International Journal of Wireless Information Networks (2022) 29:314–340
https://doi.org/10.1007/s10776-022-00561-y

Security & Privacy in Software Defined Networks, Issues, Challenges and Cost of Developed Solutions: A Systematic Literature Review

Naveed Ahmed[1,2] · Kamalrulnizam Abu Bakar[1,2] · Fatima Tul Zuhra[1,2] · Tanzila Kehkashan[1,2] · Muhammad Akram Mujahid[1,2] · Muhammad Siraj Rathore[1,2] · Muhammad Dawood[1,2] · Babangida Isyaku[1,2]

Received: 16 February 2021 / Revised: 28 December 2021 / Accepted: 18 May 2022 / Published online: 23 June 2022

Abstract

Due to fast development in digital systems, the traditional network architecture is becoming inadequate for the requirements of new technologies such as Cloud Computing, Internet of Things, Bring Your Own Device and for the expansion of internet services. These technologies and services need large-scale computing, high resource availability, dynamic infrastructure tailoring, automation, resilience, holistic knowledge and other needs, still network design demonstrated unmanageable in term of flexible network deployment, dynamic system configuration, agile system estimation, and adaptable system sending. Because of unaltered design of legacy network for recent decades and dynamic nature of modern applications, Software Defined Networks (SDN) has imagined as rising methodology giving programmability, traffic management and adaptive configuration. As SDN architecture gives intelligible centralization and agility to respond to changing demands it additionally presents new attacks conceivable threats and potential security dangers to make it vulnerable and even compromised. Still, on the other side, SDN faces many security challenges, many kinds of new security issues introduced with the advent of SDN. Therefore, an efficient literature review is carried out to collect the issues that most state of the art in SDN security. Systematic Literature Review (SLR) is a collection of 69 well-known papers that are published from 2014–2020. SLR's objective is to study SDN threats, its causes, target planes, cost of developed solutions, and challenges that are related to security. This SLR proposed the layered solution under consideration of advances and threats of technology, in which each layer finds the varying security attacks, its causes, and their proposed solutions. Moreover, to facilitate the future direction related to the security of SDN and privacy, some open problems and challenges are presented. This study will provide a new horizon for future research on SDN security.

Keywords Network Security · Software Defined Networks (SDN) · SDN Threats · SDN security · Vulnerabilities · SDN Architecture · SDN cost · Issues

✉ Naveed Ahmed
naveed@graduate.utm.my

Kamalrulnizam Abu Bakar
knizam@utm.my; knizam@graduate.utm.my

Fatima Tul Zuhra
fatima-tul-zuhra@utm.my;
fatima-tul-zuhra@graduate.utm.my

Tanzila Kehkashan
tanzila@graduate.utm.my

Muhammad Akram Mujahid
akram.mujahid@ue.edu.pk

Muhammad Siraj Rathore
sirajrathore2009@gmail.com

Muhammad Dawood
mastangalbaloshi@gmail.com

Babangida Isyaku
isyaku@graduate.utm.my

[1] School of Computing, Faculty of Engineering, Universiti Teknology Malaysia, 81310 SkudaiJohar Baurau, Malaysia

[2] Capital University of Science and Technology, Islamabad, Pakistan

1 Introduction

With the advancement of technology, the internet-based system has changed its network requirements such as topology, bandwidth requirements, and routing information. So, the network with hardwired has a little aptitude for dealing with such kind of changes. Software-Defined Network (SDN) emerged as an innovative network architecture that provides flexibility through SDN control to resolve these issues. The idea of SDN was developed by Stanford University for the first time [1]. SDN is a highly adaptable network architecture due to its cost-effective, dynamic, and manageable properties [2]. SDN empowers network performance to be measured by the software beyond the networking devices that deliver physical connectivity. Additionally, it also differentiates the data and control plane [3, 4].

SDN foundation decouples the conventional hierarchal blend of network control and sends limits by engaging the framework control programmable. By secluding the framework's control logic from the underlying switches frequently that forward the traffic, SDN establishment fulfilled current network issues' limitations. With the division of control plane, otherwise called controller managed choices and logic identified with network traffic handling. In contrast, the data plane comprised of organization switches ended up being direct, sending contraptions [142]. Separations of the data plane and control plane enables the network control to be preoccupied and programmable for network services and applications. The control plane is responsible for centralizing the SDN controller and routing of packets [5]. Whereas data plane represents the infrastructure layer, which contains the set of connected devices like SDN routers, switches, hubs, etc., which are managed by the controller. Furthermore, it also depends on transmitting information by making an effective routing order [6].

Moreover, SDN disaggregates the integrated networking stacks to customize the network operation or improve network feature velocity for a specialized environment [143]. In addition to this, SDN's primary role is to enable the administrators and network engineers to respond immediately according to changes in requirements [144]. In this way, the network administrators will be able to shape the central controller's traffic without touching the physical switches by using software to redirect, block or prioritize traffic both globally or individually at the packet level.

In Fig. 1, the SDN framework shows the interaction among SDN layers (application layer, control layer, and the Data layer) along with multiple networking attacks. Figure 2 indicates that a network administrator can establish security policies for the network through the application layer and convey the traffic to multiple safety systems. Furthermore, most of the proposals and security systems depend on the open flow because the open flow is considered a de-facto standard of SDN. Therefore, we have described a layered SDN framework under the open flow scheme.

All the interfaces and layers in the SDN proposed framework are sensitive to specific attacks, which may either target the other layer's elements or compromise the network components in the existing layer.

In recent years, SDN has received lots of attentions from government, industry, and academia, which resulted in deployment or involvement in SDN at various levels as shown in Table 1. According to a survey, top national institutes of United States actively participate in SDN research. Even SDN is taught as a part of course in most top ranked institutes of world. SDN is also being adopted by different campuses, but on the other hand, some concerns were also reported by campuses related the adoption of SDN i.e., lack of required employee skills (30%), security (36%), integration with traditional system (38%), cost (41%) [28]. In the meantime, SDN is also considered as an operational multiplier for military use. Due to overwhelming attention from academia and industry toward SDN, necessitate the rapid standardization activities in community and industry consortia, and Standard Development Organizations [30]. The results delivered by these standardization bodies are reflected as de-facto standards that most of the time came in open-source implementation form. For SDN standardization, Open Networking Foundation (ONF) is playing main role in promoting the SDN adoption through OpenFlow protocols' development. A SDN research group has been created in Internet Engineering Task force (IETF) in order to research for the development of Internet. IETF also published drafts on NFV and SDN security, SDN security requirements etc. SDN has also been opted by networking industry for revolutionizing the networking technologies. For promoting SDN technologies, Yahoo, Verizon, Microsoft, Google, Facebook, Deutsche Telekom formed ONF. In one of Google's backbone network, technology of SDN was deployed. Cisco application infrastructure based on SDN has also developed by Cisco. Lots of other companies are manufacturing SDN products and the market of SDN was surpassed by $35 billion in the year of 2018 [27].

This paper's main contribution is to provide an extensive review of SDN privacy and security issues that have been published till now. After that, the quality assessment of the paper has been presented. Moreover, the analysis shows that finding this research. Furthermore, discussed the SDN security threats on each plane, i.e., Application plane, Control Plane, and Data Plane, including, Spoofing, Tampering, Denial of Service (DoS), Repudiation, and Information

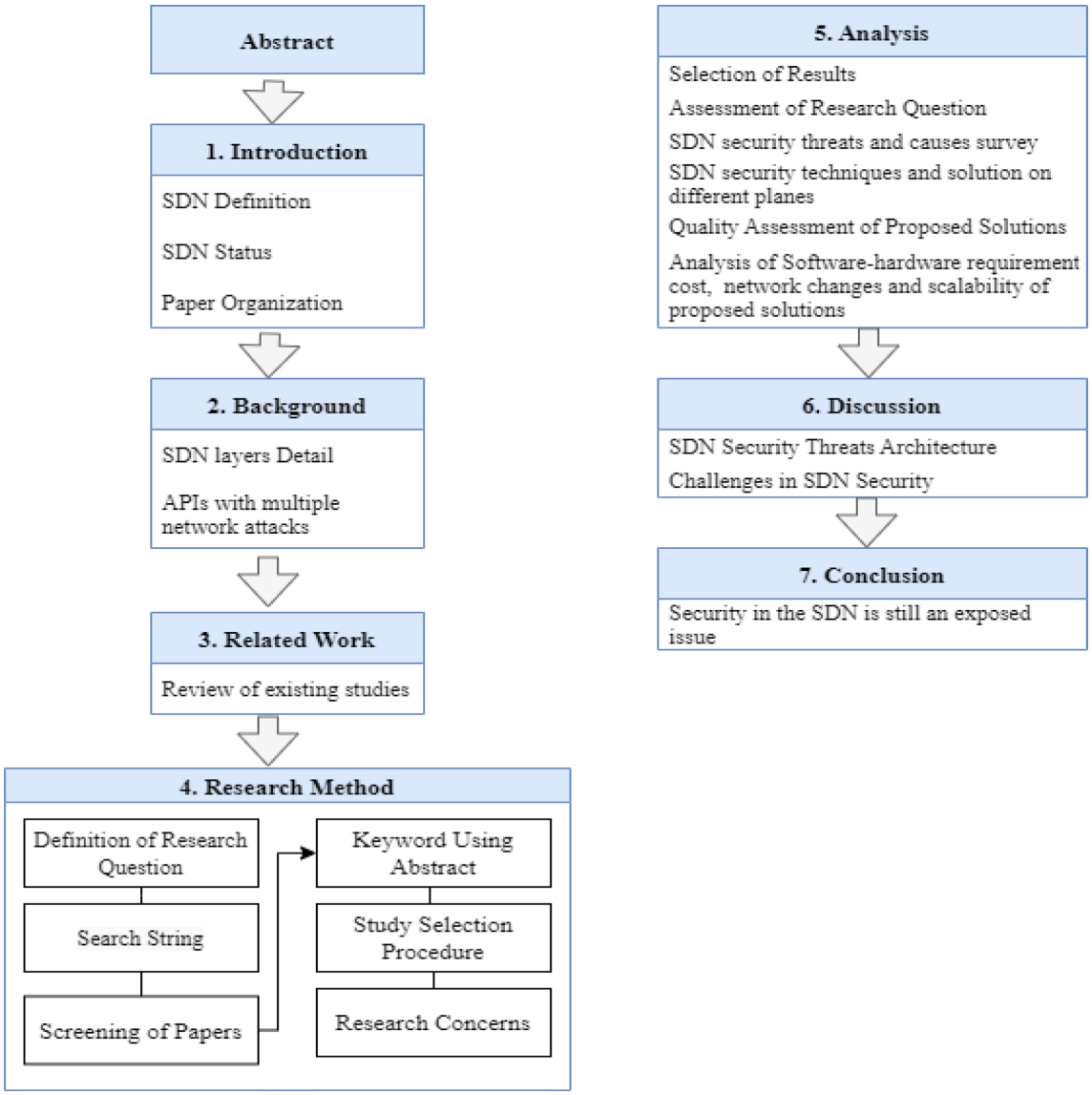


Fig. 1 General view of presented study framework

disclosure. We also identify the different SDNs security solutions as well as primary planes or target levels. At last, we discussed the implementation and deployment cost for SDN security. The general view of this presented review article is given in Fig. 1. The whole paper is structured and conducted as follows: Section 1 provides the basic SDN concept and a brief description of the different layers' security issues. Section 2 presents the background regarding SDN security and privacy issues. Section 3 consists of a research methodology in which we have defined the RQs, quality assessment criteria, inclusion/exclusion criteria, and search string.

Section 4 included the research results in tabular form, which were extracted from the selected papers. Section 5 presents the SDN architecture with possible security attacks and open challenges. Section 6 concludes the whole article.

2 Background

In this section, we have discussed three layers of SDN and southbound and northbound APIs with multiple network attacks (Fig. 3).

2.1 Application Layer

SDN acts as a bridge for applications to manipulate and interact with multiple network devices through control plans. Technically, it is giving an edge to the network to

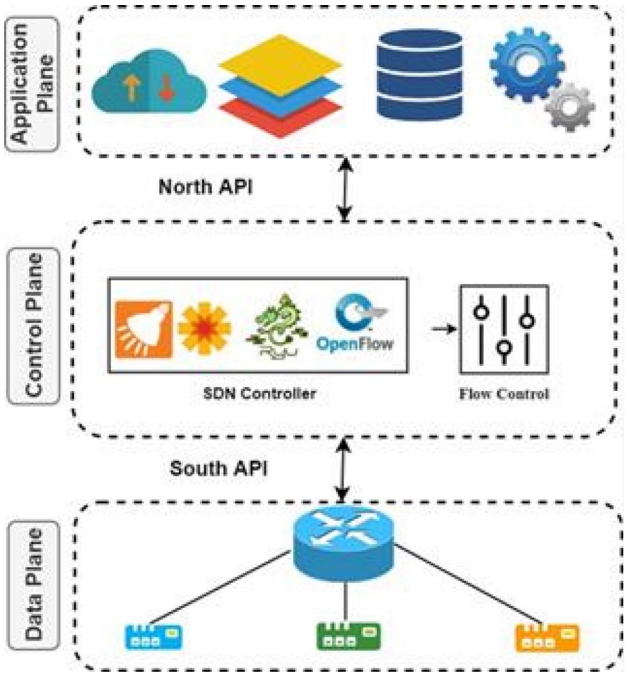


Fig. 2 Basic architecture of SDN

Table 1 SDN adoption rate by government, industry and campus

Network	Evaluating	Deployed
Government	34%	39%
Enterprise	51%	78%
Data Centre	37%	22%
Industry	32%	25%

work simultaneously. Applications take advantage of network visibility in the controller that is why it can request the accessibility of network resources in a specific way. Therefore, it is necessary to create an association among applications with virtual resources such as link discovery, topology, firewall services DNS, etc. Thus, service providers and network administrators have desired to manage, control, and manipulate the policies defined using applications for different network manipulations and configurations [7]. Also, the possible network attacks at the application layer are discussed below.

