


Article

Future Technology: Software-Defined Network (SDN) Forensic

Quadri Waseem ^{1,*}, Sultan S. Alshamrani ^{2,*} , Kashif Nisar ³, Wan Isni Sofiah Wan Din ⁴
and Ahmed Saeed Alghamdi ²

¹ AnalytiCray, No 2-16, Jalan Pandan Prima 2, Dataran Pandan Prima, Kuala Lumpur 55100, Malaysia

² Department of Information Technology, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; asjannah@tu.edu.sa

³ Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia; kashif@ums.edu.my

⁴ Faculty of Computing, University Malaysia Pahang, Gambang, Pahang 26300, Malaysia; sofiah@ump.edu.my

* Correspondence: qwaseem@analyticray.com (Q.W.); susamash@tu.edu.sa (S.S.A.)

Abstract: The software-defined networking (SDN) paradigm has recently emerged as a trend to build various protocols, develop more reliable networks, enhance the data flow controlling, and provide security in a much simpler and flexible way. SDN helps to ease management and handle asymmetric connectivity across various nodes. It solves the problems of network and cloud security and hence provides the best solution for the safety of data on the network. Therefore, we feel the urge to research more and provide the basics of SDN forensics, mention its advantages in network especially in the cloud, and present its elaborate prospects in context with Network Forensic (NF) and Cloud Forensic (CF). In this research article, we explained in detail the NF and CF with emphasis on Network security (NS) and Cloud Security (CS). The paper also provided the various security approaches and categories. Then, an overview of the software-defined networking (SDN) is mentioned. We also discussed the use of SDN in Network Forensic and Cloud Forensic. Furthermore, to aid the SDN forensic, we presented the advantages, challenges, and issues along with future research directions of SDN in network forensic and cloud forensic, and at last, we thus express and explore the need for security in forensic based on the SDN paradigm in the form of a set of suggested recommendations.

Keywords: network security; network forensic; cloud security; cloud forensic; software defined networking



Citation: Waseem, Q.; Alshamrani, S.S.; Nisar, K.; Wan Din, W.I.S.; Alghamdi, A.S. Future Technology: Software-Defined Network (SDN) Forensic. *Symmetry* **2021**, *13*, 767. <https://doi.org/10.3390/sym13050767>

Academic Editors: Debiao He and Peng-Yeng Yin

Received: 11 March 2021

Accepted: 23 April 2021

Published: 28 April 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Digital forensics [1] includes the depth investigation of attacks and the collection of traces left by the intruders after any suspicious events or malicious code is detected. The traces from the intruders act as evidence to regenerate the attack and enable the computer systems to enhance the security for future threats. The basic forensics steps are divided into five main steps which include (1) Identification phase, where it is identified whether a crime has occurred or not? This method uses the anomalies detected by IDS and suspicious events for identification purposes. (2) Evidence Collection phase, where the forensic experts identify the evidence from SaaS, IaaS, and PaaS sources of cloud service models. (3) Examination and Analysis phase, where the forensic experts inspect the gathered evidence, correlates, and produces the conclusion. (4) Preservation phase, this phase guarantees the data integrity and needs a large volume of data storage for further investigation. In this phase, the gathered information is fully protected. (5) Presentation and Reporting phase, where a finding report is created by the forensic experts based on their findings related to a specific case [1,2].

Digital forensic is categorized based on the Application domain. A digital forensic in context with network management is called network forensic, digital forensic in context with cloud computing is called cloud forensic, digital forensic in context with the web is called web forensic, and digital forensic in context with mobile is called mobile forensic.

For efficient network management, network security is always considered a priority concern. The success of network management is mostly anticipated by the smooth working of their applications [3].

Over a couple of years, we have noticed the wide adoption of a very new concept in the field of networking, which is so-called Software Defined Networks. The Software-Defined Networking (SDN) paradigm has recently turned up as an intended technology to ease network security and cloud security issues especially in context with network forensic and cloud forensic [4]. Forensics is still at an early stage in SDN and currently has a minimal number of contributions. SDN provides digital forensics support as it allows the safe preservation of network activity traces to determine the root causes of various issues. Along with storage, it provides general support in the form of centralized control. However, the centralized control of SDN facilitates to configure and manage the network devices at one point which indirectly opens a door for breaches and failure due to a single point concept. Network forensic and cloud forensic are highly dependent aspects of SDN forensic. Both aspects deliver the same aim, while both are however different in their approaches. Consequently, the network is considered a crucial part of cloud computing, Network Forensic identifies and analyzes the evidence from the network (whether Private or public). It then reclaims the information on which network ports are used [2], while cloud forensic represents the forensic of cloud architectures. Despite the significant advantages of networks and cloud architecture, security in networks and clouds is always a big concern for the forensic team or investigating team.

To the best of our knowledge, none of the research has so far focused on SDN forensics, especially in context with network and cloud forensic. The paper provides a systematic review of SDN forensic starting from its background, fundamental concepts, SDN issues in network, and cloud forensic, along with future work and recommendations.

The contribution of this paper can be summarized as follows:

- Discussing recent articles which investigate the research on network and cloud forensic from the security point of view.
- Providing various categories of network and cloud forensic, their relationship, and their comparison.
- Discussing SDN forensic and providing various approaches.
- Discussing the advantages of using SDN in network and cloud forensic.
- Investigating the challenges and issues of SDN in network and cloud forensic.
- Discussing future research directions of SDN in network and cloud forensic.

The rest of this paper is structured as follows: Section 2 of this paper discusses the background of our research (starting from network security to network forensic and cloud security to cloud forensic). In Section 3, we provide the details about the SDN, its forensic, and also its utilization in network and cloud forensic along with advantages, issues, and challenges. Moreover, the future directions of using the SDN in network forensic and cloud forensic were also discussed. The need for security in forensic (network and cloud) has been explored in the form of discussion and recommendations which are presented in Section 4. Section 5 concludes this study.

Figure 1 presents the taxonomy of this research article. We have tried to elaborate SDN, SDN Forensic in context with Network forensic and Cloud Forensic along with its strength, weakness, challenges and future research directions in the current scenario based on the current advances from academia and industry.

