IJEIT
The International Journal of Engineering and Information Technology
journal homepage:www.ijeit.misuratau.edu.ly
MISURATA UNIVERSITY

Distributed SDN Security Frameworks: A Survey

Eng. Mahmoud Nabeeh Houri
Syrian Virtual University
Syria – Damascus
Eng.mahmoud_houri@hotmail.com

Abstract— **Software-Defined Networks (SDN) have recently received much attention and deployment as a new technology that offers more flexibility and efficiency than traditional networks. SDN is a paradigm shift that revolutionizes traditional network design and makes future networks programmable, manageable, and affordable. The use of the SDN in modern networks provides much needed flexibility and transparency to organize and deploy network solutions. It is a new model that separates forwarding & controlling planes, and centralized architecture designed to increase network speed and programming capability. However, from the current security point of view, the SDN still has some problems, especially for the advanced persistent attacks such as the DDOS, the side channel attacks in Clouds, the SDN stack control plane saturation attacks, and the switch flow table exhaustion attacks. Also, the existing SDN-based security systems are constrained by a central framework that provides significant overheads for the control plane, leading to the breakdown of vital control links.**

In this paper, we will present the vulnerabilities and security threats in the SDN network, define the various approaches to solve these problems, and deploy the SDN securely in the production environments. We will survey existing research on distributed SDN security frameworks, there is a number of security frameworks and applications that have been proposed previously, and each one of them builds on a selection of the SDN characteristics.

Index Terms: **SDN, Monitoring, Network Security, Distributed Control, Scalable Security.**

I. INTRODUCTION

Today's internet applications require the underlying networks to be fast, carry large amounts of traffic, and to deploy a number of distinct, dynamic applications and services. Adoption of the concepts of inter-connected data centers and server virtualization has increased network demand tremendously.

In addition to various proprietary network hardware, distributed protocols, and software components, legacy networks are inundated with switching devices that decide on the route taken by each packet individually. The importance of software defined networks is that they provide centralized control and management, and they are programmable and open sources allowing more flexibility in design, implementation, management, time improvement, speed, reliability and security in addition to solving problems and overcoming errors in line with the needs of future and services for networks. Managing network infrastructure devices in this way will greatly reduce construction costs which is an important goal that all companies aspire to for saving their capital. The SDN networks offer promising network management opportunities in terms of simplicity, programmability and flexibility. These opportunities were quickly identified by major industry companies that started early in funding research projects aimed at developing the SDN. Today, major network providers such as Cisco announced the launch of network infrastructure which supports the SDN, furthermore it transforms the model into what is required to manage data centers and clouds. Also, the global market for software-defined networking solutions and services is expected to grow by 54 % at a compound annual growth rate over the next few years according to a research report by Global Market insights.

In the following, there are some of the SDN software products: Cisco DNA Center, IBM Cloud Internet Services, Juniper Networks offers Contrail Networking, Masergy SD WAN, Blue Planet Open Network operating system, DX Virtual Network Assurance (formerly CA Virtual Network Assurance).

In SDN-based networks, the part of the policy rules to access the network functions is distributed and delegated via Data Plane (OpenFlow) switches, thus network policies, traffic and security configuration, QOS functions (such as intrusion detection and prevention), network virtualization and bandwidth management access control is enforced via OpenFlow switches through controlled flow rules that are programmed by dedicated SDN applications in Application Plane, and unfortunately this programmable behavior can significantly expand the size of the attack on the entire SDN network.

We can summaries the advantages offered by the SDN as follows: Greater breadth of control network analysis and response, better intelligence with a comprehensive view of the network rather than viewing every element of the network from its own perspective. Improved app experience and delegation of network owner / operator,

Received 28 Sep ,2020; revised 27 Oct, 2020; accepted 3 Nov, 2020.

Available online 25 Oct, 2020.

rapid deployment of applications using networks that support specific application needs, simplified management and IT mechanism, an opportunity to open the network to various vendors.

To address all the previous challenges, several frameworks and applications have been proposed in advance based on a set of properties for SDN. In this article, we will present security frameworks for the SDN network and define the security system presented by SDN properties. Also we will presents the latest current security framework prepared for SDN.