2.1.1 Termination of an Application by Neglecting the Fixed Authority and Privileges

Control applications and a third party may negotiate to cover the execution of system commands without restricted privileges in network architecture. The system commands are often implemented to shut down or separate the specific applications or network APIs [8–11].

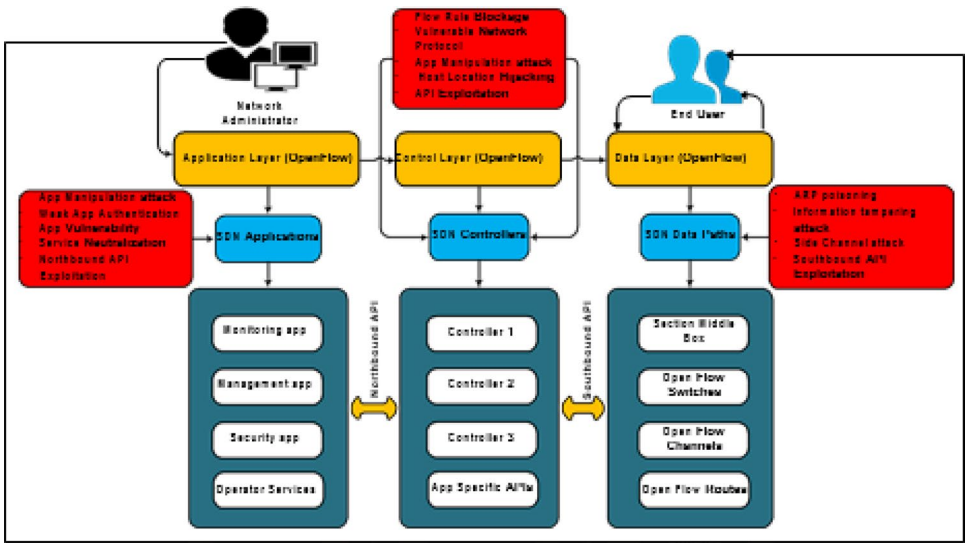
2.1.2 Service Neutralization

On controllers, vulnerable applications are all installed successfully, which can easily manipulate the control handlers. After that, yt7, by disabling the control packets, disruption service is executed to prevent the applications from malicious attacks. Control packets are also inspected to sniff the network information and execute accordingly [10].

2.2 Control Layer

In SDN, the control plane is removed from individual nodes of the network and employed separately in a centralized plane. An entity, which implements the functions of

Fig. 3 SDN layered Framework



the control layer, is referred to as an SDN controller [12]. The controller is an intelligent part of the and is responsible for setting the flow in data path elements such as open flow switches. In open flow based SDN architecture, open flow protocols provide a standard tactic for the controller to communicate with the switch [13]. Whenever a new packet of flow enters into the switch, the switch firstly checks the flow table against that specific packet. After checking it with the existing entries of flow, if it exists, then the instructions regarding the execution of the flow rule; otherwise, it is then forwarded towards the controller.

During this, attackers may avoid firewalls to drop or block flow rules if they implement malicious applications to initiate the conflicting and incompatible flow rules. The attack can overlap by captivating the advantage of the information in which controllers may not identify the conflict between new and old issued rules [9]. Malicious applications and vulnerable network protocols can poison the controller information, which returns the propitiate execution of data plan attacks. For example, the Host Profile Service is leveraged using crafted Link Layer Discovery Protocol packets, an attack known as Host Location Hijacking attack [14].

2.3 Data Layer

The separation of the data layer and the control layer makes the forwarding devices remotely controllable and simple through open interfaces. An open flow switch is one of the most suitable and well-known examples of SDN forwarding devices. Furthermore, any Ethernet switches or routers with flow tables can be programmed using the open flow protocol. Whenever an open flow switch is being programmed, the router's flow table or switch is implemented to maintain the flow entries with a set of actions [13].

Moreover, an attacker may achieve targeted switch isolation through the controller's impersonation. Through the ARP poisoning attacks, an invader can hijack the controller's identity and insist on the descent of a link to the original controller, connecting to a forged controller [15]. An attacker tampers the information installed on switches, either flushing or overwriting the existing flow rules. By doing so, an attacker can also originate from this attack via a compromised network controller or application [14].

2.4 Northbound APIs

Northbound APIs enable communication among the application layer and the SDN controller. Therefore, a misconfiguration in northbound API may leverage to terminate a victim application or expose the information which is exchanged among the controllers [9–11]. Moreover, weak authentication at northbound APIs originates the spoofing attacks, which spoofs the communication at northbound.

2.5 Southbound APIs

Southbound APIs are implemented to communicate between the data & control layer. The weak encryption of the traffic between controller and switches may cause spoofing and eavesdropping of southbound information. Moreover, lack of authentication between switches and controllers causes the man in the middle and spoofing attacks, due to which attacker analyses the traffic [16–19].

The above-layered discussion indicates that, in the advancement of new SDN based network applications, security has become a primary concern because, in SDN architecture, security features are not integrated yet. Previous research indicates that different security attacks have been identified against SDN through multiple network components [20–24]. Traffic between controller and switches may cause spoofing and eavesdropping of southbound information. Moreover, lack of authentication between switches and controllers causes the man in the middle and spoofing attacks, due to which attacker analyses the traffic [16–19].

The above-layered discussion indicates that, in the advancement of new SDN based network applications, security has become a main concern because, in SDN architecture, security features are not integrated yet. Previous research indicates that different security attacks have been identified against SDN through multiple network components [20–24].

3 Related Work

The world has progressed culture, given a growing mix of the web in the public field; everything is in access and can be reached by methods for the web. Our computerized culture is included organizations, remote associations, cell phones, IOTs, etc. Notwithstanding their expansive decision, still, IP frameworks are difficult to screen according to the case, exceptionally predefined rules, and sudden response to load, changes, and mix-up organization [145].

Programming characterized network (SDN) has taken off to the most elevated purpose of the framework's organization inspiration since its turn of events. The SDN design is depicted by the control plane's parcel from the information plane and application plane. An astutely unified sensible substance characterized as the control plane stir keeps up the framework's state and offers rules to the data plane [146]. The assortment of essential sending gadgets, otherwise called the information plane, controls the organization's information handling and sending capacities [147]. The application plane's framework applications form a disconnected perspective on an organization through the control plane by social event data. Application plane likewise advances data bundles as demonstrated by these control

bearings. While this primary move has gotten significant thought from both the scholarly world and framework industry, disengaging control and data plane convenience has been around for any more extended [148]. With the reasonably thought control plane, the regulator has the overall diagram of the entire framework. The stream table sections' adjustment is altered relying upon the pre-characterized rules and arrangements coordinated by network administrations. This centralization can bring about gainful assistance for screen measurements and keep up strong security and procedure execution to the entire framework. The concentrated regulator enabled applications to hope to upgrade coordinate exercises, for instance, security, guiding, and framework organization.

The requirement of the network protocol of the SDN environment to interact and communicate to forwarding devices in the data plane is fulfilled by Open-Flow [149]. Open-Flow Controller considers a strategic point to use the Open-Flow protocol to connect and configure the network devices and determine the best application traffic path. An Open-Flow switch has a flow table that takes care of rules. Dependent upon the rules introduced by a controller application, an Open-Flow switch can train by the controller to carry on like a switch, switch, firewall, or perform different jobs. The Open-Flow comprises flow tables and activities related to each packet route that advise the switch how to process these streams and the Channels [150].

Security is still considered to be in its initial period; even there is an extraordinary progression in SDN architecture. SDN depends on a plan to give adaptable, programmable conditions, and design; the controller is an especially appealing focus for malicious actions without strong security execution. Due to security issues fronting by SDN, giving great convenience to attackers to practice different malevolent activities. These security threats are either acquired from the conventional network or started from its underlying architecture. IDS is the most discussed and in topic from last recent years for providing security to SDN. IDS is a framework intentionally intended to identify and alarm unapproved or undesirable access activities, changes, or limits PC framework assets. The framework regularly identifies malicious activity against the system.

A secure communication network consists of integrity, confidentiality, data & authentication availability, and non-repudiation [25]. Therefore, to design a protected network from unintentional damages, the security experts must protect the network assets such as devices, data, and communication transactions over the network. In this field, the most common work is to show many protective things at the edge of doing it precisely. Simultaneously, the modifications into the architecture of the network established by SDN must evaluate to make sure that it's being secured. At the early SDN improvement, the network control and forwarding functions' security aspects were considered [26]. SDN disassociates the forwarding functions and network control. Control logic does not depend on forwarding devices like switches, routers, and a centralized logical controller [24]. The literature of this review for SDN security issues and challenges are organized into multiple security threats and numerous security solutions.

SDN shifts the conventional networking control from hardware towards software, which simplifies administration and network operations. The network designer's work has changed from low-level coding on a device to designing the software, which can endow with debugging facility and network management. On the other side, SDN has increased the network's additional security issues due to decoupled design. The centralized control feature and programming ability of SDN have developed new areas of attacks and faults. Multiple threat vectors have been discussed in [27] and proposed a platform to minimize these network threats.

There are multiple controllers in distributed SDN, which access the data plan concurrently. Similarly, an application can access the provided pool of controllers, which are from different networks. If an attacker impersonates the applications or controller, then network resources will be easily accessed and manipulated [28–32]. In this way, the attacker degrades the performance of the network and misconfigure controllers. A system ensures that distributed controller security has been proposed in [33], ensuring central control elements' security through transport layer security. The designed system in [33] consists of a signature checking scheme and a centralized trusted manager. Moreover, threats from unauthorized access can also be mitigated through a hierarchical system of controllers [30]. Also, in [31] author proposed architecture, namely fleet. The proposed architecture tries to resolve unauthorized access issues through digital signatures among network administrators. The fleet describes the switch intelligence layer that holds an instance of all switches on which the administrators decide to implement the related rules. Moreover, Hussein et al. [34] presented a comprehensive review related to SDN security issues by identifying multiple security attacks and vulnerabilities. Also, different security solutions are highlighted, which have been proposed against several security attacks.

Various studies have been done to review the security and privacy issues in SDN as shown in Table 2, and the contribution of each existing study is evaluated and shown. This study reviews main security threats, presented solution against each security threat on different planes of SDN and change over time in research approaches related to SDN security and privacy issues. Likewise, most of the existing studies contributed to research by reviewing the same areas. However, a few existing survey papers review the deployment cost and software-hardware requirements of proposed methods as

Table 2 Contribution of existing review articles and presented study

Year [ref.]	SLR	Evaluation of main security threats in SDN?	Evaluation of security solution on SDN planes?	Change in s issues with time	Deployment cost of proposed method	Software-hardware requirements of proposed method	Quality assessment of proposed techniques
2015 [25]	No	Yes	Yes	No	Yes	Yes	No
2016 [26]	No	Yes	Yes	Yes	No	No	Yes
2016 [27]	No	Yes	Yes	Yes	No	No	Yes
2018 [28]	Yes	Yes	Yes	Yes	Yes	No	No
2019 [30]	No	Yes	Yes	Yes	No	No	No
2019 [31]	No	Yes	Yes	Yes	No	No	No
2020 [32]	No	Yes	Yes	Yes	No	No	No
2020 [33]	No	Yes	Yes	Yes	No	No	No
2021 [34]	No	Yes	Yes	Yes	No	No	No
2021[35]	No	Yes	Yes	No	Yes	No	No
2021[36]	No	Yes	Yes	Yes	No	No	Yes
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes

shown in Table 1. To the best of our knowledge, till date this is first systematic literature review which assess the quality of proposed methods.

4 Research Method

According to Petersen et al. [34], the primary objective of an SLR is mostly to present an extensive overview of any research area to identify the quantity and nature of the research. Mostly, the researcher tries to map the number of papers published over time to see trends. We have identified the frequency of approaches regarding privacy and security issues in the SDN environment. Figure 4 shows the search mapping processes that cover the relevant publications, mapping the publications, and defining the categorization scheme. Moreover, these SLR results will help recognize and map the research related to SDN security solutions, security platforms, and possible research gaps. The methodology process for this research has been given in Figure. In addition to this, exclusion and inclusion criteria are also implemented for the screening of papers.

We have decided to include the following type of papers only.

i. Including the study that has emerging and new ideas.
ii. Articles published only in journals, conferences, a workshops, and symposiums.
iii. Articles with precise data collection methods and have a good data source.

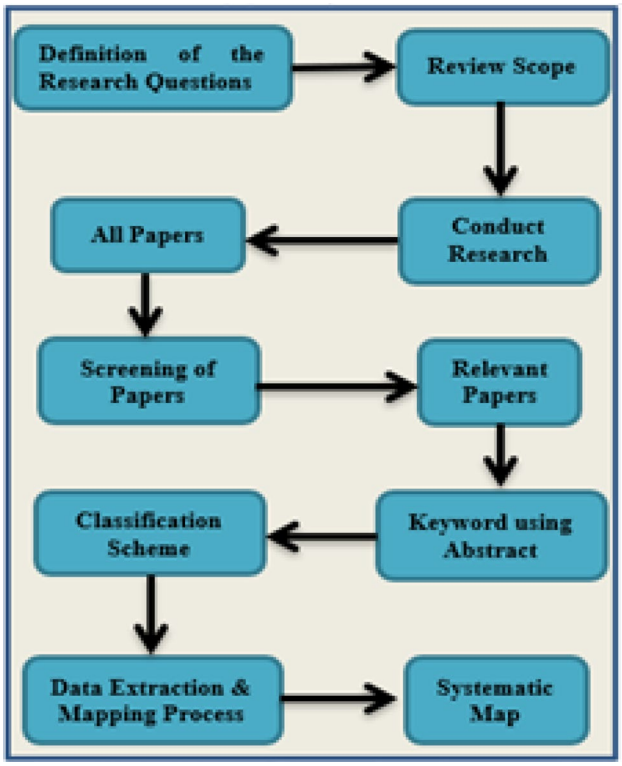


Fig. 4 Review Process

iv. Articles published only in the English language.
v. Selected the papers only relevant to the search string

4.1 Quality Assessment (QA)

We have defined quality assessment criteria by defining a questionnaire to assess the quality of each selected paper. Two authors who searched performed the quality assessment criterion. We have taken inspiration from [35] to define the questionnaire for a quality assessment.

i. Is a study highpoint the necessary clear privacy and security issues that happen mostly in SDN? The possible answers were Yes = 1 and given No = 0.
ii. Is the study representing the solution regarding security and privacy in SDN? The probable answers were Yes = 1 and No = 0.
iii. Are the study contributions inline in the presented results? The likely answers were Yes = 1 and No = 0.
iv. Have other articles cited the published paper? The probable answers were partially = 0.5 "if 1–5 authors cite a paper" and yes = 1 "when the paper is cited and used by more than 5 number of authors" and No = 0 "when not cited by any other author"

4.2 Search String

The second phase of SLR is to search for relevant papers on the research topic. We have specified a search string to collect the published articles regarding privacy and security issues in SDN. Furthermore, we performed pilot research on defined keywords and used keyword security issues in SDN. Additionally, in the pilot search, we also used SDN layers, threats, security solutions in SDN. Internet research is usually performed by using different search engines and digital libraries to obtain relevant information. After getting research results, they manually assembled them to obtain high-quality online information resources to answer the Research Questions (RQs). We select the digital libraries and search engines based on scientific content and most relevant to this SLR's objective. Selected databases and sources were IEEE, MDPI, Elsevier, Springer, Google scholar, and Hindawi. Search string with identified keywords according to our defined Research questions are given in Table 3.