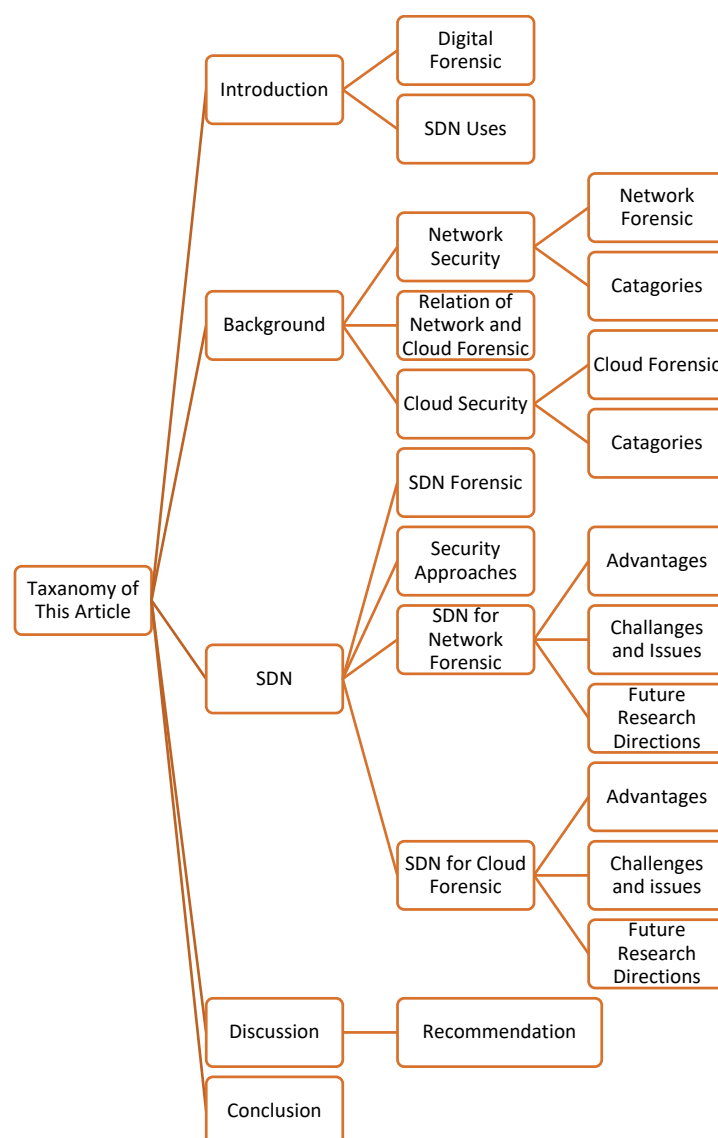


Figure 1. Taxonomy of this Article.

2. Backgrounds

Before discussing in Section 3, the software-defined networking and their utilization in network forensic and cloud forensic. In this section we attempt to narrow the scope of network forensic and cloud forensic by discussing their background starting from the network security and cloud security point of view. Our goal in this section is to explain the network and cloud forensic in context with their security. To do this, we first discuss the network security and network forensic, then we will discuss the cloud security and cloud forensic that are most pertinent to the ensuing discussion. Figure 2 unveils the background details of network and cloud forensic from a security point of view.

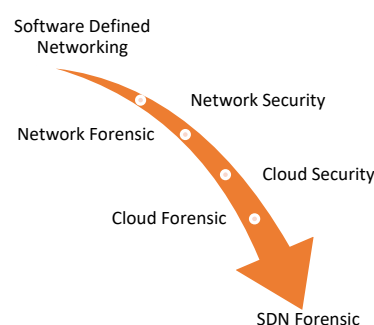


Figure 2. Background of network and cloud forensic from the security viewpoint.

2.1. Network Security

For network security, a network forensic is a preferred technique to get the hidden details of the attacks and their causes. Network forensics is a tool for the identification, compilation, storage, examination, and reporting of network digital evidence. Network forensics is a technique adopted by various network administrators to investigate to find the source of the attack [1]. For proper functioning, it is crucial to secure networks (end-hosts, servers, and other related assets) and for the forensic investigation to detect attack attempts, whether they are successful or not. It is also important to recognize simple anomalous patterns for a solution, to be able to detect as many ways of attack and malicious activities as possible, Ref. [5] for attaining better security.

2.1.1. Network Forensics

Network forensics [6,7] is a critical part of security for the network-based stream data. Network forensics focuses primarily on surveillance and analysis of network traffic to track, avoid, and diagnose security incidents [8]. In automated and real-time devices that are connected to the internet, there is always a cyber risk that harms the operations over network systems. Therefore, it is important to conduct and evaluate forensic behavior in all devices linked to a network. The network also has a specific view of the event in most data breach cases or data abuse scenarios [9]. During the investigation process, network forensics faces a huge challenge which includes a huge amount of network traffic. Therefore, rigorous processing is required for analysis and most of the data is irrelevant, which creates problems in accessing the network and cloud architectures [10]. In paper [11], the author has given many references related to network security using different aspects of the network forensic. Some of the existing approaches address the full forensics process, some references deal with managing and effectively storing the forensic data, and some mention the intrusion detection techniques for the detection and reporting purpose for the forensic investigation processing [11]. Network forensic acts as a tool to identify and detect the network loopholes and prevent further failures by detecting the root cause of the issue or exposing the attacker's intentions.

2.1.2. Categories of Network Forensic

(Investigation Mode and Data Processing Mode Classification)

There are two categories of network forensic based on investigation mode, the first one is online, and another is offline network forensic [12]. This type of investigation depends on the time of the investigation.

(A) Online/Live Network Forensics

This type of network forensic is also known as dynamic forensics, here the investigation is performed at the time of its flow. Online network forensic is mostly suitable for large, distributed networks, and hence it requires more computational resources, and a huge amount of storage is a basic requirement.

(B) Offline Network Forensic

This type of network forensic is also known as static forensics, here the network data is captured, recorded, and analyzed after the attack. It correctly records every occurrence from network logs and monitors the behavior of intruders briefly and accurately but due to lack of storage space, there is a possibility of overwriting existing data and there is no guarantee that the information is not changed by the intruder.

There are two categories of network forensic based on data processing mode, the first one is proactive, and another is reactive network forensic [12]. This type of investigation depends on the execution definition (a type of approach used).

(1) Proactive Network Forensic

Used for real-time investigation of the incident by supplying the device with automation while reducing user interaction. In real-time, it provides more accurate and precise data, offers early detection of network attacks, and reduces the likelihood that intruders can delete evidence after the attack. However, in terms of detecting attack patterns and attack patterns, this increases overhead processing and storage.

(2) Reactive Network Forensic

To investigate an attack after it has occurred is a postmortem method. To ascertain the root cause of the attack, correlate the attacker to the attack, mitigate the impact of the attack, and investigate the malicious incident with reduced processing, it examines network vulnerabilities by detecting, storing, gathering, and analyzing digital evidence collected from the network.

Figure 3 presents the taxonomic structure of the network forensics as it is presented in [12]. The figure illustrates that network forensics is subdivided into two branches namely investigation mode and data processing. The Investigation mode divides the network forensic into online and offline network forensic. The data processing mode divides the network forensics into two sub-branches: centralized and distributed network forensics.

