Computer Communications 161 (2020) 304–323

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A taxonomy of blockchain-enabled softwarization for secure UAV network

Aparna Kumari [a], Rajesh Gupta [a], Sudeep Tanwar [a], Neeraj Kumar [b,c,d,*]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[b] Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India
[c] Department of Computer Science and Information Engineering, Asia University, Taiwan
[d] Department of Computer Science, King Abdul Aziz University, Jeddah, Saudi Arabia

ARTICLE INFO

Keywords:
Unmanned aerial vehicle
Softwarization
5G
Software defined networking
Network function virtualization
Blockchain
Smart contract
Security

ABSTRACT

The recent advancements in unmanned aerial vehicles (UAVs) upsurges its usages in commercial and civilian applications such as surveillance, rescue, and crowdsensing. UAVs are vulnerable to being destroyed, lost, or stolen in case of security breaches of its network. The network management of UAVs is a crucial task due to its high mobility, which necessitates UAV network softwarization. Then, it becomes indispensable that allows the separation of control functions (i.e., control plane data) from hardware for smooth execution of complex operations. Further, UAV uses the Internet (an open channel) for communication in its complex system that raises a network security concern. The well-known softwarization techniques, i.e., software-defined networking (SDN) and network function virtualization (NFV) can be used to accomplish the secure network services on less expense. Conversely, these softwarization techniques may suffer from various threats like access control, user authentication, controller hijacking, and many more attack. The existing solutions are using a centralized system, which is having a single point of failure issue and vulnerable to security threats. Motivated from these facts, we present a comprehensive and systematic survey on the blockchain-based softwarization for a secure UAV network. Then, we propose a blockchain-enabled UAV softwarization architecture for secure communication and network management. It provides dynamic, flexible, and on-the-fly decision capabilities for communication services over the UAV network. Eventually, we analyzed the open research issues and challenges for future research directions in this emerging area.

1. Introduction

The continuous advancements in information and communication technology (ICT) tools and techniques increase the quality of service (QoS) and quality of experience (QoE) of Internet of things (IoT) applications such as smart healthcare [1], intelligent transport system (ITS), border surveillance, drone package delivery, and search & rescue. The vision of IoT is to make everything smart and accessible with low capital and operational expenditures. So, the unmanned aerial vehicles (UAVs) are the key drivers of the smart society, which offers various cost-effective services like surveillance, package delivery, healthcare [2], and traffic management. UAVs were first designed and used for military operations during the second world war and later it was used in diverse civil applications as mentioned above. It offers easy and fast deployment of user's applications with smooth execution. Due to the aforementioned benefits of UAVs, they have been widely used across the globe following their respective country laws and regulations.

As per the report of Federation of Indian Chambers of Commerce and Industry (FICCI), the adaptability of UAVs in India is expected to *885.7 million USD* by 2021 and globally to *21.47 billion USD* [3]. Despite easy deployment, the other reasons behind the adaptability of UAVs in the following application areas such as (i) security and surveillance, (ii) environmental studies and monitoring, (iii) entertainment, and (iv) infrastructure and engineering [4]. One of the crucial enabling technologies for UAVs is the wireless communication. The network functions (NF) such as routing, switching, bandwidth allocation, and load balancing are coupled with the network devices itself, i.e., each device has a memory and processor that helps to take dynamic network-related decisions [5]. Any modification in the NFs raises high maintenance costs because of the following reasons.

- The NF of each network hardware device (router, switch, and access points) needs to modify separately, i.e., a number of modifications are always greater than or equal to the number of network devices.
- It temporarily shut down the entire network during maintenance of the network hardware devices (change in functionalities of the NFs).

* Corresponding author at: Department of Computer Science and Information Engineering, Asia University, Taiwan.
E-mail addresses: 18ftphde22@nirmauni.ac.in (A. Kumari), 18ftvphde31@nirmauni.ac.in (R. Gupta), sudeep.tanwar@nirmauni.ac.in (S. Tanwar), neeraj.kumar@thapar.edu (N. Kumar).

https://doi.org/10.1016/j.comcom.2020.07.042
Received 16 May 2020; Received in revised form 2 July 2020; Accepted 28 July 2020
Available online 6 August 2020

- Reduced human efforts needed to update the NFs of all the network devices.

It is challenging for UAV system developers to maintain and control the UAV network. It is because of high mobility, fitful connectivity, dynamic network topology, and high operational expenditures cost associated with software integrated devices [6]. It also reduces the UAV network system's reliability. The aforementioned issues associated with the UAV network can be eliminated using a network softwarization (NS) technique. It decouples and provides the softwarization of NFs, which are associated with the UAVs and network hardware devices. The recent 5G technologies such as software-defined networking (SDN) and network function virtualization (NFV), are the enablers for softwarization [7]. SDN allows network programmability by separating the control plane from user plane (also called forwarding plane) using the open-source interfaces such as OpenFlow (OF) [8] and OpenDaylight (ODL) [9] over southbound application programming interfaces (APIs). The centralized control plane populates the flow table to manage the routing and switching of UAV data packets at the data plane.