4.3 Screening of Relevant Papers

After applying the search string, it is investigated that all papers were not precisely relevant to RQs. Therefore, they were needed to be evaluated according to actual relevance. To obtain the real applicability, we implemented a search process specified by Dybå et al.[21]. for the relevant papers screening. In the first phase of screening, we have selected the papers according to their title and then eliminated the studies that were not relevant to the research area. Such as keyword security returns articles related to SDN security in the cloud, SDN security in IoT, etc., which have different meanings than general SDN security topics. Such papers were excluded because they were out of scope. Moreover, in the second screening phase, we have studied the abstract of each research paper that is chosen in the first phase of screening.

4.4 Keywording Using Abstract

We have used a process defined by Petersen et al. [22]. to find out the relevant studies based on keywords by using abstract. The keywording process has two phases. In phase

Table 3 Search string

Sources	Search string	Context
IEEE, Elsevier, MDPI, Springer, Google scholar, Hindawi	("Software Defined Networks" OR "SDN") AND ("SDN security" OR "SDN threats") OR ("SDN Security Solutions" OR "SDN Layers")	SDN

Table 4 Selection process for the selected articles

Phase	Process	Selection criteria	IEEE Xplore	Springer	Elsevier	MDPI	Hindawi	Google scholar	Total
1	Search	Keywords	2313	117	585	150	503	501	4169
2	Screening	Title	173	44	51	27	31	99	425
3	Screening	Duplication Removal	128	18	21	12	22	53	254
4	Screening	Abstract	84	14	19	7	7	11	142
5	Inspection	Full Article	37	6	7	3	3	13	69

one, we studied the abstract to discover the concept and those that reflected the contribution of studies. In phase two, an advanced level of understanding is created by depending upon these keywords. Thus, we have utilized the keywords to gather and map the SLR's categories.

4.5 Study Selection Procedure

The results of the search and selection procedure are presented in Table 4. Initially, when the research protocol was implemented on selected digital libraries, 4169 papers were selected. Papers were selected after a thorough screening process, and exclusion criteria were set based on the titles, keywords, abstract and full articles from the selected studies. One author searched and retrieved all the papers, and another author scrutinized the papers, which resulted in 425 papers. After this phase, we eliminate the duplicate titles and those titles, which were irrelevant to SLR. For example, numerous papers were related to cloud computing and IoT. Moreover, we also read the full abstract of selected 254 articles, and we obtained 142 papers after removing the abstract duplication that shows the technique for the same domain work. In the last, a total 69 papers were selected out of 4169.

4.6 Research Concerns

The overall objective of SLR is to gain insight into privacy and security issues in SDN. By decoupling the hardware from software, operators can present advanced, distinguished fresh services quickly allowed from closed and registered platforms restraints. We have identified the different security threats, solutions to the attacks, and deployment costs to mitigate those threats. To obtain a detailed view regarding this study, we have defined the research concerns in the table. The table represents the six research concerns with their corresponding motivation. These research concerns allow us to classify the current security and privacy issues in SDN.

We have identified the different security threats, solutions to the attacks, and deployment costs to mitigate those threats. To obtain a detailed view regarding this study, we have defined the research concerns in the table. The table represents the six research concerns with their corresponding motivation. These research concerns allow us to classify the current security and privacy issues in SDN research concerns with their corresponding motivation. These research concerns allow us to classify the current security and privacy issues in SDN.

5 Analysis

This section presents the findings of research concerns that are described in Table 5. After the screening procedure, research studies have been used to demonstrate each research concern's answer to make a fundamental contribution to SDN's confidentiality and security concerns.

5.1 Selection of Results

The analysis of state-of-the-art safety and privacy issues in the SDN is a vital task with the technology's growing request. To investigate the status of SDN security, various research concerns are defined in this research review. According to Research concerns, 69 primary studies have been collected in this section. After analysing selected studies, we addressed the answer to each Research concerns according to the extracted information. Overall classification and quality assessment results have been presented in Tables 6, 7, 8 and 9.

Table 5 Research concerns

No	Research questions	Main motivation
Q1	Which are the main targeted publication channels to identify security and privacy issues in SDN?	The objective is to identify the main publication channels where SDN based security and privacy issues have been addressed with different proposed solutions
Q2	How the research approaches related to SDN security and privacy issues have been changed over time?	Identify the security and privacy issues in SDN with time
Q3	Which research approaches researchers have used?	To identify the different research approaches which have been proposed to provide a solution
Q4	Which are the main security dangers and causes in SDN?	Identify major security threats with their causes
Q5	Which are the proposed security solutions on different SDN plans?	Different security techniques have been identified in SDN to address the security solutions
Q6	What is the implementation and deployment cost of different?	Identify the cost for a different proposed security solution with their types

Table 6 SDN security threats and causes

Classification						Quality assessment				
References	P.Channel	Year	Research approach	Threat types	Caused by	a	b	c	d	
[66]	Journal	2020	Solution	Cyber-Physical Systems	Vulnerable services	1	1	1	0.5	3.5
[67]	Workshop	2019	Solution	Dos, and enforce the suboptimal configuration of a network via crafted requests	A network threat occurs due to external entities	1	1	1	0	3
[68]	Conference	2019	Experiment	DoS threats	Flooding attacks that change the security policies	1	0	0	0	1
[14]	Conference	2017	Experiment	Spoofing, Poisoned view of a network	Network protocols and services malware and vulnerable	1	0	0	1	2
[42]	Journal	2017	Experiment	Man-in-the-middle	Datalink vulnerability, the southbound interface is compromised, and the control channel is un-ciphered	1	1	1	0.5	3.5
[69]	Conference	2020	System	Controller hijacking	Infer sensitive information by analyzing network traffic	1	1	0	0	2
[49]	Journal	2018	Survey	Hijacking DoS	Occurs due to malicious attacks, inner and outside attacks, active and passive attacks	1	1	1	1	4
[44]	Journal	2018	Framework	Dos and Poisoning attacks	Threats take place based on the parting of control and data plane	1	1	1	1	4
[70]	Conference	2019	Solution	Cybersecurity issues during SDN and NFVs deployment	DoS, spoofing, and malware are the main causes of SDN threats in this study	1	1	1	0	3
[11]	Journal	2017	System	Flooding of Flow table	Vulnerable switches	1	1	1	1	4
[71]	Conference	2015	Solution	DDoS attacks	Generation of unauthorized traffic while connecting heterogeneous devices to exchange information for IoT services	1	0	0	1	2
[45]	Journal	2018	Model	DDoS attacks	Make the resources unavailable to the legitimate user through an overloading system	1	1	1	1	4
[15]	Journal	2015	Solution	Controller hijacking	Northbound API is influenced by malicious applications	1	1	1	0	3
[46]	Conference	2016	System	Freeloading	IP/MAC address spoofing of an	1	1	0	1	3
[37]	Journal	2017	Architecture	IP Spoofing	Attackers attack by using forged IP sources address	1	1	1	1	4
[36]	Journal	2019	Solution	ARP Spoofing	Attacker use target IP address and distinguish as a target host	1	1	1	1	4
[72]	Conference	2016	Solution	Spoofing	Saturate the DNS resources and service availability	1	1	0	1	3
[73]	Conference	2018	Solution	Tampering	Occurs due to two new threats port probing and port amnesia	1	1	1	1	4

Table 7 SDN Security techniques and solution on different plane

References	Year	P.Channel	Research Approach	Technique	Solution	Target Plane	a	b	c	d	Score
[84]	2019	Journal	Survey	Machine Learning and Deep learning approach	Surveyed the SDN based network intrusion detection system	Data, Control, App Plane	1	1	1	1	4
[38]	2019	Journal	Architecture	DPX	Improved the poor performance and complex configuration	Data Plane	1	1	1	0.5	3.5
[85]	2019	Journal	Model	Intelligent Electronic Devices (IEDs)	Proposed a security model which incorporate the role of all IEDs on smart grid networks	Control Plane	1	1	1	1	4
[86]	2020	Journal	Survey	Open state, FAST, SDPA	Formulize the security issues on data plane	Data Plane	1	1	1	1	4
[87]	2014	Symposium	Framework	Payless	Network overhead is not balanced	App Plane	1	0	0	1	2
[88]	2019	Journal	Architecture	Cryptographic authentication	SDN based security architecture proposed for 5G networks	Data Plane	1	1	1	1	4
[89]	2016	Journal	Solution	The stateless firewall application	ACI implementation on an openflow enabled switch	App Plane	1	1	1	1	4
[90]	2014	Workshop	Framework	Flow Guard	Security Policies verification	App Plane	1	1	0	1	3
[91]	2016	Journal	Solution	PERM-GUARD	An authentication scheme for flow-rule production permission	App Plane	1	1	1	1	4
[92]	2020	Journal	Architecture	Manufacturer Usage Description (MUD)	Enhance the IOT devices connectivity and secure from attacker	Data Plane	1	1	1	0.5	3.5
[43]	2016	Journal	Experiment	SD-Anti-DDoS	Action on DDoS attacks	App Plane	1	1	1	1	4
[39]	2019	Journal	Architecture	Network Function Virtualization (NFV)	Proposed an architecture to capture major security and privacy issues	Control Plane	1	1	1	1	4
[47]	2019	Conference	Algorithm	TLS and defensive algorithm	Secure SDN open flow communication	Data Plane	1	1	0	0	2
[93]	2016	Journal	Solution	Double hopping comm. (DHC)	Solution for the problem of the sniffing attack	App Plane	1	1	1	1	4
[94]	2016	Journal	System	Bro Flow	A Prevention and Intrusion Detection System based on Bro traffic analyzer	App Plane	1	1	1	1	4
[95]	2015	Journal	Architecture	CIPA	Solution for Intrusion detection	App Plane	1	1	1	1	4
[96]	2015	Conference	Framework	OFX	Switches stability among off switches deployment and performance	App Plane	1	1	0	1	3
[97]	2015	Journal	Solution	SPHINX	Attacks detection and prevention module	Control Plane	1	1	1	1	4
[98]	2015	Journal	Architecture	Flow	Security policy verification	Control Plane	1	1	1	1	4
[99]	2015	Journal	Experiment	OPERETTA	Host legacy verification	Control Plane	1	1	1	1	4
[100]	2015	Conference	Experiment	Mynah controller	DPID problem mitigation	Control Plane	1	1	0	1	3
[101]	2016	Journal	Solution	DDoS Detection	Features extraction through self-optimized map	Control Plane	1	1	1	1	4

Table 7 (continued)

References	Year	PChannel	Research Approach	Technique	Solution	Target Plane	a	b	c	d	Score
[102]	2018	Journal	Architecture	Multiple Security techniques implemented as building blocks	Integration of SDN security system		1	1	1	0	3
[103]	2017	Conference	Framework	A multilayer SDN forensics framework	Proposal for SDN forensics framework		1	1	1	1	4
[104]	2017	Journal	Framework	Fuzzy techniques	Vulnerabilities detection		1	1	1	1	4
[50]	2017	Conference	Application	Network applications access policy constrained	A mechanism for access protection		1	1	0	1	3
[105]	2018	Journal	Architecture	For the channel encryption applied Cry tokeys distribution	Authentication and trust mechanism		1	1	1	1	4
[106]	2017	Symposium	Solution	Switch authentication based on the fingerprint	Verification and authentication mechanism		1	1	0	1	3
[107]	2017	Workshop	Solution	The security requirements translation into NFVs	NFVs security		1	1	1	1	4
[108]	2018	Journal	Architecture	Third party security of a multivendor	Regular interface for the given cloud NFVs		1	1	1	1	4
[109]	2017	Journal	Solution	Translation of security policy	Virtualized security into a virtual system service chain		1	1	1	1	4

5.1.1 Assessment of Q1: Which are the Main Targeted Publication Channels to Identify Security and Privacy Issues in SDN?

Figure 5 shows the channel and publication type of selected studies where the research papers have been published. The types of publications in this systematic literature review are journals, conferences, workshops, and symposiums. Majority of the papers that have been published in journals, i.e., 41 in number, which is 60%, and conference papers, i.e., 21 in number, which is 31% of the total research papers chosen for the research review. The remaining papers have been published in workshops (5) (7%) and symposiums (2) (2%). Therefore, it can be said that the number of papers is published in journals is higher than any other publication channel.