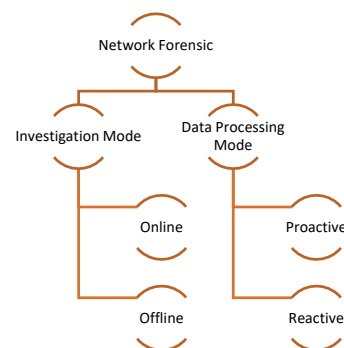


Figure 3. Taxonomy of network forensics based on [12].

2.2. Relationship of Network and Cloud Forensic

As we know, cloud computing is changing the business to increase the value of work and decrease the production cost [13]. These days, cloud computing is becoming the most promising technology, instead of providing local servers or personal computers to manage applications with a simple, on-demand use of computing resources, it relies on shared computing resources. These available services are delivered by utilizing minimal management effort and with the least interaction with the service provider [14]. The purpose of cloud computing is to migrate all computational related resources which include the storage, the network, and the requirements of the service to a platform which is service-oriented through virtual machines located at different data center [3]. It moves applications and databases to large data centers where it is not safe to outsource sensitive data and resources. This poses various threats to security and attacks on the cloud [2]. Nevertheless, the significance of networks in cloud computing has a great impact on “on-demand” resource allocation but its openness and provisioning have opened doors for intruders to attack cloud networks through malicious attacks. Hence, for network security, an efficient investi-

gation process is needed to monitor and analyze the network to detect the root cause of these attacks [13].

2.3. Cloud Security

If security practices are properly applied in clouds, they can provide proof that can justify the forensic method. The architectures that integrate various levels of security concerns include public, private, hybrid, and community cloud. The level of cloud security is a function of the level of confidence in all above-mentioned architectures that can be put in partnership with third parties (CSP) and how far the company has incorporated the cloud framework into its system architecture based on (SLA) [15].

2.3.1. Cloud Forensic

Digital forensics is an implementation of scientific concepts, practices, and procedures through the detection, compilation, storage, analysis, and reporting of digital evidence to reorganize incidents [2]. Although forensic science related to cloud computing is an application of scientific concepts and technical practices, derived and proven methods to recreate past cloud computing incidents [10]. Therefore, cloud forensics is a subset of network forensics and an application of digital forensic science in a cloud environment [16]. Evidence can exist anywhere in the cloud. However, finding the traces on the cloud server is more complicated [2].

Cloud forensic is conducted through the stepwise stages of identification, data collection, preservation, examination, interpretation, and reporting of digital evidence [17,18]. Cloud forensics is considered as one of the most significant fields in the evolving world of cloud computing. In paper [19], the issues of cloud forensics and challenges were identified in detail. In a similar paper [20], the authors discuss the overview of the challenges in the field of cloud forensics and provide suggestive solutions. Cloud computing and its architecture effects are always huge and challenging for the network forensic team. Besides the significant advantages of cloud architecture, security in clouds is always a big concern for the forensic team or the investigating team [10].

2.3.2. Categories of Cloud Forensic

(Investigation Mode and Cloud Infrastructure Mode Classification)

There are three categories of network forensic: the first one is a dynamic cloud, the second one is static cloud forensic, and the third is remote cloud forensic [15]. These three types of investigation mode-based cloud forensic depend on the time of the investigation.

(A) Dynamic Cloud Forensic

The analysis of cloud forensics often allows the device to be alive during the process to discover new data to retrieve valuable sources of evidence, such as open network links, memory dumps, and running processes. The dynamic mode is known as this type of investigation mode.

(B) Static Cloud Forensic

Based on the inquiry timeline, the conventional investigative approach conducted after defining the attack in the cloud is the static mode. IoT data has already been compromised or removed because of the attack. Using universal serial bus and scanning cache memory, static mode recovers data, among others.

(C) Remote Cloud Forensic

This type of forensic usually deals with the remote access forensic based on the legal agreements and based on the mutual contract.

There are two categories of cloud forensic based on Cloud Infrastructure Mode (dynamic cloud forensic), the first one is in-cloud forensic, and another is outside-cloud forensic.

In paper [8], the authors have provided a taxonomy of cloud forensic. According to them, the resource-driven cloud forensic category is a type of cloud forensics, which deals with forensic methods of individual cloud resources like a virtual machine, storage, and network forensic. Although network forensics is used for network security diagnosis in a

cloud computing environment and is further divided into cloud network forensic with its two important implementations as In-cloud and Outside-cloud network forensics. Besides the above two mentioned categories of cloud forensic, the paper [15] has also mentioned some of the other new categories like remote cloud forensic and live system forensic and also mentioned some of the previously existing categories like (VMF) and (StaaS) Forensics. Therefore, we provided our taxonomy of cloud forensic categories based on [8,15].

(1) In-Cloud Forensic

In-cloud Network forensics includes the network traffic inside the cloud infrastructure, which can be (a private network of the user or the underlying network framework).

(2) Outside-Cloud Forensic

Outside-cloud network forensics involves the forensic outside the cloud infrastructure.

Figure 4 presents the taxonomic structure of cloud forensics as it is presented in [8,15]. The figure illustrates that cloud forensics is subdivided into three branches, namely dynamic forensics, static forensic, and remote forensics. The live forensics (dynamic forensic) is in its turn further decomposed into two sub-branches: In-cloud forensics and Outside-cloud forensics.

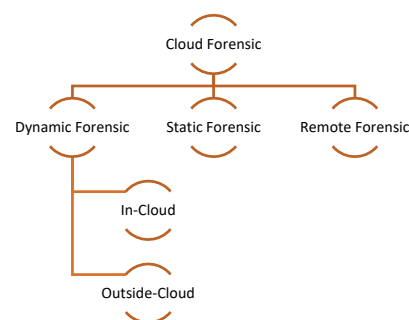


Figure 4. Taxonomy of cloud forensics based on [8,15].

3. Software-Defined Networking (SDN)

Software-defined networking (SDN) is one of the most promising options for network management and a future of next-generation networks (Future Networks). SDN possesses an intelligent configuration, better flexibility to accommodate innovative networks, and high-performance architecture. The SDN mainly consists of three layers, namely (1) Infrastructure layer, (2) Control layer, and (3) Application layer, which are stacked over each other. The infrastructure layer is the bottom layer dedicated to the data plane. Being at the lowest layer, the infrastructure layer consists of switching devices. The control layer is in the middle layer and is dedicated to performance. The control layer contains a control plane which contains the software-defined network control software. An application layer on the top resides above the control layer. The application layer includes SDN applications that are configured to meet user requirements [21,22].

3.1. SDN Forensic

Determining the root cause and finding the source of SDN-based attacks is a difficult challenge, since the techniques used in conventional networks to obtain attack evidence are not adequate when we deal with forensic of SDN attacks [23]. Each layer of SDN has its security implications and specifications because security is not initially considered as part of the SDN design. Additionally, it is even more important to build trust across an SDN [24]. In paper [25], a discussion on possible threats associated with each layer of the SDN architecture and the role of the discovery of topology in the traditional network and SDN are highlighted. A thematic taxonomy of topology discovery in SDN and insights into the potential threats to topology discovery and its state-of-the-art SDN solutions are presented.