However, NFV allows the virtualization of NFs that shares the physical resources such as compute, storage, and networking to scale the network services of the UAV system without any additional hardware cost. Containers in the NFV system helps to create the multiple instances of NFs within a single virtual machine based on the network demand [10]. Softwarization is appropriate for UAV network management where the location of UAV is temporary and the connectivity is intermittent. As per the above discussion, NS offers many benefits to the UAV network, the other benefits are as follows: (i) it logically centralizes the UAV network intelligence with programmable NFs, (ii) it allows system developers to modify the UAV NFs and policies through the centralized programming control without making the entire network off, (iii) it provides resilient and cost-effective solutions (NF virtualization without installing any additional hardware devices) for UAVs which is beneficial for mission-critical applications, (iv) it increases the end-user QoS and QoE [11], and (v) it maintains the UAV specific dynamic path information, i.e., from source to destination to accomplish the mission timely.

The aforementioned benefits increase the acceptability of UAVs by many organizations worldwide, but still, its security remains the common agenda. Security of UAV is utmost importance as it is widely used in various mission-critical applications, which includes border surveillance, battlefield surveillance, and disaster management. Any compromised UAV can disclose the vital information to the intruders and can affect the entire UAV network. For example, in 2011, Iran has captured the US-based RQ-170 drone and take complete control of it in the cyber warfare [12]. Later, in 2013, Hak5 demonstrated the vulnerabilities of UAVs using WiFi sniffer [13]. Then, in 2016, Kamkar designed a Skyjack device for UAV hacking that scans the MAC addresses and takes control of the nearby UAVs [14]. In another incident, a SkuGrabber software was used to hack the Predator drone and exposed its encrypted data [15].

Irrespective of network management, the SDN can also be preferred to settle various security issues for instance clone attack, spoofing attack, jamming attack, intrusion detection, and distributed denial of service (DDoS) attack [15]. For example, Fichera et al. [16], presented an OPERETTA system to be implemented in the controller to mitigate SYN flooding attack. It introduces long delays as the system first validates the TCP source and install the forwarding rules. Then, Mohammadi et al. [17] design a SLICOTS, an SDN-based system to resist SYN flooding attack. They have implemented the system as an extension of the ODL controller under varied attack scenarios and reduces the response time up to 50% compared to the existing state-of-the-art systems. Kreutz et al. [18], build a solution to secure the SDN control plane vulnerabilities to prevent it from Byzantine faults by specifying a threat vector. Lam et al. [19] embedded an identity-based cryptography scheme to secure the communication between SDN data and control planes.

Matsumoto et al. [20] presented an SDN controller design to protect the system availability against the malicious users. Then, Bates et al. [21] designed an SDN-based system to identify faults in the controller network along with the previously unidentified attacks. Later, Lara et al. [22] presented an SDN-based OpenSec framework that allows the design of security policies and regulations which can be tested and validated over GENI testbed. Further, Guerber et al. [23] presented an SDN-based secure architecture to protect UAVs against the specific attacks such as blackhole, wormhole, and DDoS attacks. Then, Sairam et al. [24] presented a system called NETRA, which highlights the importance of NFV in executing security functions in the IoT network. The aforementioned SDN and NFV-based security solutions can suffer from various issues like (a) possibility of DDoS attack on SDN controller that can astray the UAVs from their legitimate paths, (b) the communication between data and control planes can be spoofed with man-in-the-middle (MiM) attack, (c) software compatibility issues in case multiple policies are being installed by many trusted third-party systems, which could compromise the UAV data privacy, and (d) the compromised controller can put down the entire UAV network functionalities.

Blockchain technology is a viable solution to mitigate the aforementioned issues related to the UAV network softwarization [25]. It is a peer-to-peer (P2P) distributed ledger, which gives secure, immutable, transparent, and trustless environment to the UAVs to store their data as a transaction (hash value) in the chain of blocks [26]. Smart contracts (SC) and the consensus mechanisms are the key pillars of the blockchain technology. SC eliminates the need for a trusted third party system to preserve the privacy of data, whereas consensus mechanisms maintain the integrity of data. The security of data in the blockchain is ensured using cryptographic algorithms. These interesting features of blockchain increase the acceptability of UAVs in various civil and mission-critical applications. So, this paper presents a blockchain-enabled UAV softwarization architecture to enhance communication security and privacy. It also ensures the authenticity of SDN controllers and the authorization of virtual machines in the network functions virtualization infrastructure (NFVI) layer of the NFV architecture to protect them against various security attacks (see Table 2).