The remainder of the paper is structured as follows: Section I, SDN Security, Section II, State of article for SDN Security Framework, Section III, Comparison between the different Security Frameworks, Section IV, Latest SDN security framework, Section V, SDN Structure, Section VI, Difficulties to moving to SDN, Section VII, Vulnerabilities and Security Threats, Section VIII, Security measures of SDN and research into the protection of SDN networks, Section IX, Challenges, Section X, Conclusion and Future Aspects.

I. SDN SECURITY

The SDN security needs to be built into the architecture, as well as to be delivered as a service to protect the availability, integrity, and privacy of all connected resources and information.

Within the architecture, you need to the following points: Secure the Controller: as the centralized decision point, access to the SDN Controller needs to be tightly controlled.

Protect the Controller: if the SDN Controller goes down (for example, because of a DDoS attack), so goes the network, which means the availability of the SDN Controller needs to be maintained.

Establish Trust: protecting the communications throughout the network is critical. This means ensuring the SDN Controller, the applications loaded on it, and the devices it manages are all trusted entities are operating as they should.

Create a Robust Policy Framework: that needs a system of checks and balances to make sure the SDN Controllers are doing what you actually want them to do.

Conduct Forensics and Remediation: when an incident happens, you must be able to determine what it is, recover, potentially report on it, and then protect against it in the future.

II. SDN Security framework: state of the ART

In this section, we will show an overview of some proposed solutions concerning the security of the SDN networks.

FRESCO is a security application which applies the OpenFlow framework consisting of reusable modular libraries that can be connected together to build more sophisticated security applications. FRESCO assists the developers compose the necessary modules to produce the required security functions, like firewalls, IDS, and scan detections.

FLOWGUARD is a framework introduced to build robust SDN firewalls. FLOWGUARD provides a real-time violation resolution mechanism. Whenever the network states are updated, or the configurations are changed, it checks and compares the flow path spaces against the specified authorized space in the firewall to detect firewall policy violations.

SDNSOC is an SDN Security Operation Center which handles policy composition at application plane, flow rule conflict detection and resolution at the control plane. It follows the design principles of object-oriented paradigm such as code-re-utilization, methods abstraction, and an aggregation for the implementation of SDNSOC on a multi-tenant cloud network. The key benefits obtained using this approach are the network administrator is abstracted from complex implementation details of SFC.

SDN4S is a system and solution to minimize the time between incident detection and resolution by using automated countermeasures based on Software-Defined Networking (SDN). SDN4S creates incident-specific response workflows orchestrating actions and network-based countermeasures automatically upon receiving an alert, leading to faster and more predictable incident response.

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

Open Source SDN Project Delta is a new SDN security evaluation framework with two main functions: a) it can automatically instantiate attack cases against SDN elements across diverse environments. b) It can assist in uncovering unknown security problems within an SDN deployment. Actuated by the existing pen-testing tools for traditional networking, DELTA is considered to be one of the prior works envisaged for benchmarking the SDN devices integrated with specific fuzzing techniques to determine concealed security flaws.

SECCONTROL is a new network protection framework bridging the gap between security tools and SDN technologies, to provide sufficient protection capabilities in an SDN environment. It is designed on a new security control layer above SDN controllers, which releases SDN controllers from security processing pressure. SECCONTROL is able to perceive the real-time security threats, generate real-time defense reactions, and adjust corresponding network behaviors dynamically. With SECCONTROL, security engineers can easily add different security tools into the protection boundary and make use of their detection abilities to serve the entire network.

DELTA is a new SDN security evaluation framework, which can automatically instantiate attack cases against SDN elements across diverse environments, and which

may assist in uncovering unknown security problems within an SDN deployment. Motivated by security testing tools in the traditional network security domain. DELTA represents the first security assessment tool for SDN environments.

TENNISON, a distributed SDN security framework built on a multi-level remediation mechanism offers the ability to perform light-weight monitoring across a large number of flows whilst offering the capability to perform Deep Packet Inspection (DPI) on a selection of flows. This framework is considered as the most recent security framework designed for SDN.

III. COMPARISON BETWEEN THE DIFFERENT SECURITY FRAMEWORKS

In the following, we will review some comparisons between SDN security frameworks and compatible controllers as shown in table [1].