SDN forensic solutions in general will provide a reasonable solution to network and cloud security. The utilization of SDN in network and cloud forensic are worth studying for efficient networks and cloud.

3.2. Security Approaches for SDN

3.2.1. Content Inspection

To inspect the contents of each packet of data on a network is known as content inspection. Using IDS, a content inspection can be enhanced through flow level security and deep packet inspection. As SDN enables flow-level security for the network security systems, the flow of data is analyzed during the content inspection, and selected packets are then used for the content inspection. In IDSs and IPS, flow-based content inspection processes allow cost-effective (DPI). The (ID/PS) task is to track the networks' running status in compliance with security policies. They detect attacks/threats, introduce countermeasures to protect the network from any potential threats in the future [26]. The role of an (IDS/IPS) is to stop or allow packets based on a thorough packet survey using pattern recognition, data mining or signature matching with an established threat inventory. In real-time, the SDN IDS can use a huge amount of flow-based knowledge. In [27], the author has mentioned many referenced papers related to the IDS integration with classical tools, SDN IDS/IPS implementation, and applications.

3.2.2. Traffic Monitoring and Auditing

Traffic monitoring and auditing is another feature of SDN-based devices. Besides other fundamental network management tasks of SDN, network traffic monitoring promotes anomaly detection, network forensic analysis, and user application identification [1]. Monitoring and auditing are very important instruments for certain security tests when we talk about forensics. The amount of data that can be obtained at the flow and even packet level is directly linked to a major opportunity in SDN networks [27]. In the same paper [27], the authors have mentioned many referenced papers related to traffic management tools and traffic management platforms.

Besides the above-mentioned security approaches for SDN, there are other security approaches which are also used in various cases, which include Flow Sampling, Access Control, Network Resilience, Security of Middle-Boxes, and Security-Defined Networking.

3.3. Software-Defined Networking (SDN) for Network Forensic

3.3.1. Advantages of Using SDN in Network Forensic

The SDN promises enhanced configuration, improved performance, and encouraged innovation. A general service offered by the SDN is to provide a simple forum for centralizing, integrating, testing configurations, and adding policies to ensure that the implementation meets the security protection (proactively preventing security breaches). In SDN, the control plane is logically centralized. It enables network forensics, security policy modification, and security service insertion. Its architecture supports highly reactive security monitoring, review, and response systems [26]. Additionally, SDN provides better ways to detect and defend attacks reactively also. Simply, we can say that SDN can provide security both proactively and reactively [21].

SDN collects the network status and allows the analysis of traffic patterns and provides programmatic control over traffic flows for potential security threats. For further study, the traffic of interest can be directed straight to intrusion prevention systems. SDN is capable of providing direct and fine-grained network access and offers opportunities and platforms for the introduction of innovative information defense measures against security threats [21]. For network, forensics SDN provides quick and adaptive threat identification to analyze, update the policy and reprogram the network. Moreover, SDN encourages dynamic security policy modification during runtime to specify a security policy to decrease the chances of misconfiguration and policy conflicts. We can simply deploy firewalls and intrusion detection systems (IDS) on specified traffic in compliance with security

policies [26]. When SDN is integrated with in-cloud networks forensic, they provide the best solution for the network forensic [8].

3.3.2. Challenges and Issues of SDN in Network Forensic

The centralized control of SDN draws attackers to exploit various network devices by taking illegal control of the controller by hijacking the controller itself. In the development years of SDN, the security initially was not considered as a key characteristic of SDN architecture, but with time and due to the centralized nature of the SDN, they are vulnerable to various attackers. Therefore, the security of SDN is given more priority. In the newly evolving SDN architecture, investigating attacks is a tiring and demanding task [28]. Eventually, SDN seems to be the most intriguing development platform for future networks. SDN still faces many challenges and problems, despite its impressive advantages, particularly when it comes to a network security problem. The goal of SDN network measurement is to understand and quantify different aspects of network activity to promote network management, monitor the anomalies and the development of security mechanisms, and network troubleshooting [22].

Hence, despite various benefits and the number of resources and facilities provided by the SDN paradigm, there is always a threat that can break the security breaches and hindered the security [4]. There are different levels in an SDN architecture where a security threat may arise. First, at a data plane in the infrastructure layer, which will cover the network appliances and covers the middleboxes. Second, at a control plane in the control layer and the last one is at the application layer [21,26]. Because of SDN's intelligence, the control plane attack will interrupt the entire network and the centralized design will offer and encourage hackers by providing them the chance to discover security weaknesses in the controller itself and take over the entire network [21]. The separation of the planes (control plane and the data plane) and forwarding the control plane functionality to a centralized system (e.g., OpenFlow controller) can create a strong foundation for future networks. However, it also opens a new security challenge, which cannot be easily handled by the traditional forensic tools. The SDN controller can easily become a single point of failure and will leave the whole network down in case of a security compromise [26].

The measurement of the network is seen as a fundamental technique to defend the SDN against major security threats (like OpenFlow protocol loopholes such as deficiency of communication verification, architecture defect, single controller problem, and network resources constraint [22]). SDN can bring various security problems, e.g., unauthorized data modification, controller hijacking, and a black hole issue. These challenges cannot be fixed by using the traditional firewall or IDS-based solutions [29]. The SDN security challenges can be classified into two types: (1), hardware-based and (2), protocol-based challenges. The protocol-based challenges are handled by the network measurement which provides the way for network security [22].

SDN allows applications to communicate with the control plane to access network resources, add new functionality, and exploit network activity that can cause security threats. Additionally, shielding the network from malicious applications or irregular application activity is another significant SDN security problem [26]. In SDN, a centralized controller is responsible for controlling the entire network, and the entire network can be distracted by some form of a security breach in the controller. Furthermore, the security lapses in the communication of controller data paths may provide intruders with access to and use of network resources [26].

Besides the best advantages of using the SDN, many fundamental issues of networking security remain unsolved [22]. In [26], the authors had classified different types of threats related to each SDN plane or layer. The paper also elaborates on the network security in general for the SDN and each level in depth. In Figure 5, we have highlighted the challenges and issues of SDN in Network Forensic.



Figure 5. Challenges and issues of SDN in Network Forensic.