5.1.1.1 Information Disclosures Information disclosures are those attacks that have indirect intentions to disrupt or destroy the network. However, work as a detective on its information. Furthermore, the sensitive data or information that attackers try to obtain initially try to sniff the network information like features, topologies, nodes, or communication detail between nodes. Man-in-the-Middle (MITM) is the type of Information disclosure attack that is not on-premises, and it targets the information in transit. In open flow architecture, MITM attacks are mostly seen to be significantly possible [62]. This sort of assault is pointed toward securing framework detailed data about a site, including software dispersion, rendition numbers, and patch levels. The procured data may likewise contain the area of reinforcement documents or temporary records.

5.1.1.2 DoS DoS attacks are more severe because they increase latency, affect the network performance, and leave the legitimate packets. DoS attacks may halt the entire network or put it out from functioning. DoS may be more devastating for Open Flow networks because a constant flow amongst switches and controller exist.

The continuous communication among switches and controllers can persuade the attacker to push flow between the controller and switches that disturb the network's everyday activities. DNS amplification and flooding are those attacks measured as a flow level resolution because information at the flow level is sufficient to detect such threats [56].

Moreover, flow level information plays a vital role in detecting DoS level attacks. Flow level attack detection system, which depends only on the header's information, can detect the four threats, namely: DoS, botnets, worms, and scans. These attacks have some unique signatures. They have much unstable traffic, where most of the traffic is flowing in one direction. Loops can also cause the DoS or may be

Table 8 Analysis of proposed solutions in terms of Software-hardware requirements, cost, network changes and scalability

Security type [Ref]	Cost					Scalability
	Additional software requirements	Additional hardware requirements	Modification in network			
			Data path elements	Host/End User devices	Open flow protocol	
Controller Availability [102]	Yes	No	No	No	No	Yes
Controller Availability [103]	Yes	No	No	No	No	Yes
Configuration Verification [104]	Yes	No	No	No	No	Yes
Flow Rule Verification [105]	Yes	No	No	No	No	Yes
Network Monitoring [106]	Yes	No	Yes	No	No	Yes
Network Monitoring [107]	Yes	No	No	No	No	Yes
Network Monitoring [108]	Yes	No	No	No	No	Yes
Network Monitoring [109]	No	Yes	Yes	No	No	No
Security Monitoring [110]	Yes	No	No	No	No	Yes
Network Resilience [111]	Yes	No	No	Yes	Yes	No
Network Resilience [112]	Yes	No	Yes	Yes	No	No
Firewall [113]	Yes	No	No	No	No	Yes
Firewall [114]	Yes	No	No	No	No	Yes
Firewall [115]	Yes	No	Yes	No	No	Yes
Firewall [116]	Yes	No	No	No	Yes	Yes
Flow based IDS [117]	No	Yes	Yes	No	Yes	No
IPS [118]	Yes	Yes	No	No	No	Yes
Per Flow Sampling [119]	No	No	Yes	No	Yes	Yes
Flow Sampling [120]	No	No	Yes	No	Yes	Yes
Securing SDN-Controlled IoT Networks [121]	Yes	Yes	No	No	Yes	Yes
Enhanced IoT Security [122]	No	No	Yes	No	Yes	Yes
Cyber Threats [123]	No	No	Yes	No	Yes	Yes
Real-time security system [124]	Yes	Yes	No	No	No	No
DHCP guard [125]	No	No	Yes	No	Yes	Yes
Reinforcement Learning [126]	Yes	Yes	No	No	Yes	No
Machine Learning [127]	Yes	No	Yes	No	Yes	No
SDN-enabled switches [128]	Yes	Yes	No	No	Yes	No

utilized for networking attacks. In such loops, the packet moves from one switch to another switch without getting its final destination. Loops have been handled in open flow networks by [63]. In SDN, the attacker/hacker conducts the DoS attacks by pushing a large volume of traffic, which randomly keeps changing the attributes of the flow [64, 65]. A denial-of-service (DoS) attack happens when genuine clients can't get to data frameworks, gadgets, or other network assets because of malicious cyber-attack activities. DoS attacks can cost an association both time and cash, while their assets and services are blocked off.

5.1.2 Assessment of Q2: How the Research Approaches Related to SDN Security and Privacy Issues Have Been Changed Over Time?

We have selected the articles between 2014 and 2020, as shown in Figure 6. The graph shows how the frequency of these approaches has been changed with time. The maximum number of papers have been published between the years 2015 and 2019. Beyond architecture itself, SDN security is also highly deployed, managed, and measured along with controlling in the SDN environment. This feature is available to take as it can enable and confirm the security of the

Table 9 SDNs security solutions deployment cost

Classification													Quality assessment				
References	P.Channel	Year	Research approach	Security/Issue TYPES	Security/'Cost solution	Implementation framework	Entirely new system			Modification			a	b	c	d	Score
							App	Ctr	Dev	Data	OF	Host					
[112]	Conference	2014	Application	Firewall	OF TABLES	Flow Rule Filter	✓	✗	✗	✗	✗	✗	1	1	0	1	3
[113]	Journal	2014	Framework	Network Resilience	Management Framework	Management Pattern	✓	✗	✗	✓	✓	✗	1	1	1	1	4
[51]	Conference	2014	Application	Firewall	Soft Firewall	Flow Rule Filter	✓	✗	✗	✗	✗	✗	1	1	1	1	4
[56]	Journal	2014	Architecture	Security Monitoring	OrchSec	Security Orchestrator	✓	✓	✗	✗	✗	✗	1	1	1	1	4
[42]	Journal	2014	Platform	Network Monitoring	Payless	Monitoring framework	✓	✗	✗	✗	✗	✗	1	1	0	1	3
[114]	Workshop	2016	Model	Network Security	Techno-Economic Model	Cost model	✗	✗	✓	✓	✓	✓	1	1	0	1	3
[115]	Journal	2019	Model	Network Security	Multi-objective optimization model	Heuristic algorithm	✓	✓	✓	✓	✗	✗	1	0	1	0.5	2.5
[116]	Conference	2015	Architecture	Heavy load management system issue	Load balancing, security management	Architecture to improve controller framework interruption	✗	✓	✓	✓	✓	✗	1	1	1	1	4
[48]	Conference	2017	Algorithm	Attack detection	Cost Optimized Flow Statistic Collection scheme	Wild Card Request	✓	✗	✗	✓	✓	✗	1	1	0	1	3
[117]	Workshop	2015	Solution	Control connection security issue	TLS support	Performance measurement tool	✗	✓	✓	✗	✓	✗	1	1	0	1	3
[118]	Journal	2017	Model	Network scalability	Cost optimal design for security	Pareto optimal multi-objective	✓	✓	✓	✗	✗	✗	1	1	1	1	4
[119]	Conference	2017	Experiment	Security for network services and technologies	Cost-effective model for security and decision making analysis	Measure the unit cost based on (Capital Expenditures and operation cost	✗	✗	✓	✗	✓	✗	1	1	1	1	4
[120]	Conference	2015	Architecture	A smart grid security issue	Secure architecture	Novel architecture to improve the smart grid security	✓	✗	✓	✗	✗	✓	1	1	1	1	4
[41]	Conference	2019	Experiment	Security measurement overhead	CFlam approach	Implemented CFlam on SDN testbed	✗	✓	✗	✗	✓	✗	1	1	1	0	3
[40]	Journal	2018	Experiment	Resolve the slower convergence and interrupt	Auto regressive stochastic procedure	Proposed two control policies to reduce the routing cost	✗	✓	✓	✗	✗	✓	1	1	1	1	4
[121]	Conference	2015	Solution	Flow detection iss	Detect the flow for different application	A cost-sensitive method has been introduced for flow detection	✓	✓	✗	✗	✓	✗	1	1	0	1	3
[122]	Journal	2018	Solution	Static and comple issues	A scalable and innovative security approach	Developed a low-cost switch	✗	✗	✓	✗	✓	✗	1	1	1	1	4
[123]	Journal	2019	Algorithm	Average transmiss and flow cost issu	Heuristic policy	Developed a propagate algorithm	✓	✗	✗	✗	✗	✓	1	1	1	1	4

Table 9 (continued)

Classification													Quality assessment				
References	PChannel	Year	Research approach	Security/Issue TYPES	Security/'Cost solution	Implementation frame-work	Entirely new system			Modification			a	b	c	d	Score
							App	Ctr	Dev	Data	OF	Host					
[124]	Journal	2020	Model	Queuing system	Optimization model	Implemented a queuing system to measure the performance of packet forwarding	✗	✓	✓	✓	✓	✗	1	1	1	0	3
[125]	Journal	2018	Algorithm	Time-critical requ	Designed a cost-effect industrial IoT system	Optimize the location and type of controllers	✓	✓	✓	✗	✗	✗	1	1	1	1	4

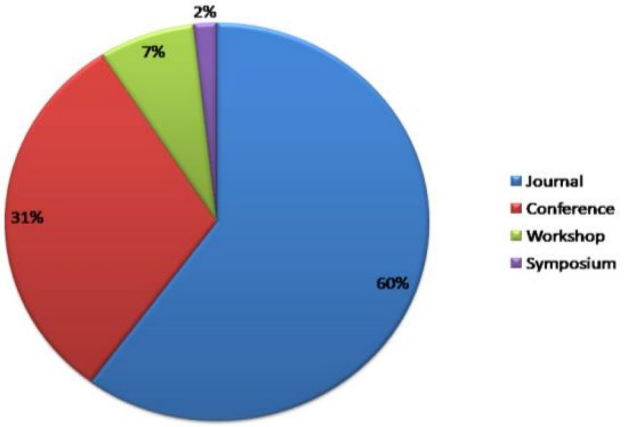


Fig. 5 Publication Channels

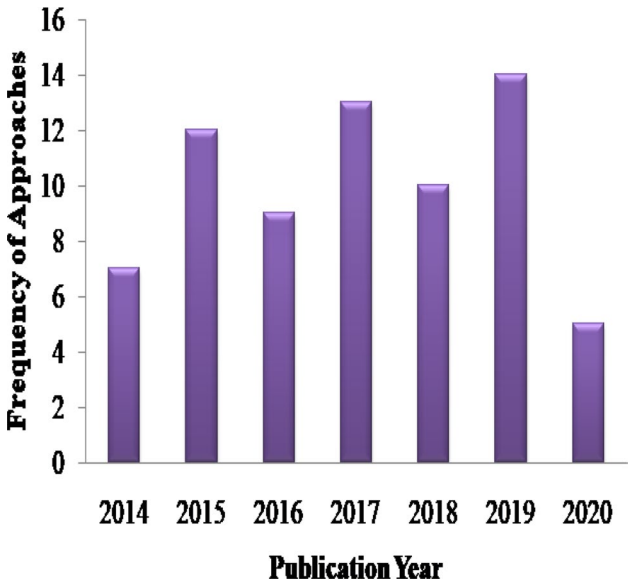


Fig. 6 Years of Publication

network. There are so many competing approaches in which some trusted security is best embedded in the network.

In contrast, others feel it is best embedded in the servers, systems, storage, and computing devices. However, a few papers are published in 2020 because the search's initial process was performed in May 2020. It indicates the publications in each year are increasing, which shows the developing interest in security and privacy issues in SDN.

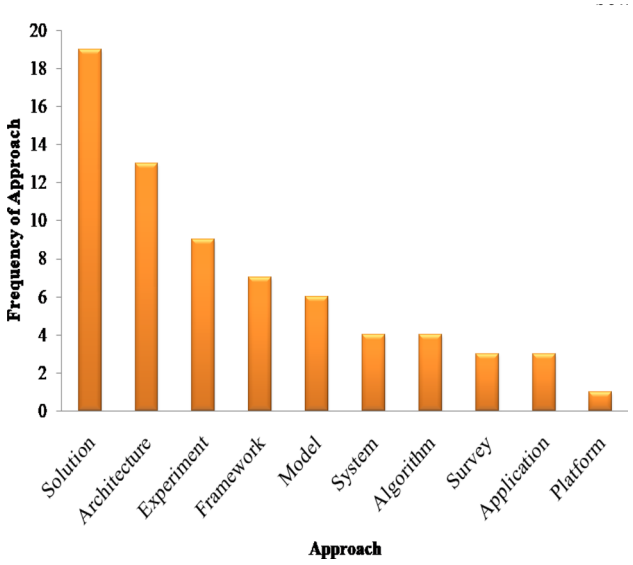


Fig. 7 Research Approaches

5.1.3 Assessment of Q3: Which Researchers Have Used Research Approaches?

Different research approaches have been shown in Fig. 7, which are implemented to investigate SDN's security and privacy issues. Every method is described in this section.

Proposed Solutions: Multiple solutions have been proposed to measure the phenomenon of security and privacy issues in SDN in the actual context. A solution has been provided, which automatically detects the poisoning attacks in real-time SDN controllers [15]. Implementation of the solution indicates that it will secure the network topology effectively. Moreover, for ARP spoofing, a defence solution can also be proposed to reduce the security threats on different SDN platforms and open-flow platforms [36].

Architecture: Different architectures have been designed to investigate the security concerns in SDN, for example, threat detection, attack mitigation, etc. [37–39].

Experiment: To measure the privacy and security challenges in SDN, researchers performed different experiments. Two policies have been proposed to calculate the cost of the average routing time [40]. These policies are based on the tools of standard linear programming. The proposed policies have been experimented on in real-time over GEANT networks [40]. There are also many other experiments performed to propose solutions and measure security threats and cost [41–43]. ***Framework:*** A conceptual illustration that is anticipated for building something to explore the guideline for SDN security. In [44], a FlowKeeper framework has been proposed to robust the data plane against malicious attacks.

Model: Model represents a developed system that explores the design properties of security issues in SDN. In [45], a JESS model was proposed to devise security solutions to mitigate DDoS attacks.

System and Algorithm: The series of steps that are executed to acquire knowledge regarding SDN security issues [11, 46–48].

Survey: A qualitative method to collect the information relevant to SDN security challenges. A comprehensive survey has been presented on SDN based VNETs security threats and services [49].

Application: Many applications have been established, which provides the best control over other SDN security and privacy issues [50, 51].