Table 1. Scalability comparison of SDN securtity systems

System Name	Controller	Multi-Level Monitoring	OF Response Methodology	Attack Detection	Distribution	SIEM-Like Human Interface
TENNISON	ONOS	Yes	Hybrid	Yes	Yes	Yes
FRESCO	NOX	NO	Reactive	Yes	NO	NO
CIPA	POX	NO	Reactive	Yes	NO	NO
SDN4S	HIPE VAN	NO	Reactive	Yes	NO	Yes
PSI	ODL	NO	Reactive	Yes Via NFV	Yes	NO
ATHENA	ONOS	NO	Reactive	Yes	Yes	NO
OFX	RYU	NO	Hybrid	Yes	Yes	NO

IV. Latest SDN security Framework– Tennison

The TENNISON framework is a multi-level framework for the distributed monitoring and treatment of SDN networks due to its unique safety pipeline. TENNISON also provides lightweight visibility across a large number of streams. The ability to distribute is also supported with multiple control instances, tunneling for efficient attack detection and treatment, and multi-level monitoring. In addition, the TENNISON framework provides the ability to perform deep Packet Inspection (DPI) on a select group of streams. The TENNISON framework stimulates the desire to provide an adaptive, extensible security platform that is technology independent and able to support a wide range of security functions. TENNISON does not eliminate control unit interaction requirements as described in Avant-Guard and OFX. However, the level of controller interaction is flexible and commensurate with the requirements of threat detection, aided by the use of other monitoring and inspection tools that are deployed on the network which relieves pressure from the control channel in the SDN.TENNISON is a next generation safety framework with the following features: Efficiency and proportionality, Scalability and visibility, Programmability and extensibility, Transparency, Availability and flexibility, the possibility of interoperability.

V. SDN Structure

The Open Networking Foundation (ONF) defined the SDN architecture as a three-tiered model: A) Application Layer, B) Control Layer, C) Infrastructure Layer.

Application Layer: it consists of services and applications provided by the network to the user such as network simulation, quality of service (QOS), Routing Filter ACL, traffic shaping, access control, bandwidth management and others where this layer communicates with the control layer via APIs. Via these interfaces, the network is programmed to provide its services and applications in any of the programming languages. This layer corresponds to the application layer in the traditional network architecture and takes this single or multiple representations as an input. A specific algorithm is implemented to find a routing policy that achieves specific objectives such as reducing delay and then returns a set of routing rules passed to the network operating system layer in the control layer.

Control Layer: The central control point represents the network devices such as giving commands to switches and routers to take the control and management function from all the infrastructure devices and leaves it to pass and direct data only, so the control and management of the network is done through the master device that represents this layer and can be considered the mind of the SDN technology, and it has different types. The controller communicates with the rest of the network devices that have been decommissioned to transmit the services and applications to be activated through a common language called OpenFlow protocol between the control layer and the infrastructure layer.

The control layer is responsible for monitoring the network, making routing decisions, and programming the network on how to behave.

The control layer consists of the network operating system layer that is connected to each switch in the network over a dual link in order to collect status information from network switches (such as link delays, connection usage) and then passes this information to the network abstraction layer that also contains it, which in turn extracts an appropriate representation of the network because there is a comprehensive view of the entire network, and the control layer has a northern interface to deal with the application layer.

Infrastructure Layer: it consists of other network devices (Forwarding Plane) that receive and execute commands from the control layer and handle the control layer. It is the physical layer responsible for collecting the network statuses such as traffic statistics, network topology, network usage, etc. and send them to the control layer.

VI. Difficulties to moving to SDN

The biggest problem for the rapid transition to SDN is moving from the current infrastructure with its design, criteria and management to this new approach. Everything from infrastructure to industry must have very special capabilities to work with that new technology, but if the advice here helps us to move our network to the SDN, there is a set of constrictions, points, notes and quick questions that must be taken into consideration during the development of the network to work with the SDN technology, so that the transition to the SDN technology is passed smoothly and free of risks or failures.

The First key: Why do I want to switch my network to the SDN? What is the benefit behind it? What are the initial steps to be taken to achieve the SDN transition goal? Are there options to switch to the SDN? Which one is the most appropriate in my case?

The Second Key: Divide your existing networks and infrastructure into four main domains, for example we can divide them into:
Campus or LAN, Edge, Data Center, Internet Service Provider or WAN. The Third key: think about the methods, tools, systems, and even people who will help you move each of these four domains separately to the SDN. The Fourth key: Start by setting up your SDN transition plan and set up your network for it, making it a simple and clear plan to help everyone overcome the resistance to change to what's new.
The Fifth key: Study the transition cost of the physical SDN as well as the time required.