1.1. Motivation of the survey

Motivation of the survey is as follows.

- UAV NS is the key basis to improve the security of various UAV applications. It also makes network management effortless, resilient, intelligent, and dynamically configurable. It creates interest among the researchers worldwide to explore this field more.
- The existing literature generally emphasis on NFV and SDN-based security in UAV network with less focus on blockchain-based UAV softwarization. Thus, there is a need for a comprehensive survey to explore the blockchain-based UAV softwarization (see Fig. 1).

1.2. Research goals of the study

As per the existing literature, many authors have presented their research work in SDN and NFV-based UAV network management and security, but very few works exist which presented the integration of blockchain UAV NS to enhance the security. To conclude, the key contributions of the survey are as follows.

- We explore the security, privacy, and network management issues in UAV communication and illustrate how softwarization (SDN and NFV) helps to mitigate such issues.
- We present the taxonomy of possible security attacks on the softwarized UAV network management along with their countermeasures.

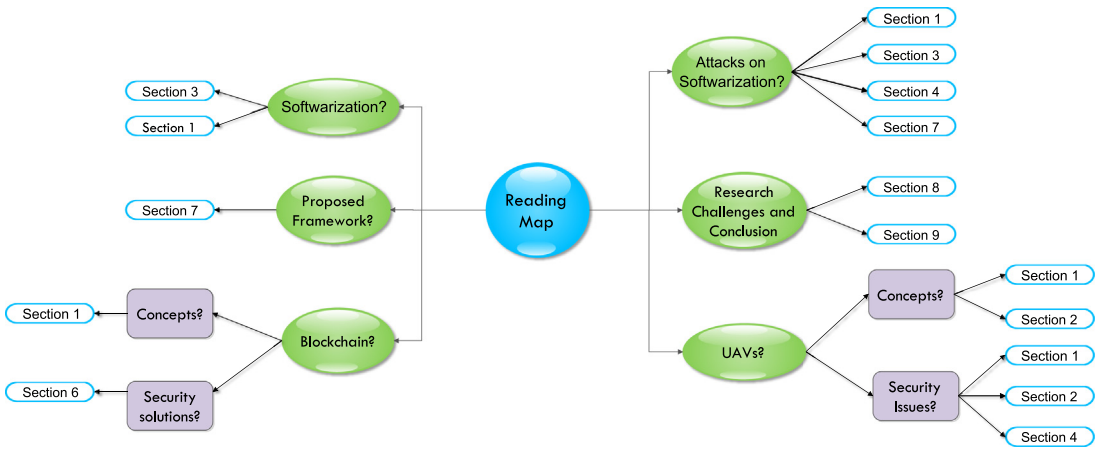


Fig. 1. Reading map of the survey.

Table 1
Nomenclature.

API	Application programming interface
CAPEX	Capital expenditure
CNC	Central Network Control
CPU	Central Processing Unit
DDoS	Distributed denial of service
DoS	Denial of service
DPI	Deep packet inspection
ETSI	European Telecommunications Standards Institute
FICCI	Federation of Indian Chambers of Commerce and Industry
GPS	Global Positioning System
GSMP	General Switch Management Protocol
ICT	Information and communications technology
IoT	Internet of things
ITS	Intelligent transportation system
MDA	Message Digest Algorithm
MiM	MiM Man-in-the-Middle
NBI	Northbound interface
NCF	Network control functions
NF	Network function
NFV	Network function virtualization
NFVI	Network functions virtualization infrastructure
NFVO	NFV orchestrator
NS	Network softwarization
ODL	Open DayLight
OF	OpenFlow
ONF	Open Network Foundation
ONOS	Open Network Operating System
OPEX	OPEX Operational expenditure
OVSDB	OpenvSwitch Database
P2P	Peer-to-peer
PCEP	Path computation element communication protocol
PoS	Proof of stake
PoW	Proof-of-work
QoE	Quality of experience
QoS	Quality of service
SC	Smart contract
SDN	Software defined networking
SHA	Secure Hashing Algorithm
SSH	Secure Socket Shell
sVirt	Secure virtualization
TI	Tactile Internet
UAV	Unmanned aerial vehicle
VIM	Virtual Infrastructure Manager
VNF	Virtualized Network Function
MANO	NFV Management and Orchestration

- We propose a blockchain-based UAV softwarized architecture to enhance the security and privacy of softwarization techniques in UAV communication.
- Finally, we highlight the number of open issues and research challenges in the proposed blockchain-based UAV NS for future research directions.