5.1.4 Assessment of Q4: Which are the Main Security Threats in SDN?

For RQ, we have conversed different types of security threats that SDN can expose. SDN attacks can be classified according to the type of resource or asset a typical SDN has. The attack may be deliberated on the controller as a central location for control and management. An attack can also occur on switches such as flow tables, where these tables contain information regarding routing, switching, access control, and network management. Moreover, channels among switches and controllers are another severe attack with those channels that have important messages. The identified SDN threats are described in the following subsections.

5.1.4.1 Information Disclosures Information disclosures are those attacks that have indirect intentions to disrupt or destroy the network.

Furthermore, the sensitive data or information that attackers try to obtain initially try to sniff the network information like features, topologies, nodes, or communication detail between nodes. Man-in-the-Middle (MITM) is the type of Information disclosure attack that is not on-premises, and it targets the information in transit. In open flow architecture, MITM attacks are mostly seen to be significantly possible [62]. This sort of assault is pointed toward securing framework detailed data about a site, including software dispersion, rendition numbers, and patch levels. The procured data may likewise contain the area of reinforcement documents or temporary records.

5.1.4.2 DoS Attacks based on DoS are more severe because they increase latency, affect the network performance, and leave the legitimate packets. DoS attacks may halt the entire network or put it out from functioning. DoS may be more devastating for Open Flow networks because a constant flow amongst switches and controller exists. The continuous communication among switches and controllers can persuade the attacker to push flow between the controller and switches that disturb the everyday activities of the network.

DNS amplification and flooding are those attacks which have been measured as a flow level resolution because information at flow level is sufficient for detecting such kind of threats [56]. Moreover, flow level information plays a vital role in detecting DoS level attacks. Flow level attack detection system, which depends only on the information of the header, can detect the four threats, namely: DoS, botnets, worms, and *scans. These attacks have some unique signatures. They have* a large number of unstable traffic, where most of the traffic is flowing in one direction. Loops can also cause the DoS or may be utilized for networking attacks. In such kind of loops, the packet moves from one switch to another switch without getting its final destination. Loops have been handled in open flow networks by [63]. In SDN, the attacker/hacker conducts the DoS attacks by pushing a large volume of traffic, which randomly keeps changing the attributes of the flow [64, 65]. A denial-of-service (DoS) attack happens when genuine clients can't get to data frameworks, gadgets, or other network assets because of the activities of a malicious cyber-attack. DoS attacks can cost an association both time and cash, while their assets and services are blocked off.

5.1.4.3 Spoofing Spoofing is the demonstration of masking a correspondence from an obscure source as being from a known, confided in source. Furthermore, spoofing that prompts the rerouting of web traffic can overpower organizations or lead clients/customers to malicious locales pointed toward taking data or distributing malware.

Spoofing is a process in which network information such as ARP, IP, MAC etc., is forged with an intent to keep the original identity of the hacker or traffic originator confidential [52]. Furthermore, spoofing is a significant attack component, such as amplification of DNS, SYN flooding, and Smurf [53]. The spoofed addresses may be part of a zombie network that initiates the DDoS attacks [54]. A module, namely AddressResolution Mapping (ARP), has been proposed, tracking the MAC address from an authorized host or user [55]. The controller consults with this module to discard those ARP responses, which are unproved by the ARP module. ARP spoofing threats can also contradict the information of packet level. Threats detection methods are divided according to the low and high-resolution methods based on information given to it as input [56]. The threats that occur at low-resolution demand packet-level detail, not flow level. Whereas the threats which occur at high-resolution demands packet-level information. Furthermore, IP spoofing is an attack in which an attacker impersonates an authentic host to hide its identity for hijacking the host file or IP address. A flow design is built on the anti-spoofing technique has been anticipated to enhance network security [57]. The developed mechanism has been tested by using the SDN approach dynamically.

5.1.4.4 Tampering Tampering is the demonstration of intentionally adjusting (wrecking, controlling, or altering) information through unapproved channels. The interruption is malignant, and the impacts on the information consistently desperate. It's one of the most significant security dangers that any application, program, or association can confront. Tempering is unauthorized and deliberate destruction or modification in the network information, like access lists, policies, topology, and flow tables. For example, an assailant may inject flow rules that cause the network disturbance. They inject the firewall rules or flow table, which permit the illegitimate host or contradict the legitimate host. Hacker may try to temper the topology information and cause to hijack some info. In such a case, it is the main objective to secure the communication channel from being tempered or hijacked [58].

Moreover, the security problems related to dynamic flow tunnelling conflicts are described [59]. These problems take place because the rules are estimated one after another. In the developed solution, they have tried to plaid out the conflicts among the firewall and flows. Furthermore, tempering can also be controlled by distributing monitoring and auditing over the multiple network points [60]. If the attack occurs at one point, then the remaining point will be utilized to detect and correct such kind of tampering.

5.1.4.5 Repudiation A repudiation happens when an application doesn't receive controls to track and log clients' activities appropriately, allowing noxious control or manufacturing the ID of new activities. This attack can change the writing data of activities executed by a noxious client to log the wrong information to log documents. Its utilization can be reached out to general information control for others' sake, likewise as ridiculing mail messages. On the off chance that this assault happens, the information put away on log records can be viewed as invalid or deluding.

Repudiation performs malicious actions without leaving any trace. Repudiation is the denial by one entity that involves taking part in all or an element of communication. None-repudiation should target property measured as a legal try to ensure such kind of denials does not occur. The receiver should authenticate the packets delivered from the actual sender and integrated them into the packet's header. In contrast, the sender should also receive the packet, which is, transmitted towards the receiver that is integrated into the packet's header. None-repudiation is related to the accountability regarding entities accountable or holding individuals or liable for their action [61].

5.1.5 Assessment of Q5: Which are the Proposed Security Solutions on Different SDN Planes?

SDN architecture maintains highly reactive systems, including monitoring, analysing, and responding to the whole system to assist the security services insertion, security policy, and network forensics [74]. In-network forensics, the SDN supports an adaptive and quick identification via harvesting intellect cycles from a network to update and analyse the policy to reprogram the network. Different security platforms are addressed in this section, proposal, and security measures to secure the applications planes, control planes, and data planes. The identified security solutions have been presented in Table 6 to boost up the security for each plan. The addressed solutions regarding SDN planes in Table 6 indicate the effectiveness and impact of security on a specific plan.

5.1.5.1 Security Solutions for Application Plane To hide the network complexity from different application controller works as an intermediate among applications and network hardware in SDN. Consequently, SDN-based control architecture implements new applications easy to retrieve the packet characteristics and network statistics via the controller to deploy the new security techniques. That's why multiple networking programming languages like NetCore, Frentic [75], and Procera [76] are developed, simplifying the development of application in SDN. A scripting language called FRESCO is used to develop the new security services, which might be deployed on switch implementation or any open flow controller. Applications should have a controlled entree to the network's resources and needs to perform in its defined functional limitations.

PermOF is the fine-grained permission method utilized to provide access to the open flow controller [77]. To enforce permission control design has been specified because of isolation and permission mechanism. Furthermore, in SDN, environment applications should have a reliable interpretation of the network and be responsive to network changing conditions. In [78], a method has been proposed to debug and verify the SDN application to stay reliable and responsive. Assertion language helps in checking and investigating SDN applications with progressively changing check conditions. The language permits software to define a network to comment on regulator applications with C-style affirmations about the data plane. Assertions comprise of standard articulations on ways to depict path properties for classes of packets and existential quantifiers that range over programmer sets of hosts, switches, or others. As controller programs progressively add and eliminate these sets' components, they produce new check conditions that the current data plane should fulfill.

5.1.5.2 Security Solutions for Control Plane The security solutions for the control plane have been classified into various approaches and proposals for the protection of the control plane from DDoS or Dos attacks, faulty or malicious applications, and ensure the availability as well as security through a consistent controller placement. Furthermore, the control plane should ensure the access of legitimate applications concerning their functional requirement but within the security limitations.

Security enhanced floodlight (SEF) is an extension of the original floodlight controller, which is an ideal attempt to secure the SDN control layer [79, 80]. SEF provides a mechanism by adding the secure northbound API into the controller to perform like a mediator among the data plane and applications. SEF has also introduced a run time open flow application to validate the integrity of the class, a module that generates flow rules. Moreover, SEF also allocates the authorization rules to open flow applications to solve the conflicts that arise by comparing the authorization rules.

5.1.5.3 Security Solutions for Data Plane The data plane's security is a must to dodge malicious submissions that can modify, install, or change the flow rule. Therefore, the fine-grained security mechanism (like authorization, authentication) is used for applications that may alter the flow rule. Fort NOX is a policy that allows the NOX open flow controller to ensure the flow rules contradict and authorize the open flow applications [29]. Fort NOX provides security limitations enforcement via software extension in NOX and role-based authentication through digital signatures. Another configuration tool called Flow checker is implemented to identify the inconsistency in open flow rules among single switch or multi-interlinked data path elements [81]. Flow checker is also used to enforce, analyse, and validate end-to-end open flow configuration at run time. Furthermore, a networking tool called Veri Flow is used to find out the defective rules added by the SDN controller and secure them from irregular network behaviour [82].

A controller replication has been proposed to retain the switch operation [83]. In this situation, the switch sends a probe message occasionally to a controller. If the controller does not respond in a specific period, then the switch presumes that the controller is down. SDN controller is controlled to forestall unauthorized action. Role-based access strategies that are evaluated and explored on a predictable premise should be utilized. Any unauthorized endeavours should start up cautions to the safety crew. Additionally, arrangement changes to it should be examined and investigated regularly. Best practices for hardening and fixing the system should be set up. When a best practice or security standard isn't followed, at that point, the risk and impact

effect of it must be reported, estimated, and affirmed by the authority.

Table 9 represents the various solutions and their technique and indicates that either a solution requires innovative and up-to-date security elements, or it can be modified based on current SDN elements. One can debate that SDN's security charges may be advanced if a security system demands security solutions on specific devices like security controllers. By taking advantage of the network's ability to program and centralizing control, it is mostly understood that adding a new security module to a data path element or an open flow controller might be less costly. On the contrary, the integration of security solutions in the controller will upsurge controller scalability and availability challenges. That is why security solutions cost depends on the architecture and size of the network.

In addition to this, the evaluation of performance penalty costs (such as latency, network overhead, and complexity of deployment) is necessary as compared to the cost of deploying and implementing the right security solution.

For example, consider the active and passive measurement methods for monitoring networks [110], where passive measurement techniques measure the network traffic through the observations when active measurement techniques inject an addition packet into the network to evaluate their conduct. Therefore, passive measurement requires synchronization among the observation beacons that make the monitoring process difficult. On the other side, active measurement induces the extra traffic load, which has an effect on the network and manipulates the accuracy of measurements themselves [111]. By doing so, the passive measurement enhances the delay, while the active measurement boosts up overhead through the addition of extra packets.

5.2 Quality Assessment

The score of quality assessment is presented in Table 7. According to the results, 91% of the papers have above an average score, whereas 2% of the papers have an average score, and only 1% of the papers are below-average scores. The defined quality assessment criteria will help the researchers and practitioners to find out the privacy and security challenges in SDN according to their requirements.

ARP Spoofing: By using ARP destroying attack, the attacker takeovers the identity of the given controller, and then it forces the marked switch to put down the link to the authentic controller and connects with a forged controller. In this, the network suffers the switch dis-connectivity issues [11, 15]. ARP spoofing is a sort of attack wherein a malevolent entertainer sends misrepresented ARP (Address Resolution Protocol) messages over a local network. This outcome in connecting an aggressor's MAC address with the IP address of an authentic PC or worker on the organization.

API Exploitation: Vulnerabilities and misconfiguration in APIs can lead to exposure of the information exchange or terminate the victim application used to perform vulnerability among targeted applications aimed to be targeted and controller [10, 11].

Furthermore, the security system use network processing memory, capacity and bandwidth resulting in penalty in performance in terms of latency and complexity. In Table 7. Proposed studies are evaluated in terms of associated cost with SDN security solutions. Normally cost of security solution can be divided into two categories i.e., firstly, cost of modification to the end user or host devices and OpenFlow protocols, and adding security modules in data path elements, and in OpenFlow controllers. Secondly, cost of deploying or developing new security system including the expenses of specific devices or security applications for security solution and security controllers. Table 9 shows that whether a solution require network changes and which kind of cost the proposed system required either it require a new security element or modification in existing system of SDN. It is obvious that adding security module in data path elements, and in OpenFlow controllers of SDN would be less expensive rather than adding an entire new security system. However, adding security module in existing SDN elements can give rise to the challenges of scalability and controller adaptation. So, the cost of security solution depends upon the tolerable penalty in system performance with security solution architecture and size.

6 Discussion

The discussion part is divided into two sections. Section 6.1 presents a detailed discussion on privacy and security issues in SDN. Moreover, to summarize the findings of this research, SDN architecture is presented in Fig. 3 with multiple security attacks on three layers (Application layer, Control layer, Data Layer). On the other hand, Sect. 6.2 consists of open issues on security in SDN.