The Sixth key: You have to take advantage of others' experiences and start where they finished by reading what the available experiences, books and researches, and rearrange your papers if you find a better course. The last one: Make sure you document everything during this long journey.

VII. Vulnerabilities and security threats

Security threats to the SDNs can be classified in three main categories based on the target or affected SDN layer as shown in Table [2].

Table 2. Categorization of the security issues associated with the SDN Framework by layer/interface affected

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	APP-ctl interface	Control Layer	Ctl-data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access			X	X	X
Unauthenticated Application	X	X	X		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					
Forwarding Policy Discovery (Packet Processing Timing Analysis)					
Data Modification e.g.					
Flow Rule Modification to Modify Packets			X	X	X
Malicious Applications e.g.					
Fraudulent Rule Insertion	X	X	X		
Controller Hijacking			X	X	X
Denial of Service e.g.					
Controller-Switch Communication Flood			X	X	X
Switch Flow Table Flooding					X
Configuration Issues e.g.					
Lack of TLS (or other Authentication Technique) Adoption			X	X	X
Policy Enforcement	X	X	X		

And the most common ways to attack SDN are: Unauthorized Access, Data Modification, Data Leakage, DOS, and Malicious Application Configuration Issues. Most security problems that may arise as a result of attacks on the SDNs are: Interception and change of Control Plane packets, and a change in the installed programs of the network component with other malicious programs. Disable the installed programs for the network component as a conversion to programs of an old version. The following is a general explanation of the threats to sensitive functions and communication channels in the SDN structure as shown in Figure [1].

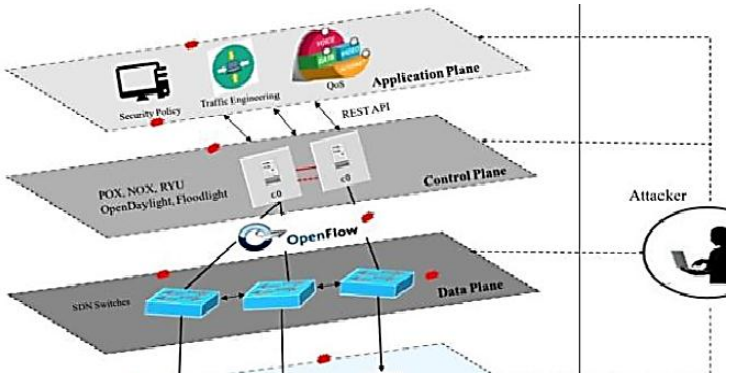

Figure [1]. Attacker Searching for Potential Targets

VIII. Security measures of SDN and research into the protection of SDN networks.

The researchers applied countermeasures to counter attacks via custom programs, modifications, or additions to SDN elements. Protection and vulnerability reduction measures are categorized as Data Plane or OpenFlow switcher, Control Controller and the communication channel between Control Plane and Application. Many researches devoted to finding possible security countermeasures that could be taken for attacks in Table [2], the countermeasures collected in Tables 3 and 4 by target area and affected by the attack.

Table 3. Categorization of Security Solutions

Solution to security issue	Research work	SDN Layer / Interface				
		App	App -Ctl	Ctl	Ctl - Data	Data
Unauthorized Access	Securing Distibuted control, Byzantine – Resilient SDN			×	×	
	Authentication For Resillience			×		
	PermOF	×				
	Operation Checkpoint	×	×	×		
	SE-Floodlidht	×		×	×	
	Authflow	×	×	×	×	×
Data Leakage						
Data Modifications						
Malicious Applications	Fortnox	×	×	×		
	ROSEMARY	×		×	×	
	LogoSDN	×	×	×		
Denial of Service	AVANT – GUARD, CPRecovery			×	×	×
	VAVE	×		×	×	×
	Delegating Network Security	×	×	×	×	×
Configurations Issue	NICE		×		×	
	FlowChecker,Flover,Anteater,VeriFlow,NetPlumber	×	×	×	×	
	Security-Enhanced Firewall, FlowGuard, LPM	×		×	×	
	Frenetic,Flow-Based Policy, Consistance Update	×	×	×	×	×
	Shared Data Store	×		×	×	
	Splendid Isolation	×	×	×		×
	Verificare, Machine-Verified SDN, VeriCon		×	×	×	
System Level SDN Security	Debugger for SDN					
	OFHIP, Secure-SDMN	×			×	
					×	
	FRESCO	×	×	×	×	