3.3.3. Future Research Directions of SDN in Network Forensic

SDN security is considered in several application contexts, including wireless communications. The application-controller communication and the security for the control channel between the controller and the network devices in SDN is an important area of security where a lot of research needs to be done. Likewise, the trust among all the network devices and the applications is one more related topic of security where researchers should focus on. Another extension related to security is the concern for the standardized framework, vulnerability analysis, mitigation studies in SDN architectures for the controller-switch and their communication. A lot of research is being done to consider and evaluate the feasibility of finger-printing attacks and (DoS) attack on the controller through exploiting flow tables of data plane elements and control channels. Control-data plane and control plane communication is more prone to vulnerabilities and requires substantial hardening to mitigate security threats regarding communication protocol security for infrastructure and software services. Other potential enhancements for network management include attack detection and mitigation by cost-effectively using the SDN framework. Additionally, intrusion detection/prevention systems in networking are the best protection against threats [30]. The use of various security approaches such as contents inspection, traffic monitoring, flow sampling, security middleboxes, etc. when combed with the capabilities of the program, control, and data planes, can protect the entire network [26]. In the same direction, security software may be introduced and used to enforce the security features of the network on top of the control plane. They are used to acquire the network state from the network control plane or to get the resource information from the control plane. Moreover, protection programs are also able to obtain packet samples from the control plane. Security applications can enforce security policies and redirect traffic through the control plane, in compliance with higher security policies. However, in terms of protection, scalability, supportability, and many more, SDN has its complexities and weaknesses. The primary concern for such types of applications is protection [26]. In Figure 6, we have listed the future research directions of SDN in Network Forensic.

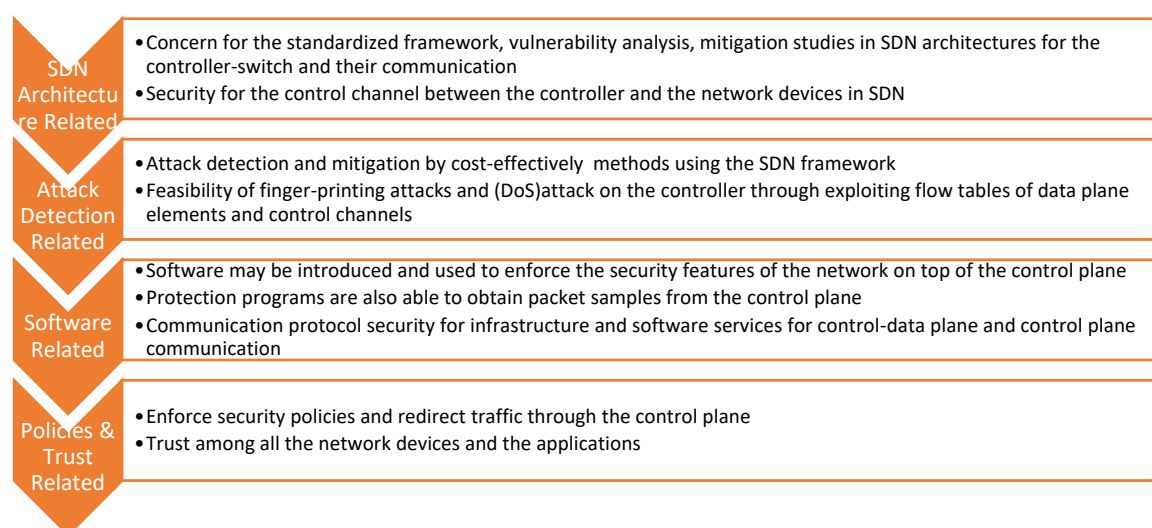


Figure 6. Future Research directions of using SDN in Network Forensic.

3.4. Software-Defined Networking (SDN) for Cloud Forensic

3.4.1. Advantages of Using SDN in Cloud Forensic

SDN is an emerging technology and a centrally located best-based solution to defeat DDoS attacks and TCP SYN flooding attacks. SDN specifically provides centralized control, software-enabled traffic analysis, and a global view of the network. Therefore, they are considered as a perfect tool to enhance the forensic in cloud-based setups [31]. Since cloud computing systems are composed of various shared resources among different users. There are various possibilities that a user can spread malicious traffic on the whole system or access the resources of other users or will consume more resources. Similarly, interactions can cause conflicts in network configurations in multi-tenant cloud networks where tenants run their control logic. However, these problems can be effectively solved, provided the unified view of all the resources using SDN's centralized control plane framework [26].

Applying digital forensics in the cloud environment is labeled as cloud forensics. The main purpose of cloud forensics is to deal with incidents. This involves the forensic of cloud infrastructure and their services for both criminal investigations and civil legal actions [8]. The latest technologies like digital forensics, network forensics, and cloud computing, when integrated for performance, are always best in practice. However, there is always a threat, and these types of integrated systems are always prone to security threats due to their heterogeneous nature. The outcome of cloud computing is the combination of provision computing, network virtualization, charges on usage, and storage resources on demand. SDN in data center networks, usually in cloud computing environments, can fully meet the requirements like the fine-grained control of SDN provides the opportunities to extend the service provisioning beyond storage resources, location independence for dynamic resource provision, scalability for large scale deployment, computing, QoS differentiation for different tenants, and network visibility [21]. Therefore, a need is created which forms the basis for cloud forensic as a strong tool for network-related forensic in clouds. However, due to the distributed nature of the cloud infrastructures, forensic investigators face several challenges, and those challenges are different for different traditional digital forensics types [14].

3.4.2. Challenges and Issues of Using SDN in Cloud Forensic

Due to distributed nature of cloud services, data is mostly residing in multiple legal jurisdictions, leading to an increase in the time of the investigation, cost, difficulty associated with data collection, and analyzing the data remotely for a forensic purpose. The multi-tenancy of many cloud systems is associated with different types of complexity for the forensic including the privacy and the confidentiality of the users, the acquisition

of vast volumes of data, the use of IP anonymity, and the easy-to-use features of many cloud systems are favorable for cloud-based crimes. Similarly, there are other issues for the cloud forensic investigation that include encryption and time of acquisition of data which is dynamic and keeps frequently updating [32]. In paper [33], the author has provided various references which are related to the cloud forensic specifically in context with different aspects of network forensic based on the DFRW Investigative Process, (DIP) Model and the ACPO guidelines. The paper evaluated the different concerns posed in each process of a digital forensic investigation concerning cloud computing, which includes identification, preservation, examination, and presentation phases. The paper also highlighted the distributed nature of cloud control and storage, which makes it more difficult to track activities and recreate incidents during cloud forensic processing. Other problems mentioned in the paper include the loss of essential forensic information such as registry entries, temporary files, and metadata due to the lack of cloud data center investigative resources [33]. In cloud computing, the forensic tools are not much competition and are poor in their performance due to different limitations faced by various (NFIs) including the volatility of the network data, high bandwidth data, heterogeneity, unavailability of cloud networks, network virtualization, fast-moving network data, multi-tenancy, and jurisdiction issues [1]. In paper [8], the author has mentioned many research papers that display the different domains and the different techniques used for controlling the attacks in SDN based on different aspects of digital forensic. In paper [34], the authors discussed the security threats to the SDN by proposing the framework for SDN Forensics. The solutions were divided into three categories: protection for controllers, security for applications, and safety for DoS/DDoS attacks. They set out a set of SDN forensic objectives and criteria and introduced a six-component forensic system, including data collection, extraction, fusion, identification of anomalies, security warning, and conservation of evidence. The shortcoming of the proposed SDN forensic framework is its theoretical conceptual design without any practical implementation. The solution is based solely on SDN architecture security assumptions by putting confidence in both network devices and controllers. The framework lacks implementation and framework evaluation [8].