1.3. Paper organization

The rest of the paper is organized as follows. In Section 2, we discussed the concepts and security issues in UAVs. In Section 3, we explain softwarization techniques such as SDN and NFV. In Section 4, the possible attacks on various softwarization enablers are highlighted. In Section 5, we discussed the various state-of-the-art SDN and NFV-based security solutions. In Section 6, the blockchain technology for the security of UAV softwarization is illustrated. In Section 7, a proposed blockchain-based UAV softwarization architecture is presented. In Section 8, the open issues and research challenges in the proposed system are analyzed, and finally, Section 9 concludes the paper.

Fig. 1 provides a reading map to the readers with interest in SDN, NFV, UAV, blockchain, their security issues, and future directions. Table 1 lists all the acronyms used in the paper.

2. Unmanned aerial vehicles: Concepts and issues

UAV (also known as a drone) is an autonomous aerial vehicle that can fly without a pilot and being controlled by the UAV ground stations, as depicted in Fig. 2. It was first designed in the 1920s to perform military operations and later it was deployed for various civil applications such as traffic management, environmental monitoring, communication relays, healthcare, movie shooting, package delivery and many more. A single UAV comprises of sensors (temperature, gas, location, and ultrasonic), flight controller unit, radar, high definition cameras, actuators, firmware, and the communication channel. Based on the capabilities of these components, the UAVs are classified into two classes, i.e., altitude and size-based UAVs [32].

In altitude-based categorization, the UAVs are classified as high altitude and low altitude UAVs. High altitude UAVs covers the wide geographical area, extended battery life, and costly, whereas the low altitude UAVs are cost-effective, high mobility, fast deployment, and limited battery life. In size-based, the UAVs are classified as small and large UAVs [28]. Small UAVs are light-weight and high-speed aircraft, whereas the large UAVs are heavy-weight and low-speed aircraft. Large UAVs have the capability to hover at one stationary area, but small UAVs cannot. As mentioned above, the widely used in various mission-critical applications, that need a low-latency and reliable communication channel. The 5G-enabled Tactile Internet (5G-TI) is an integral part of the UAV communication that offers ultra-low latency ($< 1ms$), ultra-high reliability (99.999%), and superior connectivity [33].

The deployment of UAVs is increasing at a rapid rate in almost all application areas worldwide. This increases the UAV network management complexity. To deal with this, the 5G-enabled technologies, i.e., SDN and NFV, helps to make the UAV network management robust and easy by decoupling the UAV control plane from the data

Table 2
A comparative analysis of the proposed survey and existing surveys.

Reference	Year	Objective	Merits	Demerits
[5]	2016	Presented the softwarized integrated protocol of UAV and wireless sensor networks using the centralized cloud platform	Improved network management and virtualization of network functions over heterogeneous network	Security concerns in the integration of technologies not considered
[27]	2016	Presented the softwarized integrated protocol of UAV and wireless sensor networks as a part of the centralized cloud platform	Improved network management and virtualization of network resources in the centralized cloud platform	Security issues are not taken into account in the integration of technologies like UAV, WSN, and cloud
[28]	2016	Authors have Presented an exhaustive and comprehensive survey on various security, privacy and network management issues in UAV network	Better network management, security enhancements of UAV network management	Blockchain based enhanced trust and security measures not explored by the authors.
[29]	2017	Authors have designed a flexible cloud or fog, SDN and NFV-based fleet of UAV softwarization network architecture to monitor the rural zones	Easy network management easier with 5G-enabled SDN and NFV technologies	Resource allocation management security is not considered as foremost study
[30]	2018	Network functional Virtualization-based adaptable and automated UAV deployment	Increased scalability of UAV network with virtualized resources such as computing, storage, and network resources	Network function management is bit difficult because of no separation of data and control plane of network hardware devices and Security not guaranteed
[15]	2019	Presented a SDN-based UAV network system for network management and security enhancements	improved network flexibility and visibility for efficient network management. Discussed the security enhancements using SDN	Attack mitigation solutions are explored but rely on centralized system which is having single point failure
[31]	2020	Assessment of UAV applications in SDN environment and their associated security risks	Elaborative security assessment of SDN-based UAV network with attack taxonomy	Not presented any solution architecture to mitigate such attacks and no blockchain concept discussed
Proposed	2020	Presented a blockchain-based decentralized and secure architecture to mitigate cyber-attacks	Enhanced security, efficient network management, improved UAV network scaling, and no single point failure	–