Table 4.Summary of Security Comparisons at SDN

Security Comparison at Switch Level					
Technique	**Year**	**Confidentiality**	**Integrity**	**Availability**	**Attacks**
DIFANE	2010	✓	✓	✓	STRIDE,DOS, DDOS,MITM (Main in the middle)
FLOWCHECKER	2010	✓	✓		
KANDOO	2012	✓	✓	✓	
VERIFLOW	2012	✓	✓	✓	
OF-GUARD	2014	✓	✓		
FLOWMON	2015	✓	✓	✓	
FS-OPENSECURITY	2016	✓	✓	✓	
Security Comparison at Controller Level					
Technique	**Year**	**Confidentiality**	**Integrity**	**Availability**	**Attacks**
VAVE	2011	✓	✓	✓	Hijacked, Controller, Malicious, Application,
NICE	2012	✓	✓		
FOR-NOX	2012	✓	✓	✓	
FRESCO	2013	✓	✓	✓	
FLOWGUARD	2014	✓	✓		
SE-FLOODLIGHT	2015	✓	✓	✓	
FS-OPENSECURITY	2016	✓	✓	✓	
Security Comparison at Communication Channel					
Technique	**Year**	**Confidentiality**	**Integrity**	**Availability**	**Attacks**
FLOWVISOR	2010	✓	✓		DOS/DDOS
AVANT-GUARD	2013	✓	✓	✓	CONTROL-DATA
LINESWITCH	2015	✓	✓	✓	LINKE PLANE
UMON	2015	✓	✓		ATTACKS
SPHINX	2015	✓	✓		
OFX MOUDEL	2016	✓	✓	✓	BUFFER SATURATION
FS-OPENSECURITY	2016	✓	✓	✓	ATTACK

The following are some of the techniques used to protect the SDN networks:

A. Difane

Network mechanisms rely highly on the SDN controllers, resulting in problems with scalability and degradation. The researchers found the Difane technique to quickly and easily track network flow in Data Plane is by extracting sensitive or specific flows through open and intermediate Vswitches that stores certain flow rules. The Difane structure includes a built-in distributed controller with an authority switches that act as a subset of existing SDN open Vswitches or legacy switches (including ingress/egress switches) that include immense memory and processing capacity. When traffic from the host port does not match the flow table in the open Vswitches, the ingress switch directs the traffic to the corresponding authority switch unit. The corresponding switch in the Difane structure sends the response to the ingress access switch, after which the next network packets corresponding to the flow rules are forwarded directly to the egress switch.

B. Avant-Guard

It is introduced to the Vswitches that integrates two modules, the communication transmission module in Vswitches to detect network saturation attacks such as TCP SYN attacks, and the trigger catalyst to continuously report network status and advance header and payload information for Control Plane, this technology protects flood control.

C. Line Switch

Data Plane-level solution and Avant-Guard policy enhancement to detect buffer fullness and to manage proxy connection status via delayed TCP connection transfer method.

***D.** OpenFlow Extension Framework – OFX*

Avant-Guard is a custom OpenFlow add-on and modules coming from another OFX module. Avant-Guard and Line Switch both experience performance of the load, and the distribution challenges. OFX enables reliable SDN applications within the OpenFlow architecture via dynamic load modules that include security applications such as BotMiner and DDOS Finder, OFX modules contain a library as a prerequisite for performing specific network monitoring tasks that are tightened as a new security function that enables the Data Plane OFX agent to handle unit packets.

E. Kandoo

Kandoo is a technology that ensures a safe, scalable and scalable control level by switching SDN switches with effective discharge of control applications; the two-layer controllers are encapsulated in a Kandoo working environment that program a set of controllers at the bottom layer and a logical distributed controller on the top layer to maintain the technical state. The Kandoo working environment allows operators to replicate controllers in the SDN network, and this may result in inconsistent traffic.

F. Flood Guard

Defensive Mechanism is an independent, effective protocol which use relies on a proactive flow rule analyzer that efficiently analyzes real-time flow rules and transmits packets in order to prevent overloading of the controller results in a table or packet loss via packet buffering in an SDN controller using threshold limit algorithms.