6.1 SDN Security-Threats Architecture

The overall SDN architecture with consideration of technological advances and different security threats is shown in Fig. 8. All interfaces and layers are very sensitive to the specific attacks that may be compromising network components or target elements on another layer. The architecture has been divided into north, south, east, and west APIs as well as three layers with possible threats. We have identified

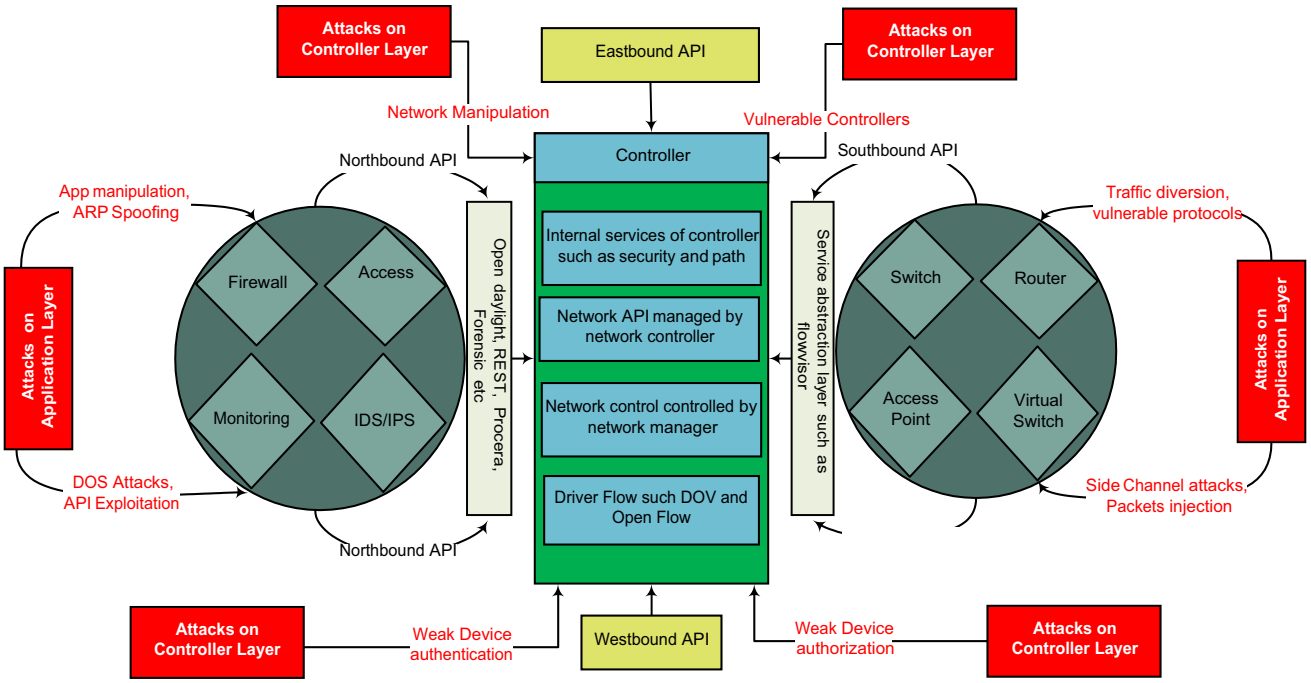


Fig. 8 SDN Architecture with threats and vulnerabilities

the set of most common attacks in each layer that are discussed below.

6.1.1 Attacks on the Application Layer

App Manipulation: Control applications and third parties with unrestricted authority in the network system may be compromised by abusing fixed authority and privileges [9–11]. As the application layer is the first layer in SDN architecture, it shows how the first layer can get affected immediately when any threat and vulnerability occur.

6.1.2 Attacks on Controller Layer

Network Manipulation: The most common threat in this scenario is the flushing of flow rule in switches and network policy removal, which grant unauthorized access to internal databases and administrative stations [126–128]. Network Manipulation is the endeavour to adjust the Web chart and an informal community, and in this way, impact the web network devices in manners advantageous to the controllers. The adjustment of an organization is regarding modifying its structure and additionally its substance. The online organization devices that controllers attempt to impact are normally web indexes and, on the web, online media.

Vulnerable Controllers: Malicious applications and vulnerable protocols may be used to poison the controller information that causes the execution of the attacks on the data plane. For example, the packet injection attack in link layer discovery protocol (LLDP) sends crafted packets of LLDP to a controller to poison the network topology. Furthermore, an attack called location hijacking also occurs in that defencelessness of the host's profiling service has leniency by the implementation of the prepared LLDP packets [14].

Weak device authorization and authentication: Attackers exploit the weak access control mechanism to award themselves an unverified entree to SDN elements. Furthermore, by launching the instinctive force attacks counter to the administrative stations and exploit the vulnerabilities or expose the logging sessions by installing the rouge devices [126, 127].

6.1.3 Attacks on the Data Layer

Packet Injection: A targeting switch may go to an uninvited condition exposed to a fuzzy attack situation.In this way, a control crafted packet is received, which misusing or malformed the headers, which are forged to expose the existing vulnerabilities [11]. Parcel injection (otherwise called forging packet or spoofing packet) in PC organizing is the way toward meddling with a setup organization association by methods for building bundles to show up as though they are essential for the typical correspondence stream.

Side-channel attacks: These attacks usually influence specific targeted devices' resulting response alongside the particular network conditions to infer. For example, an attacker may track the round-trip time that is experimented via a

Table 10 Quality assessment score

References	Score	Total
[11, 36, 37, 39, 40, 43–45, 49, 51, 56, 73, 84–86, 88, 89, 91, 93–95, 97–99, 101, 103–105, 107–109, 113, 116, 118–120, 122, 123, 125]	57%	4
[38, 42, 66, 92]	6%	3.5
[15, 41, 42, 46, 48, 50, 67, 70, 72, 90, 96, 100, 102, 106, 112, 114, 117, 121, 124]	28%	3
[115]	1%	2.5
[14, 47, 69, 71, 87]	7%	2
[68]	1%	1

particular packet; such kind of information can influence later to launch the flooding attack [11]. Attacks at this layer can emphasize the uncertainty of the protocols used or the lack of reinforcing on the routing devices. As the switches focus on giving the LAN connectivity, most attacks come from inside the organization itself. A side-channel attack breaks cryptography by utilizing data spilled by cryptography, for example, observing the electromagnetic field (EMF) radiation discharged by a PC screen to see data before it's scrambled in a van Eck phreaking assault, otherwise known as Transient Electromagnetic Pulse Emanation Standard (TEMPEST).

The summary of different security threats has shown in Table 6, which might support defining the stages of damages that may be accredited to specific outbreaks.

6.2 Challenges in SDN Security

This section presents the SDN security open issues and challenges.

6.2.1 Security Assessment in SDN

With flexible and programmable SDN architecture, most public operators are convinced to participate in the difficult and vast solution for the mitigation of certain situations. On the other hand, they often ignore the changes and effects in network dynamics, which occurs due to integrating such situations [129]. Moreover, the new security elements in the network are added, which can check how solutions react to the intended situation without covering the effects of deployment and integration of elements with other system members. A situation in which policies conflicts with security measures is given the applications causing the switches' flow entry mechanism. Therefore, it is mandatory to evaluate the system constraints through different steps in its complete life span. From the safety perspective, there should be a mechanism to monitor the network's present state by measuring the ideal state of network security and certain security artifacts [130, 131].

6.2.2 SDN Forensics

It is very challenging to determine the sources and root causes of the attacks in SDN. According to the SDN perspective, the methods implemented for the evidence of the attack in conventional networks are not enough. [132].

Till now, digital forensics research delivers the ability to estimate the security of deployed systems using collected and analysed detailed information about the devices and network traffic. Therefore, researchers who execute digital forensics on the devices and network traffic to contribute to the evolving capabilities like SDN. Attacks detection methods usually react to the data which is collected on multiple network elements. The network application that tracks down the entire verification with the attack flow path may require complex algorithms, machine learning instances, and threat feature databases. Forensics plays a vital role in some other security mechanisms because the results collected from the evidence and analysis can be implemented as a source to develop new protection techniques. Since data obtained from relevant attacks through the forensics handling might be giving leniency for evolution and proposal of security policies set.

Furthermore, the obtained data is also used for the exercise of machine learning methods. Also, collected packet proof can be utilized for identical criteria for inspection of profound packet mechanism.

Once the attack source is identified, the network can restructure to stop the sources which cause harm to the network [133–135].

6.2.3 Network Resilience

The fault-tolerant condition can return the network into a steady-state despite disabling or enabling the system to work properly. A significant network consists of connectivity disruption, the controller may stop working, and outages of energy [136]. These incidents affect the deployments of SDN, especially when the network is under some specific attack vector. Literature indicates that most of the researchers focus on predicting, protecting, preventing, and reacting to security concerns; nonetheless, few offers to regain the

state of the network after a very convincing and thriving attack/threat. Research has been made to detect the congested links after DDoS/DoS attacks, and the path computation method has been implemented to redistribute the congestion flows [137]. Moreover, to resolve this security challenge, a complete security system should be proposed in compound architecture, which includes proactive and reactive mechanisms. The proactive mechanisms consist of a forward-facing line to go contrary to the security circumstances; on the other side, the reactive mechanism focus on recovering the state of the network after compromising [138, 139].

6.2.4 Trusted Network App

It is hard to distinguish the controllers when a network application demands the installation of malicious flow rules in the whole infrastructure or exploit the vulnerabilities in northbound API during packet handling (Table 10). Although many applications are not specifically designed to execute the deviant behaviour, their integration with the system releases the vulnerabilities. To audit the security of a network, there is a need to implement a security technique in two ways. In the first method, an application may be audited separately, and later, they will be integrated into the SDN system for the assessment of code inspection and vulnerability. Whereas, in the second method, functional assessment is performed to detect the interaction and integration of applications with other SDN instances, which provoked an undesired behaviour. So, the suggested methods could be accompanied by a trusted authorized and authenticated mechanism [140, 141].

7 Conclusion

Despite the enhancement of existing schemes and innovative technologies where the result delivers the new mechanisms and tools to higher system security, a reliable, vital, and authenticated security in the SDN is still an exposed issue. The network attacks and vulnerabilities in SDN can increase its complexity and made it sophisticated. Therefore, a lot of work is still needed for SDN security. There are some essential SDN security perspectives, which have been discussed in this research. The paper has offered a very detailed and informative systematic literature review that reviews the status of security and privacy issues in SDN. We eliminate SDN security in the cloud, IoT perspectives and include only the main SDN security perspectives.

A total number of 69 studies were selected by implemented a systematic methodology. After extracting the required articles, an analysis was performed to investigate the SDNs security threats, security causes, solutions, and cost for implementing the solution. Furthermore, the research approaches presented in this SLR may help the practitioners and researchers to categorize the strategies that can be implemented to develop security quality. The obtained research attention relevant to SDN security issues has been paid since 2015. Apart from this, an SDN architecture also proposed possible security attacks and discussed some open challenges. Moreover, this paper would help the researchers and technologists research the security and privacy issues in SDN.

Declarations

Conflict of interest All authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Informed consent was obtained from all individual participants included in the study.

References

1. S Ortiz (2013) Software-defined networking: On the verge of a breakthrough?" Computer (Long. Beach. Calif)
2. A. Abdelaziz, et al., Distributed controller clustering in software-defined networks, *PLoS One*, Vol. 12, No. 4, pp. e174715, 2017.
3. Open Networking Foundation, Software-defined networking: the new norm for networks [white paper]", *ONF White Pap*, Vol. 2, pp. 11, 2012.
4. N. N. Dao, J. Kim, M. Park and S. Cho, Adaptive suspicious prevention for defending DoS attacks in SDN-based convergent networks", *PLoS One*, Vol. 11, No. 8, pp. e0160375, 2016.
5. F. Pakzad, M. Portmann, W. L. Tan and J. Indulska, Efficient topology discovery in OpenFlow-based Software Defined Networks, *Comput. Commun.*, Vol. 77, pp. 52–61, 2016.
6. A. Al-Najjar, S. Layeghy, and M. Portmann (2016) Pushing SDN to the end- host, network load balancing using OpenFlow," in 2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops
7. H. S. Saini, R. Sayal, and S. S. Rawat (2019) Innovations in Computer Science and Engineering, vol. 32. Springer Singapore
8. H. Bos, F. Monrose and G. Blanc, Research in attacks, intrusions, and defenses", *Lect. Notes Comput. Sci.*, Vol. 9404, pp. 427–447, 2015.
9. R. Christian (2016) SDN Malware: problems of current protection systems and potential countermeasures," pp. 89–100
10. S. Hogg (2014) SDN Security Attack Vectors and SDN Hardening | Network World," pp. 1–5
11. C. Yoon, et al., Flow wars: systemizing the attack surface and defenses in software-defined networks, *IEEE/ACM Trans. Netw.*, Vol. 25, No. 6, pp. 3514–3530, 2017.
12. Z. Zhou and T. A. Benson (2019) Composing SDN Controller Enhancements with Mozart pp. 351–363