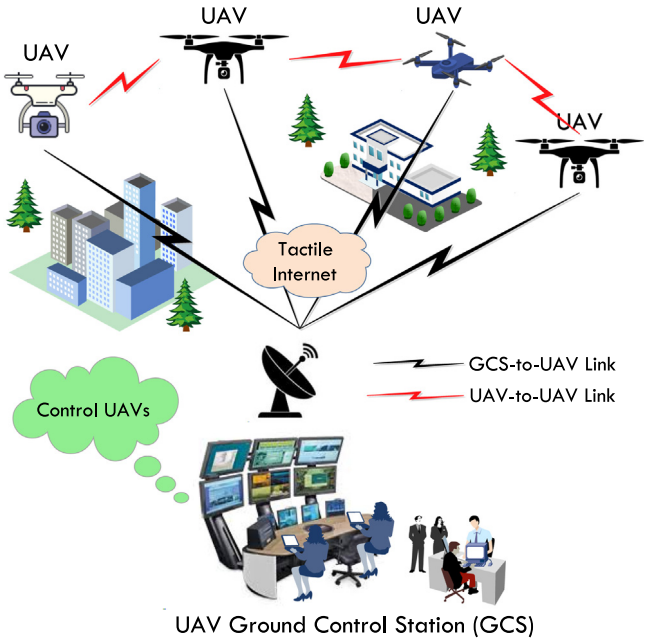


Fig. 2. UAV-Ground control station communication.

or forwarding plane. SDN allows the programming implementation of UAV NFs at the control layer to take real-time dynamic decisions (such as path selection, monitoring, and surveillance) efficiently and increases the scalability of the UAV network. 5G offers an exceptionally wide spectrum for UAV communication, which enables the transfer of an abundant amount of data such as video-feeds, trajectory values, and environmental conditions to the ground control stations with QoS and QoEv [34]. The detail description of the integration of UAVs with SDN and NFV-based softwarization is discussed in Section 7.

UAVs are being controlled by their remote ground stations over the open wireless channel, i.e., the Internet, which is more vulnerable to various security threats [35]. It is mandatory to secure the UAV communication channel, as it may carry sensitive information for mission-critical applications [36]. Various possible cybersecurity attacks on the UAV communication channel are as follows.

2.1. Jamming attack

The purpose of this attack is to suspend the ongoing UAV communication by injecting excessive test packets, packet collisions, or increasing the channel interference or noise [37,38]. It is easy to implement and does not require any knowledge of the victim's system.

2.2. Black hole attack

It is a type of DoS attack, in which the compromised or malicious UAV drops the data packets instead of forwarding it to the next UAV for information sharing [39].

2.3. Gray hole attack

It is a type of attack, in which a malicious UAV agrees to be part of the application network, but later it denies to forward information to either other UAVs or ground control station [40].

2.4. GPS Spoofing attack

In this attack, a compromised UAV sends the false GPS location signals to the target UAVs without disrupting the existing GPS operation, which aims to bind the target UAV with fake latitude and longitude data [41].

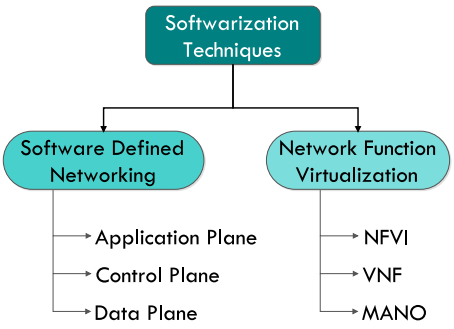


Fig. 3. SDN-NFV architecture components.

2.5. Hijacking attack

The purpose of an attacker is to acquire the complete control of the UAV network and add some delay in data forwarding. This attack can be hazardous for mission-critical and delay-sensitive applications such as healthcare, surveillance, and disaster management.

2.6. False traffic information dissemination

In this attack, a malicious UAV broadcast the false traffic information to the other UAVs in order to force to take falsified decisions [42, 43]. A malicious UAV can broadcast the wrong environmental data to force other UAVs not to come in that area.

2.7. Eavesdropping

In this attack, a malicious UAV listens to the secret communication between the other UAVs and do nothing. It is a kind of passive MiM attack which only listens the data from vulnerable communication links [44].

There exist some challenges that hinder the full adaptability of UAVs. The first challenge is the UAV development and maintenance cost, which is quite high and everyone cannot afford it. The second issue is the regulation and legislation of the UAV in a specific country [45]. Softwarization can be the possible solution to overcome above-mentioned issues in UAVs.

3. Softwarization: Features and working philosophy

This section explains the softwarization technologies, i.e., SDN and NFV, to perform an efficient UAV network management, as shown in Fig. 3. The detailed description of these technologies is as follows.