***G.** Open Source SDN Project Delta*

Work environment with two main functions: It can automatically create attack situations against SDN elements in various environments.

It can help detect unknown security issues in the SDN. This technology can be considered as an assessment technology for embedded SDNs with spurious techniques to identify hidden security flaws.

The below figure describes the deferent technologies to protect SDN.

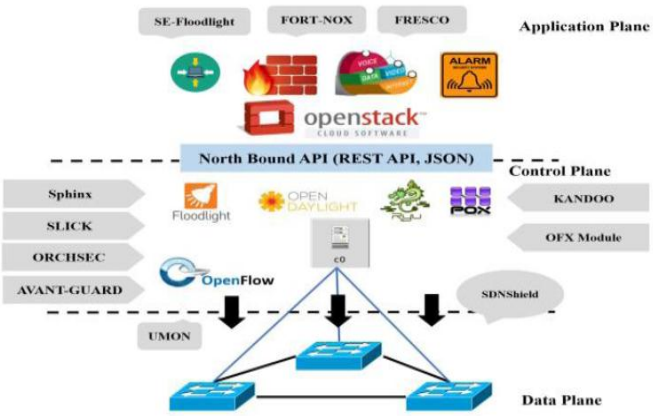

Figure [2].Different Approaches for Securing SDN Architecture

IX. CHALLENGES

The SDN is the next generation of future network infrastructure because of its advantages over traditional networks. Before an enterprise adopts the SDN, it needs to ensure that the technology is well-proven, has low-risk, and will help them achieve their core business goals. Companies need wired and wireless equipment to provide connectivity to their users and want to minimize capital expenditures. At the same time, they must provide their users with security, reliable connectivity, and high performance. Here are some of the benefits that all companies want to achieve: improved security, low operating costs, and better user experience. In the following paragraph, we will review some of the scientific articles that talk about the practical investments of the SDN and the advantages of these networks.

The researchers in [3] presented a scientific paper containing a survey on the latest developments on the integration of 5G with SDN. (5G) SDN-based easy and concise vision of emerging trends by 2020. The below figure [3] describes the SDN based cellular network.

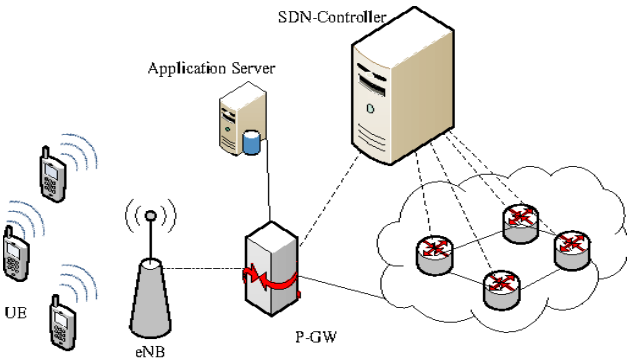

Figure [3]. SDN Based Cellular Network

Also, researchers in [5] presented a paper containing a study on how to programmatically use networks with wireless networks and the features that will be utilized by improving the control of wireless network resources. Encryption and decryption for an access point.

The researcher in [6] also provide a scientific paper containing a study on the SDN and the role of these networks in industrial control systems, and how this leads to an SDN network engineering with lower engineering cost as well as strengthening management systems control.

In another paper, [7] researchers presented a paper describing a general model for integrating the SDN and IoT through the general flexibility and programming provided by software-defined networks and their immense ability to control and apply these benefits to the Internet of Things (IoT), thus solving some of the key challenges they uncover the ability to allow devices connected to heterogeneous networks to communicate with each other.

Figure [4] describes the integration overview between SDN and IOT.

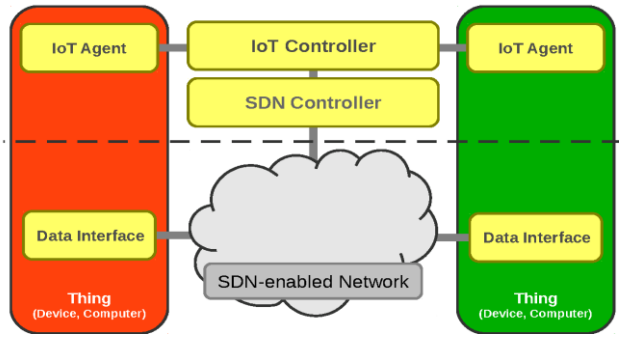

Figure [4]. Integration Overview

In another paper [4], the former researcher presented a paper containing a study showing how to apply the SDNs to automate libraries in order to bring your own devices (BYOD) to access the library's online resources.