There are many other technical and related issues for cloud forensic which need utmost consideration for better cloud forensic results in SDN. Some of the technical issues may arise since the cloud server contains various files from many users and the isolation of a particular user file is always burdensome. Some of the other related issues may be linked to jurisdictions-related issues, dependencies on cloud providers, minimum access and control over forensic data, and lack of forensics experts [2]. In Figure 7, we have highlighted the challenges and issues of using SDN in Cloud Forensic.

3.4.3. Future Research Directions of Using SDN in Cloud Forensic

SDN protection is also considered in certain application contexts for the technology to gain wider acceptance in specific avenues, such as in cloud computing [26]. The open research options for cloud related to SDN, which mostly arise and need an utmost consideration before SDNs, are commercially deployed as an efficient cloud forensic tool include the scalability consideration, which directly increases the availability and as more control plane are added, the new addition opens gates for more threats. Therefore, it is important to compare security and scalability in SDN to design stable SDN architectures that ensure the high availability of the control plane rather than will support adding more control planes. The other concern includes the class-based application protection, as it is clear that SDN with its current application trends may generate various security issues by providing direct access to several applications. There are many other correlated open research options of SDN which include control-data planes intelligence trade-off, synchronization of network security and network traffic, programming and development model introduction, identity location split, and network security automation which must be addressed to make SDN more commercial [26].

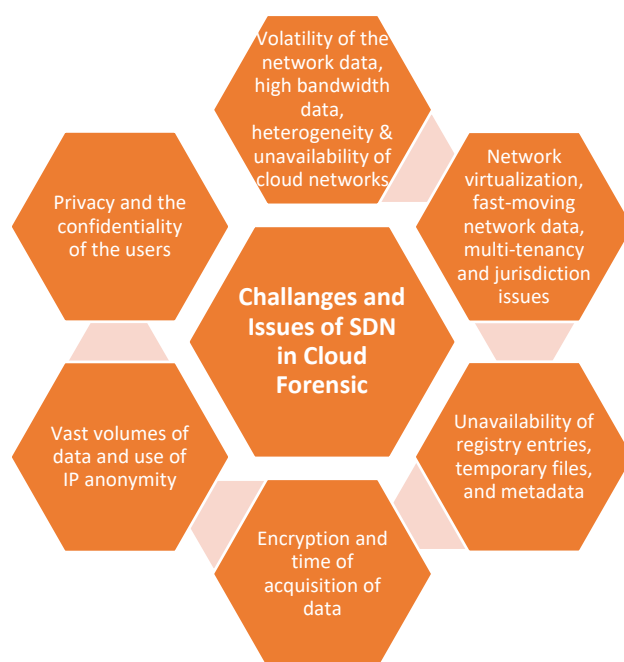


Figure 7. Challenges and issues of using SDN in Cloud Forensic.

Generally, in cloud computing enabled with SDN, additional security may be introduced and applied at each SDN layer to make intracloud and intercloud communication more secure for resource provision. Additionally, data generated from traffic analysis or identification of anomalies in the cloud and its network may often be transferred to the SDN controller for analysis and feedback, thus improving safety. Real-time SDN monitoring must be robust enough to provide timely and efficient identification for cloud forensics of anomalous network events. Not only does the monitoring information provide insight into the traffic but should also stress to focus on storage to satisfy the technical requirements. Finally, there is room for research and concern related to monitoring storage and for subsequent forensic analysis for the SDN [30]. There is also a change for the IDS to get improved for better results in SDN cloud-based platforms, hence the SDN in data centers offers opportunities to researchers for enhancing security [26]. In Figure 8, we have listed the future research directions of using SDN in Cloud Forensic.

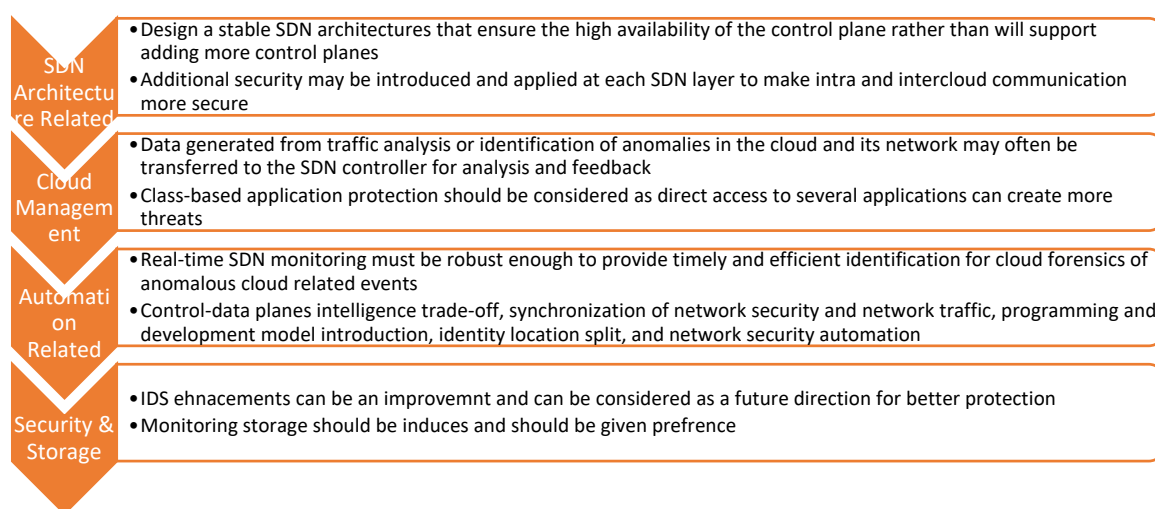


Figure 8. Future Research directions of using SDN in Cloud Forensic.

3.5. Network Forensic Versus Cloud Forensic

Comparison between network forensic and cloud forensic is mentioned in Table 1.

Table 1. Provides the summary of the Network Forensic vs. Cloud Forensic.