3.1. SDN-enabled softwarization

It is a technology that offers software-enabled dynamic network configuration and management to improve network monitoring and performance [46]. It logically separates the control plane from the data plane and centralizes the intelligence of the network devices (router, switches, and access points) at the SDN controller to make real-time dynamic decisions [47]. In traditional network, the data packet routing decisions were destination-based (i.e., each router has a routing table and based on that data packet will be forwarded to the next node), instead of flow-based in SDN network (i.e., centralized SDN controller takes the decision in forwarding the data packet to destination) [48]. SDN is a compliment for those applications which require ample-bandwidth, real-time dynamism, faster decisions, and cost-effective solutions [49]. The well explained the definition of SDN is as follows:

> *SDN is the re-factorization of correspondence between the network hardware devices and the software functions that controls them [50].*

Various features of the SDN architecture are programmable, agile, responsive, centrally managed, easily manageable, and vendor-neutral [51]. However, the concept of SDN came into the picture in the around late 1980s and the researchers worldwide are continuously working on its advancements, as shown in Fig. 4. In general, the SDN architecture is bifurcated into three logically separable layers (i) forwarding layer or data plane, (ii) control plane, and (ii) application layer, as shown in Fig. 5(a). The brief description of these layers is as follows.

3.1.1. Data plane

It is also referred to as the forwarding engine or infrastructure layer. It consists of physical networks hardware devices such as routers, switches, and access points that help to forward the data packets from source to destination based on the path specified in the flow table (route to the destination node) received from the central control plane via OpenFlow protocol. If flow arrived at the network devices, a look is performed in the lookup table. If there exists no flow for a data packet in the flow table, then an automatic request will be forwarded to the SDN controller in this regard. Therefore, the controller either creates a new rule (reactive mode) or populates the entries of the flow table (proactive mode) to overcome the aforementioned issue. Along with the NFs, it also centralizes the management of network device policies to make them as vendor-neutral or inter-operable. The nature of devices can be either collocated or dislocated [52]. Collocated devices are the traditional devices where the control functions are embedded in the device itself, whereas the control functions are managed at the central location in the dislocated devices.

The open and vendor-independent interface used to exchange the communication between the control and the data plane is southbound interface. It provides the softwarization of flow operations, error reporting, and notification.

3.1.2. Control plane

It is known as intelligent layer where all decisions related to routing, switching, and access control can be taken here only. SDN controller at this layer manages the network devices at the data plane by creating flow rules for them. The benefit of centralization of NFs is that each controller has a complete view of the network, which helps it to make dynamic decisions efficiently. A single control plane can have multiple controllers to manage heterogeneous networks. Each SDN controller can have more than one northbound interface agents to establish communication between the controller and the application layer.

It has a scalability issue, as the size and dynamism of the network increase with the increase in a diverse number of applications. To overcome the aforementioned issue of scalability, Yaganeh et al. [53] and Ahmed et al. [54] suggested the hierarchical and fully distributed approaches for the SDN controller. The placement of the controller is utmost important in case of large networks to resolve the reliability, latency, and fault-tolerant related issues [55].

3.1.3. Application layer

It presents the end-to-end view of the entire network where the user or business applications resides [56] for instance, military surveillance, healthcare, and intelligent transport system to gain the benefits of available resources. It exchanges the control information with the SDN controller via the northbound interface. Various security risks associated with the different planes of the SDN architecture are mentioned in Section [57] 4.1.

3.2. NFV-enabled softwarization

The concept of NFV was first given and evaluated by the European Telecommunications Standards Institute (ETSI) for its stability and interoperability [58]. NFV is a technique for cost-effective and fast network services and infrastructure (computing, storage, and network