13. N. McKeown et al., (2008) OpenFlow: enabling innovation in campus networks," ACM SIGCOMM Comput. Commun. Rev.
14. T. H. Nguyen and M. Yoo, (2017) Analysis of link discovery service attacks in SDN controller," Int. Conf. Inf. Netw., pp. 259–261
15. S. Hong, L. Xu, H. Wang, and G. Gu, (2015) Poisoning network visibility in software-defined networks: new attacks and countermeasures
16. K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, Software-defined networking (SDN): a survey", *Secur. Commun. Networks*, Vol. 9, No. 18, pp. 5803–5833, 2016.
17. Z. Hu, M. Wang, X. Yan, Y. Yin, and Z. Luo (2015) A comprehensive security architecture for SDN," in 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015
18. A Sebbar, M Boulmalf, M Dafir Ech-Cherif El Kettani, and Y Badd (2018) Detection MITM Attack in Multi-SDN Controller," in Colloquium in Information Science and Technology, CIST
19. P. W. Chi, C. T. Kuo, J. W. Guo, and C. L. Lei (2015) How to detect a compromised SDN switch," in 1st IEEE conference on network softwarization: software-defined infrastructures for networks, clouds, IoT and Services, NETSOFT 2015
20. A. Pradhan and R. Mathew, Solutions to vulnerabilities and threats in software defined networking (SDN), *Procedia Comput. Sci.*, Vol. 171, No. 2019, pp. 2581–2589, 2020.
21. Y. Meng, Z. Huang, S. Wang, G. Shen, and C. Ke (2020) SOM-based DDoS Defense Mechanism using SDN for the Internet of Things," 1–10
22. A. R. Abdou, P. C. Van Oorschot and T. Wan, Comparative analysis of control plane security of SDN and conventional networks, *IEEE Commun. Surv. Tutorials*, Vol. 20, No. 4, pp. 3542–3559, 2018.
23. T. Han et al., (2019) A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers," Concurr. Comput., pp. 3–5
24. H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li, and C. F. Cheang (2018) A Survey on Security-Aware Measurement in SDN," Secur. Commun. Networks, 2018
25. I. Ahmad, S. Namal and M. Ylianttila, Security in software defined networks: a survey, *IEEE Communication Surveys & Tutorials*, Vol. 17, pp. 4, 2015.
26. Wenjuan Li and Weizhi Meng, Lam For Kwok, A survey on OpenFlow-based software defined networks: security challenges and countermeasures, *Journal of Network and Computer Applications*, Vol. 68, pp. 126–139, 2016.
27. W. Li and W. Meng, A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures, *Journal of Network and Computer Applications*, Vol. 68, pp. 126–139, 2016.
28. Vasileios Gkioulos, Håkon. Gunleifsen and Goitom K. Weldehawaryat, A Systematic literature review on military software defined networks, *Future Internet*, Vol. 10, No. 9, pp. 88, 2018.
29. W. Hassan, T. Chou and L. Xiaoming, Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks, *International Journal of Informatics and Communication Technology*, Vol. 8, pp. 162, 2019.
30. T. Han, S. R. U. Jan and T. Zhiyuan, A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers, *Concurrency Computat Pract Exper*, Vol. 32, pp. 16, 2019.
31. A. Shirmarz and A. Ghaffari, Performance issues and solutions in SDN-based data center: a survey, *J Supercomput*, Vol. 76, pp. 7545–7593, 2020.
32. Camilo, J., Chica, C., and Botero, J.F., Security in SDN: A comprehensive survey, Journal of Network and Computer Applications, 2020
33. Shaghaghi A., Kaafar M.A., Buyya R., Jha S. (2020) Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer
34. S. K. Keshari, V. Kansal and S. Kumar, A Systematic Review of Quality of Services (QoS) in Software Defined Networking (SDN), *Wireless Pers Commun*, Vol. 116, pp. 2593–2614, 2021.
35. S. Ahmad and A. H. Mir, Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN Controllers, *J Netw Syst Manage*, Vol. 29, pp. 9, 2021.
36. S. Matsumoto, S. Hitz, and A. Perrig (2014) Fleet: Defending SDNs from malicious administrators," HotSDN 2014 - Proc. ACM SIGCOMM 2014 Work. Hot Top. Softw. Defin. Netw., pp. 103–108,
37. S. Scott-Hayward, C. Kane, and S. Sezer, "OperationCheckpoint: SDN application control," Proc. - Int. Conf. Netw. Protoc. ICNP, pp. 618–623
38. P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran, "Securing the Software Defined Network Control Layer," 2015
39. K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson (2018) Systematic mapping studies in software engineering," in 12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008
40. A. Fernandez, E. Insfran, and S. Abrahão, "Usability evaluation methods for the web: A systematic mapping study," in Information and Software Technology, 2011
41. J. Xia, Z. Cai, G. Hu and M. Xu, An active defense solution for arp spoofing in open flow network, *Chinese J. Electron.*, Vol. 28, No. 1, pp. 172–178, 2019.
42. C. Zhang, et al., Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack, *IEEE Access*, Vol. 6, pp. 22764–22777, 2017.
43. T. Park et al., "DPX : Data-Plane eXtensions for SDN Security Service Instantiation
44. A. Molina Zarca, et al., Security management architecture for NFV/SDN-Aware IoT systems", *IEEE Internet Things J.*, Vol. 6, No. 5, pp. 8005–8020, 2019.
45. A. Destounis, et al., Minimum Cost SDN Routing With Reconfiguration Frequency Constraints, *IEEE/ACM Transactions on Networking*, Vol. 26, No. 4, pp. 1577–1590, 2018.
46. Z. Su and L. Wang, "CFlam : cost-effective flow latency monitoring system for software defined networks", 2019 IEEE 20th Int, *Conf. High Perform. Switch. Routing*, Vol. 25, pp. 3309–3322, 2019.
47. K. Kogan, S. I. Nikolenko, P. Eugster, A. Shalimov and O. Rottenstreich, "Distributed Platforms, *IEEE/ACM Trans. Networking*, Vol. 25, No. 6, pp. 1–14, 2017.
48. Y. Cui, et al., Author ' s Accepted Manuscript SD-Anti-DDoS : Fast and Efficient DDoS defense in software-defined networks reference, *J. Netw. Comput. Appl.*, Vol. 68, pp. 65–79, 2016.
49. S. Gao, Z. Li, B. Xiao and G. Wei, Security threats in the data plane of software-defined networks, *IEEE Netw.*, Vol. 32, No. 4, pp. 108–113, 2018.
50. K. Kalkan, L. Altay, G. Gür and F. Alagöz, JESS: joint entropy-based DDoS defense scheme in SDN, *IEEE J. Sel. Areas Commun.*, Vol. 36, No. 10, pp. 2358–2372, 2018.
51. Y. Park, S. Y. Chang, and L. M. Krishnamurthy, "Watermarking for detecting freeloader misbehavior in software-defined networks," 2016 Int. Conf. Comput. Netw. Commun. ICNC 2016, 2016
52. S. Midha and K. Triptahi, "Extended TLS security and defensive algorithm in openflow SDN," Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019: 141–146, 2019
53. H. Xu, Z. Yu, C. Qian, and X. Li (2017) Minimizing Flow Statistics Collection Cost of SDN Using Wildcard Requests," pp. 1–9

54. H. Shafiq, R. A. Rehman, and B. S. Kim (2018) Services and Security Threats in SDN Based VANETs: A Survey," Wirel. Commun. Mob. Comput., 2018
55. C. Yoon, P. Porras, M. Fong, B. O. Connor, and T. Vachuska A Security-Mode for Carrier-Grade SDN Controllers," pp. 461–473
56. M. Suh, S. H. Park, B. Lee, and S. Yang, "Building firewall over the software-defined network controller," Int. Conf. Adv. Commun. Technol. ICACT, pp. 744–748, 2014
57. I. Farris, T. Taleb, Y. Khettab and J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, *IEEE Commun. Surv. Tutorials*, Vol. 21, No. 1, pp. 812–837, 2019.
58. T. V. Phan, N. K. Bao and M. Park, Distributed-SOM: A novel performance bottleneck handler for large-sized software-defined networks under flooding attacks, *J. Netw. Comput. Appl.*, Vol. 91, No. April, pp. 14–25, 2017.
59. L. A. Trejo, V. Ferman, M. A. Medina-Pérez, F. M. Arredondo Giacinti, R. Monroy and J. E. Ramirez-Marquez, DNS-ADVP: A machine learning anomaly detection and visual platform to protect top-level domain name servers against DDoS attacks", *IEEE Access*, Vol. 7, pp. 116358–116369, 2019.
60. Z. Shah and S. Cosgrove, Mitigating arp cache poisoning attack in software-defined networking (sdn): A survey, *Electron.*, Vol. 8, No. 10, pp. 1–26, 2019.
61. A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions," IEEE/IFIP NOMS 2014 - IEEE/IFIP Netw. Oper. Manag. Symp. Manag. a Softw. Defin. World, no. May, 2014
62. S. Ahmed and N. Medhi, A flow marking based anti-spoofing Mechanism (FMAS) using SDN approach, *Adv. Intell. Syst. Comput.*, Vol. 563, pp. 245–255, 2018.
63. J. Zhou, J. N. B, and Y. Rao (2017) Block-based convolutional neural network. nternational Workshop on Digital Watermarking 1: 65–76
64. S. Shin, L. Xu, S. Hong, and G. Gu (2016) Enhancing Network Security through Software Defined Networking (SDN)," 2016 25th Int. Conf. Comput. Commun. Networks, ICCCN 2016
65. N. Noceti, L. Zini and F. Odone, A multi-camera system for damage and tampering detection in a postal security framework, *Eurasip J. Image Video Process.*, Vol. 2018, No. 1, pp. 1–13, 2018.
66. P. Ahmad, S. Jacob, and R. Khondoker, "Security Analysis of SDN Applications for Big Data
67. K. Benton, L. J. Camp, and C. Small, "OpenFlow Vulnerability Assessment Categories and Subject Descriptors," Proc. Second ACM SIGCOMM Work. Hot Top. Softw. Defin. Netw. - HotSDN '13, pp. 151
68. P. Kazemian, M. Chang, H. Zeng, G. Varghese, N. McKeown, and S. Whyte, "Real time network policy checking using header space analysis," Proc. 10th USENIX Symp. Networked Syst. Des. Implementation, NSDI 2013, pp. 99–111, 2019
69. S Shin G Gu Attacking software-defined networks: A first feasibility study", HotSDN 2013 - Proc. 2013 ACM SIGCOMM Work Hot Top. Softw. Defin. Netw. 3 165–166 2013
70. S. Shin, V. Yegneswaran, P. Porras, and G. Gu, (2013) AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," Proc. ACM Conf. Comput. Commun. Secur., 413–424, 2013
71. J. Moura and D. Hutchison (2020) Resilient Cyber-Physical Systems: Using NFV Orchestration," pp. 1–13
72. M. Niemiec, P. Jaglarz, M. Jekot, P. Chołda, and P. Boryło, "Risk Assessment Approach to Secure Northbound Interface of SDN Networks," pp. 164–169, 2019
73. Y. Tian, V. Tran and M. Kuerban, "DOS Attack mitigation strategies on SDN controller", 2019 IEEE 9th Annu, *Comput. Commun. Work. Conf. CCWC*, Vol. 2019, pp. 701–707, 2019.
74. V. Sridharan, K. S. K. Liyanage, and M. Gurusamy, "Privacy-Aware Switch-Controller Mapping in SDN-Based IoT Networks," 2020 Int. Conf. Commun. Syst. NETworkS, COMSNETS 2020, pp. 1–6
75. M. M. Alshaer, M. Al-Akhras and A. Albesher, IEEE World Conf, *Complex Syst. WCCS*, Vol. 2019, No. 4, pp. 1–5, 2019.
76. S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers", 2015 Int, *Conf. Comput. Netw. Commun. ICNC*, Vol. 2015, pp. 77–81, 2015.
77. N. M. Sahri and K. Okamura, Protecting DNS services from IP spoofing-SDN collaborative authentication approach, *ACM Int. Conf. Proceeding Ser.*, Vol. 15–17, pp. 83–89, 2016.
78. R. Skowyra, et al., Effective topology tampering attacks and defenses in Software-Defined networks", Proc. - 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst, *Networks, DSN*, Vol. 2018, pp. 374–385, 2018.
79. A. Shirmarz and A. Ghaffari, *Performance issues and solutions in SDN- based data center: a survey*, Springer, US, 2020.
80. M. Li, X. Wang, H. Tong, T. Liu, and Y. Tian, "SPARC: Towards a scalable distributed control plane architecture for protocol-oblivious SDN
81. W. Rankothge (2019) Past before future: a comprehensive review on software defined networks road map 19: 1
82. H. Hu, et al., Towards a reliable firewall for software-defined networks, *Comput. Secur.*, Vol. 87, 101597, 2019.
83. R. Beckett, X. K. Zou, S. Zhang, S. Malik, J. Rexford, and D. Walker An assertion language for debugging SDN applications," HotSDN 2014 - Proc. ACM SIGCOMM 2014 Work. Hot Top. Softw. Defin. Netw., pp. 91–96, 2014
84. A. Al-Alaj, R. Sandhu, and R. Krishnan, "A formal access control model for SE-floodlight controller," SDN-NFV 2019 - Proc. ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct
85. L. V. Morales, A. F. Murillo, S. J. Rueda and "Extending the floodlight controller", Proc. -, IEEE 14th Int, *Symp. Netw. Comput. Appl. NCA*, Vol. 2015, No. 126–133, pp. 2016, 2015.
86. E. Al-Shaer and S. Al-Haj (2010) FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures," Proc. ACM Conf. Comput. Commun. Secur., 37–44
87. G. N. Nde and R. Khondoker (2016) SDN testing and debugging tools: A survey," 2016 5th Int. Conf. Informatics, Electron. Vision, ICIEV 2016, pp. 631–635
88. P. Fonseca, R. Bennesby, E. Mota and A. Passito, A replication component for resilient OpenFlow-based networking", Proc. 2012 IEEE Netw, *Oper. Manag. Symp. NOMS*, Vol. 2015, pp. 933–939, 2012.
89. N. Sultana, N. Chilamkurti, W. Peng and R. Alhadad, Survey on SDN based network intrusion detection system using machine learning approaches, *Peer-to-Peer Netw. Appl.*, Vol. 12, No. 2, pp. 493–501, 2019.
90. H. Maziku, S. Shetty and D. M. Nicol, Security risk assessment for SDN-enabled smart grids, *Comput. Commun.*, Vol. 133, pp. 1–11, 2019.
91. A. Shaghaghi, M. A. Kaafar, R. Buyya and S. Jha, *Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions"*, Comput. Networks Cyber Secur, Handb, 2020. https://doi.org/10.1007/978-3-030-22277-2_14.
92. S. R. Chowdhury, F. Bari, R. Ahmed, and R. Boutaba (2014) PayLess : A Low Cost Network Monitoring Framework for Software Defined Networks
93. J. Yao, Z. Han, M. Sohail and L. Wang, A robust security architecture for SDN-based 5G networks, *Futur. Internet*, Vol. 11, No. 4, pp. 1–14, 2019.
94. C. Yoon, T. Park, S. Lee, H. Kang and S. Shin, Enabling security functions with SDN : A feasibility study, *Comput. Networks*, Vol. 85, No. 2015, pp. 19–35, 2016.