X. CONCLUSION AND FUTURE ASPECTS.

There is no doubt that the SDN technology is the next generation of future network infrastructure because of its advantages over the traditional networks. The SDN is a common research area in recent years, especially in terms of traffic engineering, network coordination, quality of service and security. However, these networks still have problems to be overcome, and the most important one is the security. Therefore, the SDN needs to be further developed and proved to be safe and deployable. In this paper, we presented a comprehensive study on the weaknesses, threats and risks in the SDN architecture. We also presented the security frameworks that are currently used to protect the SDN network. In addition, we focused on the last security framework prepared for SDN network, and our future work involves automating the metering process for TENNISON framework, including providing additional controllers to meet network overload. Also according to the P4 matures and the SDN concept, new attack identification methods can be introduced to TENNISON with the potential to improve the security pipeline. In addition to that, we will define the techniques used to protect the SDN networks. We also aspire to improve the overall network security, specifically the SDN stack, by advancing the state of the art through optimizations and hardened-network-operating-system.

REFERENCES

[1], Lyndon Fawcett, Sandra Scott-Hayward, Matthew Broadbent, Andrew Wright, and Nicholas Race, "*A Distributed SDN Framework for Scalable Network Security*," vol. 36, 2018.

[2], Prabhakar Krishnan and Jisha S Najeem, *"A REVIEW OF SECURITY THREATS AND MITIGATION SOLUTIONS FOR SDN STACK*," International Journal of Pure and Applied Mathematics, vol. 115, no. Special Issue, pp. 93-99, 2017.

[3], Sahrish Khan Tayyaba, Munam Ali Shah ،"*5G Cellular Network Integration with SDN: Challenges, Issues and Beyond* "،2018.

[4], A. Yusuf ،"*5 -Software Defined Networking (SDN) Application for Bring-Your-Own-Device (BYOD) Implementation in Library Automation.2016 "*،

[5], Kristián Košťál, Rastislav Bencel,Michal Ries,Peter Trúchly and Ivan Kotuliak ،"*High Performance SDN WLAN Architecture*.2019 "،

[6],. K´alm´an ،"Prospects of Software-Defined Networking in Industrial Operation.2016

[7], Pedro Martinez-Julia, Antonio F. Skarmeta ،"*Empowering the Internet of Things with Software Defined Networking*".

[8], Simply SDN, Adel Hmide, Fouad bin Omran.

[9], Ankur Chowdhary, Dijiang Huang, Gail-Joon Ahn,Myong Kang, Anya Kim and Alexander Velazquez ،"*Object Oriented SDN Framework*،" 2019.

[10], S. Scott-Hayward ،"SDN Security – What's done, what's next?، " 5 2017 .Available: http://itc.committees.comsoc.org/files/2017/07/Scott-ITCMeeting-May2017.pdf.

[11], SDN 101: Networking Foundations Guide, SDxCentral Staff. https://www.sdxcentral.com/networking/sdn/definitions/security-challenges-sdn-software-defined-networks/.

[12], SDN4S: Software Defined Networking for Security. Theo Koulouris, Marco Casassa-Mont, Simon Arnell, HPE-2017-07.

[13], Bridging the Gap between Security Tools and SDN Controllers, 2018 Li Wang and Dinghao Wu.

[14], DELTA: A Security Assessment Framework for Software-Defined Networks. Seungsoo Lee, Changhoon Yoon, Chanhee Lee, Seungwon Shin, Vinod Yegneswaran, Phillip Porras.

[15], WHAT IS SOFTWARE-DEFINED NETWORKING. Published By - Brian Curtis. https://www.yourtechdiet.com/blogs/software-defined-networking-sdn/
[16], Software Defined Networking (SDN) Products. https://www.trustradius.com/software-defined-networking.
[17], Software defined networking: State of the art and research challenges. Manar Jammal, Taranpreet Singh, Abdallah Shami, Rasool Asal, Yiming Li