G HetNets at the same time largely reduce the authentication handover cost.
7	Ting Ma et al [18]-2017	Fast Physical Layer Based Authentication Scheme	The fundamental an algorithm is developed based on the nonparametric K-S test.	The proposed authentication scheme consumes less computational and storage resources when compared with the GLRT methods	Proposed K-S test based scheme can provide reliable security performance for Complementary authentication purpose.
8	Cong Wang et al [19]-2019	SDN-Based Handover Authentication Scheme	SHAS the scheme achieves not merely mutual authentication but also secret key confidentiality	SHAS scheme can effectively cut down the handover authentication latency with less use of the cryptography operations which have higher computation cost, compared with the CHS scheme and the LMA scheme.	The scheme has high efficiency.

9	Osamah Ibrahiem Abdullaziz et al [20]-2019	Lightweight Authentication Mechanism-Hidden Authentication (HiAuth)	A lightweight authentication solution, called Hidden Authentication (HiAuth), to protect the SDN controller against DoS by hiding the identities of the forwarding devices into the control packets via efficient bitwise operations.	HiAuth can effectively mitigate outsider DoS attacks and provide high undetectability to attackers	HiAuth is the first to incorporate information hiding techniques into OpenFlow to provide security against DoS attacks.
10	Liming Fang et al [21]-2019	New Authentication Scheme called The Hidden Pattern (THP)	The Hidden Pattern (THP), which combines graphics password and digital challenge value to prevent multiple types of authentication attacks at the same time	THP can provide better performance than the existing schemes in terms of security and usability.	THP can resist mainstream attacks and has significant performance.

VII. CONCLUSION

The SDN platform is experiencing many vectors of threat, some of which are introduced across weak authentication and authorization mechanisms, others due to SDN design. To create a secure cloud networking environment controlled by SDN, it is important to consider that threat vector in isolation. This survey aimed at security issues impacting SDN's security, reliability, and availability.

For the SDN data plane, SDN control plane and OpenFlow protocol, the security design objectives and best practices, security countermeasures have been described in detail. Apart from the mechanisms mentioned in this section, the controlled architecture configuration depends on many other factors, such as latency and throughput impact due to a particular secured configuration. Nonetheless, these considerations are beyond the scope of this survey and should be weighed before the recommendations as part of this survey are implemented.

REFERENCES

1. Ihsan H. Abdulqadder ; Deqing Zou ; Israa T. Aziz ; Bin Yuan "Enhanced Attack Aware Security Provisioning Scheme in SDN/NFV Enabled over 5G Network" 2018 27th International Conference on Computer Communication and Networks (ICCCN) Year: 2018 | Conference Paper | Publisher: IEEE.
2. Ihsan Abdulqadder ; Deqing Zou ; Israa Aziz ; Bin Yuan ; Weiqi Dai "Deployment Of Robust Security Scheme In SDN Based 5G Network Over NFV Enabled Cloud Environment" 2018 IEEE Transactions on Emerging Topics in Computing Year: 2018 | Early Access Article | Publisher: IEEE.
3. Sahil Garg ; Kuljeet Kaur ; Georges Kaddoum ; Syed Hassan Ahmed ; Dushantha Nalin K. Jayakody **"**SDN-Based Secure and Privacy-Preserving Scheme for Vehicular Networks: A 5G Perspective" 2019 IEEE Transactions on Vehicular Technology Year: 2019 | Volume: 68, Issue: 9 | Journal Article | Publisher: IEEE.
4. Jun Wu ; Mianxiong Dong ; Kaoru Ota ; Jianhua Li ; Zhitao "Guan Big Data Analysis-Based Secure Cluster Management for Optimized Control Plane in Software-Defined Networks" 2018 IEEE Transactions on Network and Service Management Year: 2018 | Volume: 15, Issue: 1 | Journal Article | Publisher: IEEE.
5. Gengshen Lin ; Mianxiong Dong ; Kaoru Ota ; Jianhua Li ; Wu Yang ; Jun Wu ICC **"**Security Function Virtualization Based Moving Target Defense of SDN-Enabled Smart Grid" 2019 IEEE International Conference on Communications (ICC) Year: 2019 | Conference Paper | Publisher: IEEE.
6. Rajat Chaudhary ; Gagangeet Singh Aujla ; Sahil Garg ; Neeraj Kumar ; Joel J. P. C. Rodrigues **"**SDN-Enabled Multi-Attribute-Based Secure Communication for Smart Grid in IIoT Environment" IEEE Transactions on Industrial Informatics Year: 2018 | Volume: 14, Issue: 6 | Journal Article | Publisher: IEEE.
7. Reem Melki ; Ali Hussein ; Ali Chehab **"**Enhancing Multipath TCP Security through Software Defined Networking" 2019 Sixth International Conference on Software Defined Systems (SDS) Year: 2019 | Conference Paper | Publisher: IEEE.
8. Jingjing Xu ; Hanshu Hong ; Guofeng Lin ; Zhixin Sun "A New Inter-Domain Information Sharing Smart System Based on ABSES in SDN" IEEE Access Year: 2018 | Volume: 6 | Journal Article | Publisher: IEEE.
9. Sugandhi Midha ; Khushboo Triptahi **"**Extended TLS security and Defensive Algorithm in OpenFlow SDN" 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) Year: 2019 | Conference Paper | Publisher: IEEE.
10. Jean Claude Nikoue ; Sergey Butakov ; Yasir Malik "Security Evaluation Methodology for Software Defined Network Solutions" 2019 International Conference on Platform Technology and Service (PlatCon) Year: 2019 | Conference Paper | Publisher: IEEE.
11. Haifeng Zhou ; Chunming Wu ; Chengyu Yang ; Pengfei Wang ; Qi Yang ; Zhouhao Lu ; Qiumei Cheng **"**SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices" IEEE/ACM Transactions on Networking Year: 2018 | Volume: 26, Issue: 5 | Journal Article | Publisher: IEEE.
12. Yanbing Liu ; Yao Kuang ; Yunpeng Xiao ; Guangxia Xu **"**SDN-Based Data Transfer Security for Internet of Things" IEEE Internet of Things Journal Year: 2018 | Volume: 5, Issue: 1 | Journal Article | Publisher: IEEE.
13. Ying Qian ; Prabir Bhattacharya ; Wanqing You ; Kai Qian "Security Threat Analysis of SDN Switch Flow Table" 2018 27th International Conference on Computer Communication and Networks (ICCCN) Year: 2018 | Conference Paper | Publisher: IEEE.
14. Ramissa Djouani ; Karim Djouani ; Fateh Boutekkouk ; Roumissa Sahbi "A Security Proposal for IoT integrated with SDN and Cloud" 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM) Year: 2018 | Conference Paper | Publisher: IEEE.
15. Xiao Liang ; Heyao Chen "A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address" 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) Year: 2019 | Conference Paper | Publisher: IEEE.
16. Jin Cao ; Maode Ma ; Yulong Fu ; Hui Li ; Yinghui Zhang **"**CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets" IEEE Transactions on Dependable and Secure Computing Year: 2019 | Early Access Article | Publisher: IEEE.
17. Hui Yang ; Haowei Zheng ; Jie Zhang ; Yizhen Wu ; Young Lee ; Yuefeng Ji "Blockchain-based trusted authentication in cloud radio over fiber network for 5G" 2017 16th International Conference on Optical Communications and Networks (ICOCN) Year: 2017 | Conference Paper | Publisher: IEEE.
18. Ting Ma ; Feng Hu ; Maode Ma "Fast and efficient physical layer authentication for 5G HetNet handover" 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) Year: 2017 | Conference Paper | Publisher: IEEE.