	Network Forensic	Cloud Forensic
Brief Description	The Forensic Network is a method for finding and detecting network loopholes and preventing further failures.	In a cloud world, cloud forensics is a branch of network forensics and an extension of digital forensic science.
Key Features	Network forensics focuses on network traffic monitoring and analysis to track, prevent, and diagnose network security incidents.	Incidents are primarily handled by cloud forensics. This covers cloud computing forensics and its services.
Advantages	Security and Enhanced Network Management.	Cloud Security and Cloud protection.
Issues	Because of the enormous amount of network traffic and intensive processing needed for forensic analysis, much of which is unrelated to the available data, which creates problems accessing network and cloud architectures.	Forensic investigators face many challenges due to the dispersed nature of the cloud infrastructures, such as contributing to an increase in the time of the investigation, expense, data collection problems and remote analysis of the data.
Future Directions	It is possible to incorporate advanced networking intrusion detection/prevention systems.	Sophisticated network virtualization, consumption costs, and on-demand storage capacity can be enforced.

4. Discussion

In this research paper, we evaluated network security and forensic and discussed the use of SDN in forensic. As we know, SDN distinguishes the control plane from the data plane, gives the controller the network and resource management characteristics, and is programmable by the user. That adds distinguishing features to SDN like centralized control, the flexibility of flow management, programmability for network application development, and many more. SDN provides better performance, best efficient configuration, and higher flexibility to innovative network designs [21]. A traditional SDN network is vulnerable to various types of anomalies based on the control flow operations (such as symmetric, asymmetric, and intra-controller control flow operations). We ask ourselves a question in our work: using the opportunities of SDN forensic, is there any possibility to enhance the network and cloud security? What can be improved and what can we do better [3]?

Recommendations

We recommend designing the below-mentioned security-related primitives to be considered for a better and efficient network and cloud-based forensic.

- To prevent disruption and protection compromises, SDN security reference models and approaches based on protecting network entities should be introduced.
- Using the control channel, traffic tracking of the application-controller and identification of irregularities in particular avenues, such as cloud setups can be implemented.
- Various methods and tools should be implemented to provide strong security in different forensic process stages.
- Different techniques should be used to provide strong security at different layers of SDN.

- It is possible to store and retrieve network/state data for post-event and forensic analysis for efficiency.
- Developing frameworks for the cloud forensic having ease to detect the attacks.
- Enhance the security, content inspection, traffic monitoring, auditing, and attack detection in cloud forensic.
- Creating enhanced Intrusion detection systems and improve their utilization in SDN.

These set of recommendations are provided to forward the researchers to develop efficient SDN based network and cloud forensic platforms. Figure 9 provides a pictorial overview of the suggested recommendations for Software-Defined Network (SDN) Forensic in context with Network Forensic (NF) and Cloud Forensic (CF).



Figure 9. Suggested Recommendations.

5. Conclusions

Detecting attack attempts for securing the networks by using forensic analysis is very important for the smooth running of the data on a cloud and to save the network and the cloud from future threats. Security has always remained an issue when we are talking about the networks in the cloud. Detecting fundamental anomalous patterns in a network is considered an improvement to enhance the security of the clouds. Additionally, a network forensic is an investigation to find the source of the attack to avoid any attacks/security threats. The SDN promises enhanced configuration, improved performance, and encouraged innovation. Hence, security and forensic in SDN is considered as the best option to secure the future networks. By using the centralized concept of SDN, the security in cloud networks can be enhanced but the centralized control concept of SDN draws attackers to breach and attack the cloud. So, we need to do develop more strong techniques to enhance the forensic in SDN in cloud-based networks. This important diversion of forensic in SDN will help the clouds to be more secure and will help in securing the networks using SDN. This paper surveys the state-of-the-art contribution such SDN forensic. Additionally, comparison with other survey works on SDN, new information about the controller, details about OpenFlow architecture, configuration, comprehensive contribution about SDN security threat and countermeasures, SDN in network forensic and cloud forensic. Also, future direction of SDN security solutions is discussed in detail.

In future, on top of the current SDN layers, additional security layers may be applied. Even, to incorporate more traffic filtering granularities specific to heterogeneous networks,

such as wireless environments, an agent can be added in data plane components. Moreover, additional protection can be enforced on each SDN layer in SDN-enabled cloud computing, depending on the underlying operational requirements to make intra- and intercloud communication less insecure.

Our focus in future work is to present various case studies of SDN forensics, which will expand the concept of SDN forensics and will strengthen the approaches along with improvements in the latest techniques for a real-time implementation of SDN forensic in today's world. The implementation will involve and will cover up many applications and other related technologies such as cloud computing and blockchain. The motivation for our future work will be based on the concepts utilized in [35–37].

Author Contributions: The authors of this article have contributed to this research paper as follows: Writing and preparation, Q.W.; Review and visualization, S.S.A., K.N., W.I.S.W.D. and A.S.A.; Editing and revision, Q.W. All authors have read and agreed to the published version of the manuscript.

Funding: Taif University Researchers supporting Project number (TURSP-2020/215), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Abbreviation	Full forms
CF	Cloud forensic
CS	Cloud security
CSP	Cloud service provider
DDoS	Distributed denial of service
DPI	Deep packet inspection
DoS	Denial of service
DPI	Deep packet inspection
NFI	Network forensics investigator
IaaS	Infrastructure as a service
ID	Intrusion detection
IDS	Intrusion detection systems
IPS	Intrusion prevention systems
NF	Network forensic
NS	Network security
PaaS	Platform as a service
PS	Protection systems
SaaS	Software as a service
SDN	Software defined networking
SLA	Service level agreement
StaaS	Storage as a service
QoS	Quality of service
VMF	Virtual machine forensics

References

1. Harbawi, M.; Varol, A. An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017; pp. 1–6.
2. Sree, T.R.; Bhanu, S.M.S. Data Collection Techniques for Forensic Investigation in Cloud. *Digit. Forensic Sci.* 2020. [\[CrossRef\]](#)
3. Belyaev, M.; Gaivoronski, S. Towards load balancing in SDN-networks during DDoS-attacks. In Proceedings of the 2014 International Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), Moscow, Russia, 28–29 October 2014; pp. 1–6.