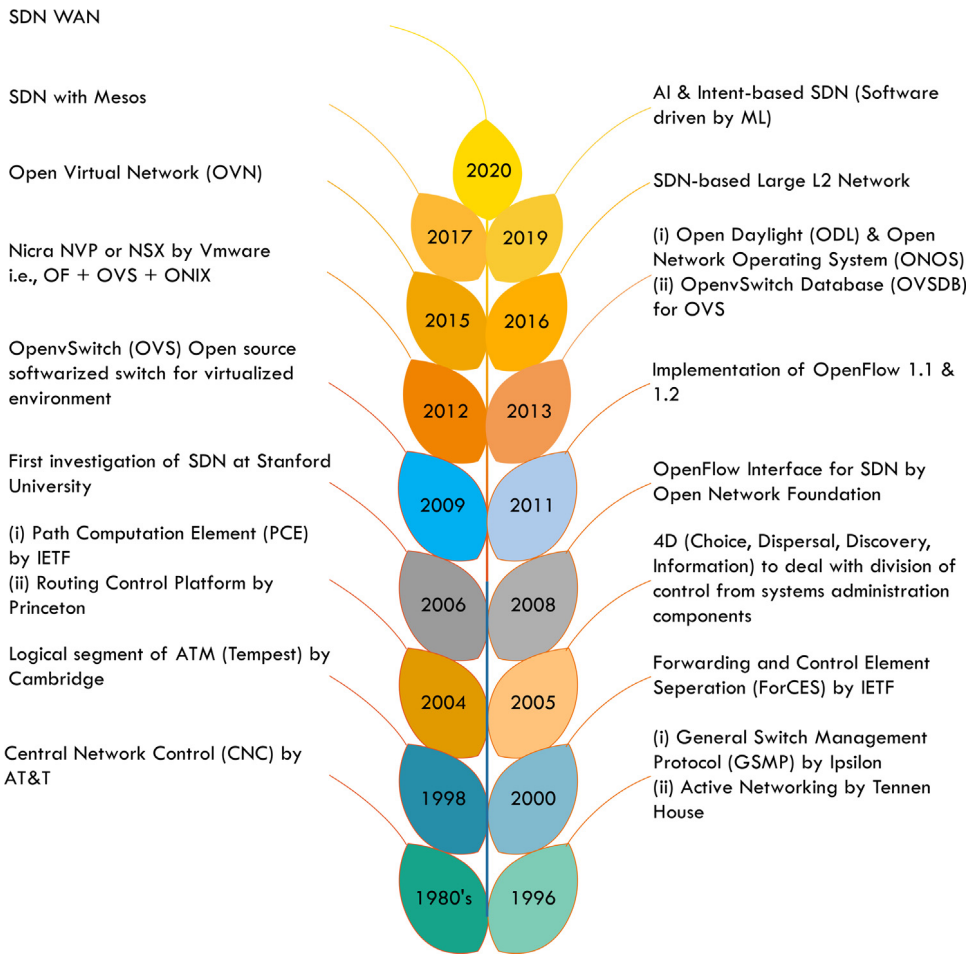
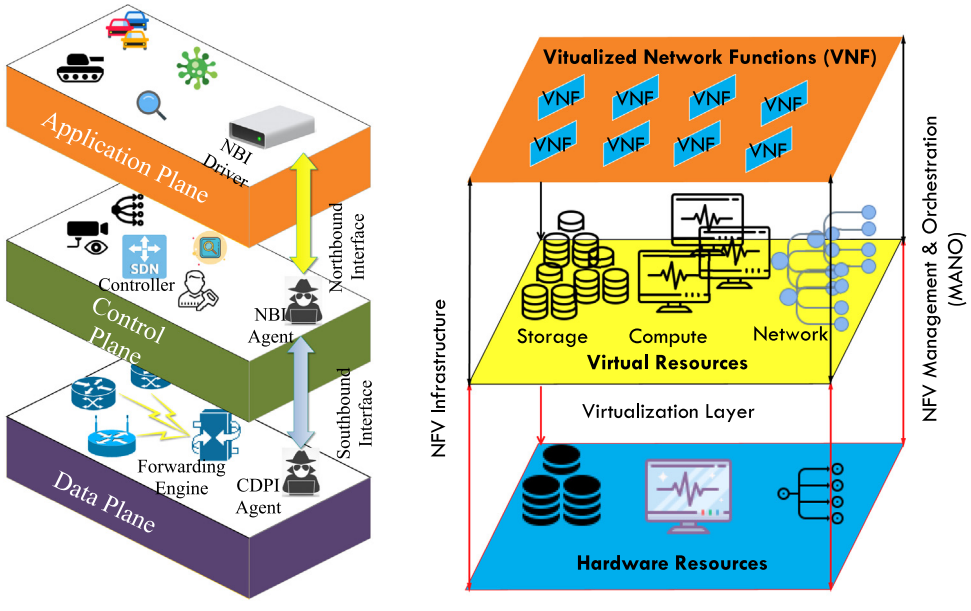


Fig. 4. Year-wise advancements in software-defined networking .



(a) Layered architecture of SDN.

(b) Layered architecture of NFV.

Fig. 5. 5G-enabled softwarization technologies.

devices) deployment for the network operators by separating the NFs such as firewalls or encryption from the network hardware to the virtual machines [59]. It saves the network deployment cost because there is no need to install any dedicated hardware to run the NCFs [60]. If anyone wants to add a new NF, then the network operator simply creates a new virtual machine to perform the NF.

Decoupling NFs from the dedicated network hardware offers many benefits to network operators such as easier network updation, minimize network management cost, minimize network power consumption, and eliminates network hardware cost. The standard NFV architecture comprises three abstraction layers, such as (i) Virtualized network functions (VNFs), (ii) Network functions virtualization infrastructure (NFVI), and (iii) NFV Management and Orchestration (MANO) layers as shown in Fig. 5(b). The detailed functionalities of NFV layers are explained as follows.