19. Cong Wang ; Yiying Zhang ; Xi Chen ; Kun Liang ; Zhiwei Wang **"**SDN-Based Handover Authentication Scheme for Mobile Edge Computing in Cyber-Physical Systems" IEEE Internet of Things Journal Year: 2019 | Volume: 6, Issue: 5 | Journal Article | Publisher: IEEE.
20. Osamah Ibrahiem Abdullaziz ; Li-Chun Wang ; Yu-Jia Chen **"**HiAuth: Hidden Authentication for Protecting Software Defined Networks" IEEE Transactions on Network and Service Management Year: 2019 | Volume: 16, Issue: 2 | Journal Article | Publisher: IEEE.
21. Liming Fang ; Yang Li ; Xinyu Yun ; Zhenyu Wen ; Shouling Ji ; Weizhi Meng ; Zehong Cao ; M.Tanveer **"**THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN-based IoT Network" IEEE Internet of Things Journal Year: 2019 | Early Access Article | Publisher: IEEE.
22. Ju-Ho Choi ; Sung-Gi Min ; Youn-Hee Han "MACsec Extension over Software-Defined Networks for in-Vehicle Secure Communication" 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN) Year: 2018 | Conference Paper | Publisher: IEEE.
23. Yongli Tang ; Tao Liu ; Xu He ; Jinxia Yu ; Panke Qin **"**A Lightweight Two-Way Authentication Scheme Between Communication Nodes for Software Defined Optical Access Network" IEEE Access Year: 2019 | Volume: 7 | Journal Article | Publisher: IEEE.
24. Tahira Mahboob ; Iqra Arshad ; Aqsa Batool ; Maryam Nawaz **"**Authentication Mechanism to Secure Communication between Wireless SDN Planes" 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST) Year: 2019 | Conference Paper | Publisher: IEEE.
25. Hongyan Cui ; Zunming Chen ; Longfei Yu ; Kun Xie ; Zongguo Xia "Authentication mechanism for network applications in SDN environments" 2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC) Year: 2017 | Conference Paper | Publisher: IEEE.
26. Ke Ding ; Xiulei Wang ; Guomin Zhang ; Zhen Wang ; **"**A flow-based authentication handover mechanism for multi-domain SDN mobility environment" Ming Chen China Communications Year: 2017 | Volume: 14, Issue: 9 | Magazine Article | Publisher: IEEE.
27. Yanling Zhao ; Xinchang Zhang **"**New media identity authentication and traffic optimization in 5G network" 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) Year: 2017 | Conference Paper | Publisher: IEEE.
28. Jing Yang ; Xinsheng Ji ; Kaizhi Huang ; Yajun Chen ; Xiaoming Xu ; "Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet" Ming Yi IET Communications Year: 2019 | Volume: 13, Issue: 2 | Journal Article | Publisher: IET.

AUTHORS PROFILE

Mr. Ravindra.S. completed M.Tech in the year 2003 from NITK Surathkal and currently doing Ph.D under VTU in the field of Electronics and Communication Engineering. He has 16 years of rich experience in Academics.He has published many papers in National and International Journals. He holds lifetime ISTE membership. His research area includes Wireless Networking, Security in Mobile Communication.

Dr. Shankaraiah received his Ph.D. in the year of 2012 from IISc Bangalore and currently working as a Professor and Head in the Department of Electronics and Communication Engineering at JSS Science and Technology University (Formerly SJCE), Mysore. He has 23 years of rich experience in Academics. He has published more than 25 research articles in National and International Journals. His research area includes Wireless Networking, Hybrid wireless Networks, Context-Aware Computing, Ubiquitous Networks, Security in Mobile Communication, Privacy Issues in WSN.