4. Celdrán, A.H.; Gil Pérez, M.; Clemente, F.J.G.; Pérez, G.M. Policy-Based Management for Green Mobile Networks through Software-Defined Networking. *Mob. Netw. Appl.* **2016**, *24*, 657–666. [\[CrossRef\]](#)
5. Divakaran, D.M.; Fok, K.W.; Nevat, I.; Thing, V.L. Evidence gathering for network security and forensics. *Digit. Investig.* **2017**, *20*, S56–S65. [\[CrossRef\]](#)
6. Shrivastava, G. Network forensics: Methodical literature review. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 2203–2208.
7. Pilli, E.; Ramesh, S.; Joshi, C.; Niyogi, R. Network forensic frameworks: Survey and research challenges. *Digit. Investig.* **2010**, *7*, 14–27. [\[CrossRef\]](#)
8. Manral, B.; Somani, G.; Choo, K.-K.R.; Conti, M.; Gaur, M.S. A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. *ACM Comput. Surv.* **2020**, *52*, 1–38. [\[CrossRef\]](#)
9. Koroniotis, N.; Moustafa, N.; Sitnikova, E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Futur. Gener. Comput. Syst.* **2020**, *110*, 91–106. [\[CrossRef\]](#)
10. Desai, P.; Solanki, M.; Gadhwal, A.; Shah, A.; Patel, P. Challenges and Proposed Solutions for Cloud Forensic. *Int. J. Eng. Res. Appl.* **2015**, *1*, 37–42.
11. Gebhardt, T.; Reiser, H.P. Network forensics for cloud computing. In *IFIP International Conference on Distributed Applications and Interoperable Systems*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 29–42.
12. Khan, S.; Gani, A.; Wahab, A.W.A.; Shiraz, M.; Ahmad, I. Network forensics: Review, taxonomy, and open challenges. *J. Netw. Comput. Appl.* **2016**, *66*, 214–235. [\[CrossRef\]](#)
13. Rittinghouse, J.; Ransome, J.F. *Cloud Computing: Implementation, Management, And Security*; CRC Press: Boca Raton, FL, USA, 2016.
14. Rani, D.R.; Sravani, P.L. Challenges of Digital Forensics in Cloud Computing Environment. *Indian J. Sci. Technol.* **2016**, *9*, 90–100. [\[CrossRef\]](#)
15. Farina, J.; Scanlon, M.; Le-Khac, N.-A.; Kechadi, M.T. Overview of the Forensic Investigation of Cloud Services. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 24–27 August 2015; pp. 556–565.
16. Alex, M.E.; Kishore, R. Forensics framework for cloud computing. *Comput. Electr. Eng.* **2017**, *60*, 193–205. [\[CrossRef\]](#)
17. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit. Investig.* **2013**, *10*, 34–43. [\[CrossRef\]](#)
18. Khan, S.; Gani, A.; Wahab, A.W.A.; Iqbal, S.; Abdelaziz, A.; Mahdi, O.A.; Abdallaahmed, A.I.; Shiraz, M.; Al-Mayouf, Y.R.B.; Khan, Z.; et al. Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis. *IEEE Access* **2016**, *4*, 9800–9820. [\[CrossRef\]](#)
19. Simou, S.; Simou, S.; Kalloniatis, C.; Kalloniatis, C.; Kavakli, E.; Kavakli, E.; Gritzalis, S.; Gritzalis, S. Cloud forensics: Identifying the major issues and challenges. In *International Conference on Advanced Information Systems Engineering*; Springer: Cham, Switzerland, 2014; pp. 271–284.
20. Mohiddin, S.K.; Yalavarthi, S.B.; Sharmila, S.A. A complete ontological survey of cloud forensic in the area of cloud computing. In *Proceedings of Sixth International Conference on Soft Computing for Problem Solving*; Springer: Singapore, 2017; pp. 38–47.
21. Blenk, A.; Basta, A.; Reisslein, M.; Kellerer, W. Survey on Network Virtualization Hypervisors for Software Defined Networking. *IEEE Commun. Surv. Tutorials* **2015**, *18*, 655–685. [\[CrossRef\]](#)
22. Zhang, H.; Cai, Z.; Liu, Q.; Xiao, Q.; Li, Y.; Cheang, C.F. A Survey on Security-Aware Measurement in SDN. *Secur. Commun. Networks* **2018**, *2018*, 1–14. [\[CrossRef\]](#)
23. Chica, J.C.C.; Imbachi, J.C.; Vega, J.F.B. Security in SDN: A Comprehensive Survey. *J. Netw. Comput. Appl.* **2020**, *159*, 102595. [\[CrossRef\]](#)
24. Akhunzada, A.; Ahmed, E.; Gani, A.; Khan, M.K.; Imran, M.; Guizani, S. Securing software defined networks: Taxonomy, requirements, and open issues. *IEEE Commun. Mag.* **2015**, *53*, 36–44. [\[CrossRef\]](#)
25. Khan, S.; Gani, A.; Wahab, A.W.A.; Guizani, M.; Khan, M.K. Topology Discovery in Software Defined Networks: Threats, Taxonomy, and State-of-the-Art. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 303–324. [\[CrossRef\]](#)
26. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A. Security in Software Defined Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2317–2346. [\[CrossRef\]](#)
27. Alsmadi, I.; Xu, D. Security of Software Defined Networks: A survey. *Comput. Secur.* **2015**, *53*, 79–108. [\[CrossRef\]](#)
28. Khan, S.; Gani, A.; Wahab, A.W.A.; Abdelaziz, A.; Ko, K.; Khan, M.K.; Guizani, M. Software-Defined Network Forensics: Motivation, Potential Locations, Requirements, and Challenges. *IEEE Netw.* **2016**, *30*, 6–13. [\[CrossRef\]](#)
29. Cheng, H.; Liu, J.; Mao, J.; Wang, M.; Chen, J.; Bian, J. A Compatible OpenFlow Platform for Enabling Security Enhancement in SDN. *Secur. Commun. Netw.* **2018**, *2018*, 1–20. [\[CrossRef\]](#)
30. Bakhshi, T. State of the Art and Recent Research Advances in Software Defined Networking. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 1–35. [\[CrossRef\]](#)
31. An, Q.; Yu, F.R.; Gong, Q.; Li, J. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 602–622.
32. Lillis, D.; Becker, B.; O’Sullivan, T.; Scanlon, M. Current challenges and future research areas for digital forensic investigation. *arXiv* **2016**, arXiv:1604.03850. Available online: <https://arxiv.org/pdf/1604.03850v1.pdf> (accessed on 23 April 2021).
33. Grispos, G.; Storer, T.; Glisson, W.B. Calm before the storm: The challenges of cloud computing in digital forensics. *Int. J. Digit. Crime Forensics* **2012**, *4*, 28–48. [\[CrossRef\]](#)

34. Zhang, S.-H.; Meng, X.-X.; Wang, L.-H. SDNForensics: A comprehensive forensics framework for software defined network. In *International Conference on Computer Networks and Communication Technology (CNCT 2016)*; Atlantis Press: Paris, France, 2016; pp. 92–99.
35. Li, M.; Lalb, C.; Contic, M.; Hua, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Futur. Gener. Comput. Syst.* **2021**, *115*, 406–420. [[CrossRef](#)]
36. Pourvahab, M.; Ekbatanifard, G. Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology. *IEEE Access* **2019**, *7*, 153349–153364. [[CrossRef](#)]
37. Park, J.H.; Park, J.H. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* **2017**, *9*, 164. [[CrossRef](#)]