95. H. Hu, W. Han, G. Ahn, and Z. Zhao (2014) F LOW G UARD : Building Robust Firewalls for Software-Defined Networks 97–102
96. M. Wang, J. Liu, J. Chen, X. Liu, and J. Mao (2016) PERM-GUARD : Authenticating the validity of flow rules in software defined networking," J. Signal Process. Syst., 37
97. S. N. Matheu, et al., Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems, *Sensors (Switzerland)*, Vol. 20, No. 7, pp. 1–33, 2020.
98. Z. Zhao, D. Gong, B. Lu, F. Liu, and C. Zhang (2016) SDN-based double hopping communication against sniffer attack
99. M. Andreoni, L. Diogo, M. Ferrazani, and O. C. M. B. Duarte (2016) An elastic intrusion detection system for software networks," Ann. Telecommun
100. X. Chen and S. Yu, (2015) CIPA : A Collaborative Intrusion Prevention Architecture for Programmable Network and SDN," Comput. Secur
101. J. Sonchack, A. J. Aviv, E. Keller, and J. M. Smith (2015) Poster : OFX : Enabling OpenFlow Extensions for Switch-Level Security Applications pp.1678–1680
102. M. Dhawan (2015) S PHINX : detecting security attacks in software-defined networks," no. 8–11
103. B. Wang, Y. Zheng, W. Lou and Y. T. Hou, DDoS attack protection in the era of cloud computing and software-defined networking, *Comput. NETWORKS*, Vol. 81, pp. 308–319, 2015.
104. S. Fichera, L. Galluccio, S. C. Grancagnolo, G. Morabito, and S.Palazzo (2015) OPERETTA : An OPEnflow-based REmedy to mitigate TCP SYNFLOOD Attacks against web servers," Comput. Networks
105. J. W. Kang, S. H. Park, and J. You (2015) Mynah : enabling lightweight data plane authentication for SDN controllers
106. M. S. H. Ll, G. A. I. E, J. I. Vélez, and L. C. O (2016) Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype," pp.33–41
107. Kaur S., Kumar K., Aggarwal N. (2021) A Review of Security Threats in Software-Defined Networking. In: Singh B., Coello Coello C.A., Jindal P., Verma P. (eds) Intelligent Computing and Communication Systems. Algorithms for Intelligent Systems. Springer, Singapore
108. K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed SDN controllers in a multi-domain environment," in Proc. IEEE NOMS, May 2014, pp. 1–2
109. K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed multidomain SDN controllers in Proc. IEEE NOMS, May 2014, pp. 1–4
110. E. Al-Shaer and S. Al-Haj, FlowChecker: Configuration analysis and verification of federated openflow infrastructures in Proc. 3rd ACM Workshop SafeConfig, 2015, pp. 37–44
111. P. Porras et al., A security enforcement kernel for OpenFlow networks," in Proc. 1st Workshop HotSDN, 2016, pp. 121–126
112. N. L. van Adrichem, C. Doerr, and F. A. Kuipers, "OpenNetMon: Network monitoring in OpenFlow software-defined networks," in Proc. IEEE NOMS, May 2014, pp. 1–8
113. S. R. Chowdhury, M. Bari, R. Ahmed, and R. Boutaba, "PayLess: A low cost network monitoring framework for software defined networks," in Proc. IEEE NOMS, 2014, pp. 1–9
114. K. Wang, Y. Qi, B. Yang, Y. Xue, and J. Li, "LiveSec: Towards effective security management in large-scale production networks," in Proc. ICDCSW, Jun. 2015, pp. 451–460
115. X. Liu, H. Xue, X. Feng, and Y. Dai, "Design of the multi-level security network switch system which restricts covert channel," in Proc. IEEE 3rd ICCSN, May 2016, pp. 233–237
116. A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions," in Proc. IEEE NOMS, May 2017, pp. 1–9
117. P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A replication component for resilient OpenFlow-based networking," in Proc. IEEE NOMS, Apr. 2016, pp. 933–939
118. P. Smith, A. Schaeffer-Filho, D. Hutchison, and A. Mauthe, "Management patterns: SDN-enabled network resilience management," in Proc. IEEE NOMS, May 2017, pp. 1–9
119. M. Suh, S. H. Park, B. Lee, and S. Yang, "Building firewall over the software-defined network controller," in Proc. 16th ICACT, Feb. 2016, pp. 744–748
120. M. Koerner and O. Kao, "Oftables: A distributed packet filter," in Proc. 6th Int. Conf. COMSNETS, Jan. 2017, pp. 1–4
121. Hao, T. Lakshman, S. Mukherjee, and H. Song, "Secure cloud computing with a virtualized network infrastructure," in Proc. 2nd USENIX Conf. Hot Topics Cloud Comput., 2016, 16
122. H. Hu, W. Han, G.-J. Ahn, and Z. Zhao, "FLOWGUARD: building robust firewalls for software-defined networks," in Proc. 3rd Workshop Topics Softw. Defined Netw., 2017, 97–102.
123. E. Maccherani et al., "Extending the NetServ autonomic management capabilities using OpenFlow," in Proc. IEEE NOMS, Apr. 2012, pp. 582–585
124. T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar (2016) SnortFlow: A openflow-based intrusion prevention system in cloud environment," in Proc. 2nd GREE, Mar. 89–92
125. S. Shirali-Shahreza and Y. Ganjali (2015) Empowering software defined network controller with packet-level information," in Proc. IEEE ICC, pp. 1335–1339
126. S. Shirali-Shahreza and Y. Ganjali, (2015) Efficient implementation of security applications in openflow controller with flexam," in Proc. IEEE 21st Annu. Symp. HOTI, 49–54
127. J. Hu, M. Reed, N. Thomos and M. F. AI-Naday and K. Yang, Securing SDN-Controlled IoT Networks Through Edge Blockchain, *IEEE Internet of Things Journal*, Vol. 8, No. 4, pp. 2102–2115, 2021.
128. T. Hasan, A. Adnan, T. Giannetsos and J. Malik, "Orchestrating SDN Control Plane towards Enhanced IoT Security," 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020
129. D. Javeed, T. Gao and M. T. Khan, SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT, *Electronics*, Vol. 10, pp. 918, 2021.
130. Marcos V.O.. de Assis, Luiz F. Carvalho, Joel J.P.C.. Rodrigues, Jaime Lloret and Mario L. Proença Jr, Near real-time security system applied to SDN environments in IoT networks using convolutional neural network, *Computers & Electrical Engineering*, Vol. 86, pp. 1067, 2020.
131. Mevlut Serkan Tok, Mehmet Demirci (2021) Security analysis of SDN controller-based DHCP services and attack mitigation with DHCP guard, Computers & Security
132. I. Akbari, E. Tahoun, M. A. Salahuddin, N. Limam and R. Boutaba (2020) ATMoS: Autonomous Threat Mitigation in SDN using Reinforcement Learning NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium pp. 1–9
133. Revathi, M., Ramalingam, V.V. & Amutha, B. A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework. Wireless Pers Commun (2021)
134. A. H. M. Jakaria, M. A. Rahman and A. Gokhale, Resiliency-Aware Deployment of SDN in Smart Grid SCADA: A Formal Synthesis Model in, *IEEE Transactions on Network and Service Management*, Vol. 18, No. 2, pp. 1430–1444, 2021.
135. H. Jo, J. Nam, and S. Shin (2018) NOSArmor: Building a Secure Network Operating System," Secure. Commun. Networks 2018

136. S. ZHANG, X. MENG, and L. WANG (2017) SDNForensics: A Comprehensive Forensics Framework for Software Defined Network," 54: 92–99
137. S. Lee, C. Yoon, C. Lee, S. Shin, V. Yegneswaran, and P. Porras, "DELTA: A Security Assessment Framework for Software-Defined Networks 2017.
138. D. Kreutz, J. Yu, P. Esteves-Verissimo, C. Magalhaes and F. M. V. Ramos, The KISS principle in software-defined networking: A framework for secure communications, *IEEE Secure. Priv.*, Vol. 16, No. 5, pp. 60–70, 2018.
139. N. Gray, T. Zinner, and P. Tran-Gia, "Enhancing SDN security by device fingerprinting," Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integer. Netw. Serv. Manag., pp. 879–880, 2017
140. M. Cheminod, L. Durante, L. Seno, F. Valenza, A. Valenzano and C. Zunino, *Leveraging SDN to improve security in industrial networks*, pp. 1–7, IEEE Int. Work. Fact. Commun. Syst. - Proceedings, WFCS, 2017.
141. S. Hyun, et al., Interface to network security functions for cloud-based security services, *IEEE Commun. Mag.*, Vol. 56, No. 1, pp. 171–178, 2018.
142. W. Lee and N. Kim, Security policy scheme for an efficient security architecture in software-defined networking", *Inf.*, Vol. 8, No. 2, pp. 65, 2017.
143. L. Gifre, B. Shariati, and L. Velasco (2018) Experimental Demonstration of Active and Passive Optical Networks Telemetry," pp. 2017–2019
144. N. L. M. Van Adrichem, C. Doerr, and F. A. Kuipers, "OpenNetMon: Network monitoring in OpenFlow software-defined networks," IEEE/IFIP NOMS 2014 - IEEE/IFIP Netw. Oper. Manag. Symp. Manag. a Softw. Defin. World, 2014
145. M. Koerner and O. Kao, "Oftables: A distributed packet filter," 2014 6th Int. Conf. Commun. Syst. Networks, COMSNETS 2014, pp. 14–17, 2014
146. A. Schaeffer-Filho, P. Smith, A. Mauthe and D. Hutchison, Network resilience with reusable management patterns, *IEEE Commun. Mag.*, Vol. 52, No. 7, pp. 108–115, 2014.
147. C. Bouras, P. Ntarzanos, and A. Papazois, "Cost Modeling for SDN / NFV Based Mobile 5G Networks," pp. 87–92, 2016
148. C. Zhang, X. Wang, Y. Zhao, A. Dong, F. Li and M. I. N. Huang, Cost efficient and low-latency network service chain deployment across multiple domains for SDN, *IEEE Access*, Vol. 7, pp. 143454–143470, 2019.
149. D. Chourishi, A. Miri, M. Milic, S. Ismaeel and "Role-based multiple controllers for load balancing and security in SDN", IEEE Canada Int, *Humanit. Technol. Conf. IHTC*, Vol. 2015, pp. 2015, 2015.
150. Diego and Ramos, Fernando MV and Verissimo, Paulo Esteves and Rothenberg, Christian Esteve and Azodolmolky, Siamak and Uhlig, Steve Kreutz, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, Vol. 103, pp. 14–76, 2014.

Naveed Ahmed is a Ph.D. scholar at Universiti Teknologi Malaysia. He is a member of Pervasive Computing Research Group (PCRG). He received his master degree in Computer Science from International Islamic University Islamabad, Pakistan, in 2004, MS degree in Computer and Communication Security, from School of Electrical Engineering & Computer Sciences, NUST, Islamabad, Pakistan, in 2015. His research interested includes Software Defined Network (SDN), Network Virtualization, Network Security, Cloud & Edge Computing, Blockchain, Internet of things(IOT), and Secure Artificial Intelligent(AI) Systems.

Kamalrulnizam Bin Abu Bakar is a Professor in Computer Science at Universiti Teknologi Malaysia, Malaysia, and a member of the Pervasive Computing Research Group (PCRG). He received M.Sc. degree in Computer Communications and Networks, from Leeds Metropolitan University, United Kingdom, in 1998, and his Ph.D. degree in Computer Science from Aston University, United Kingdom, in 2004. His research interest includes mobile and wireless computing, information security. He is member of the ACM, Internet Society (ISOC), and International Association of Engineering (IAENG). He involves in many research projects and is a referee for several scientific journals and conferences.

Fatima Tul Zuhra Dr. Fatima Tul Zuhra is a Researcher of Universiti Teknologi Malaysia under the Post-Doctoral Fellowship project: Efficient Route Stability-Aware Routing Scheme for Wireless Body Sensor Networks. She is a member of the PCRG. She received her BS(cs) degree in 2009 from the Quaid-e-Awam University of Engineering, Science & Technology, Pakistan and the MCS degree in 2016 from the University of Malaya, Malaysia. She received her Ph.D. degree in Computer Science

from the Universiti Teknologi Malaysia, Malaysia in 2020. Her research interest includes wireless networks, routing algorithms, IoT, AI, blockchain and cloud computing.

Tanzila Kehkashan is a lecturer in Computer Science at University of Lahore, Pakistan. She is a Ph.D. scholar at Universiti Technologi Malaysia and a member ofVirtual, Visualization and Vision Research Group (UTM VicubeLab). She received her Master degree in CS in 2003 and MS in 2005 from University of Central Punjab, Lahore, Pakistan. Her research interest includes cloud computing, computer vision, deep learning and NLP. She has been involved in research projects including sensor-based irrigation, SaaS-based predictions, speech synthesis, NER, VQA and image captioning, plagiarism detection and removal. She has many publications in international journals and conferences.

Muhammad Akram Mujahid received the MSc. Degree in computer science from Punjab University College of Information Technology, Lahore, Pakistan in 2004, and MS degree from University of the Lahore in 2015. He is working as Assistant Professor at University of Education, Lahore, Pakistan. He is currently pursuing the PhD degree with Universiti Teknologi Malaysia. His research interests include VANETs, big data analytics, and cloud computing.

Muhammad Siraj Rathore is an assistant professor at capital University of Science and Technology Islamabad Pakistan, Pakistan. He earned his Ph.D. degree from KTH Royal Institute of Technology, Sweden in 2017. At KTH, he engaged with teaching and networking research activities for several years. He received MS computer engineering degree from University of Engineering and Technology Taxila, Pakistan in 2005. His research interests are network unction virtualization, programmable networks, software defined networking, network security and cloud computing.

Muhammad Dawood is a Ph.D. scholar at Universiti Teknologi Malaysia, he received his MS Degree in computer science from Universiiti Teknologi Malaysia. He is working as Assistant Professor at Balochistan University of Engineering and Technology Khuzdar. His research interests include Network Security, Cloud & Edge Computing, Internet of things(IOT), and Secure Artificial Intelligent(AI) Systems.

Babangida Isyaku is a Ph.D scholar at Universiti Teknologi Malaysia. He received his MSc. Computer Science from the same university. He completed his BSc. Computer science and information system degree from Oxford Brookes University. His research interest includes Software Defined Networking, Failure Recovery, etc.