3.2.1. NFV infrastructure (NFVI)

It consists of physical as well as virtual network resources such as compute, storage, and network [61]. It offers cost-effective and standardized computing infrastructure, i.e., hardware and software. It spans across the remote locations in lieu of connectivity between the network components. It is managed by the virtual infrastructure manager (VIM) to orchestrate the resource allocations for virtual NFs (VNFs). It is useful to build complex and distributed networks that span across the geographic location.

3.2.2. Virtualized network function (VNF)

VNFs are the network function that reduces the dependency on network hardware devices for executing the network services and operations [59]. It used to connect the NFVI layer virtualized infrastructure to deliver scalable and efficient network services.

3.2.3. NFV management and orchestration (MANO)

It is a key framework designed by the ETSI working group to orchestrate the VNFs in NFV architecture synchronize the network elements through automation and catering of VIM and VNFs. This framework has the following functional areas such as NFV Orchestrator, VNF Manager, and VIM. Orchestrator is responsible for resource validation, authorization, & orchestration, lifecycle management, and network service management, whereas VNF takes care of network deployment, configuration, and event reporting. The VIM component handles the virtualization of NFVI compute, storage, and network resources [61].

4. Threats to UAV softwarization technologies

This section describes the various security and privacy issues on the softwarization technologies such as SDN and NFV in UAV application scenarios.

4.1. Security and privacy issues in SDN-enabled UAV softwarization

SDN is on the verge to replace the traditional centralized UAV network systems due to its ample functionalities to handle system integrity, privacy, confidentiality, and efficiency of the network. SDN is a softwarization technique, which makes the NFs programmable at the control layer and can have many security and privacy-related issues and vulnerabilities. So, this section gives an insight into various security attacks on the SDN-enabled UAV system [64–66]. An illegitimate access to the central SDN controller can cause gigantic damage to the entire UAV network and can also introduce malicious codes into the system. The standard SDN architecture has three different planes as mentioned in Section 3.1. A malicious node can target any plane of the SDN architecture. Though, we have classified the attacks based on the target plane such as data plane, control plane, and application plane as shown in Fig. 6.

4.1.1. Attacks on data plane

- *Man-in-the-Middle Attack*: In SDN architecture, the effective communication between the control and data planes can be established over the southbound interface (an open source interface) using the protocols, i.e., OpenFlow, Cisco onePK, Opflex, and path computation element communication protocol (PCEP). A malicious user can add or update the new routing path in the flow table, which navigates the traffic flow to a different destination.
- *Denial of Service (DoS) Attack*: In this type of attack, a malicious user can get the unauthorized access to the various UAV network devices, for instance, switches, routers, and access points. It can be achieved by sending continuous route flow requests to the SDN controller [67].
- *Replay Attack*: In SDN architecture, the malicious user can gain access to the network resources using a replay of authentication messages. Here, the replay could be launched using the overheard information of traffic flow in the UAV network.
- *Eavesdropping*: In this type of attack, a malicious user overhears the traffic flow among all the layers of the SDN system to recognize or analyze the UAV network behavior. It breaches the privacy of UAV communication architecture.

4.1.2. Attacks on control plane

- *Controller Hijacking Attack*: In SDN architecture, the complete network can be compromised if any attacker confiscates the centralized controller. The controller can be compromised by connecting through switches and routers of the UAV network.
- *Spoofing*: A malicious node over the UAV network can take illegal control on the network to modify the decision-making data, i.e., UAV path selection.
- *Duplicacy*: There is a likelihood that a malicious user can create their own SDN controller to establish the trust between the UAV network elements to make them believe in a malevolent flow table.
- *Time-delay Attack*: In SDN architecture, attackers can attack the resources of the SDN controller to decrease the request–response time from the application or data plane to the control plane.

4.1.3. Attacks on application plane

- *Brute Force Attack*: In this type of attack, a malicious user try various distinguish combinations to crack the password (by guessing it) and take control of the SDN application.
- *Authentication*: In an application plane, the authentication of UAV applications or devices is a major challenge. An attacker can log in to the UAV applications and manipulate the behavior of the network if no compelling authentication mechanism available.
- *Access Control and Accountability*: To ensure the security of the UAV system, the proper access control and accountability approaches are required to get affected by the various conventional attacks such as DOS and replay attack.

4.2. Security and privacy issues in NFV-enabled UAV softwarization

In NFV, all VNFs work on virtual machines (VM) and the security threats related to VNFs are the combinations of the physical networking attacks and the attacks on VM technologies. The NFV specific attack as shown in Fig. 7 materializes when the multiple attacks intersect each other [68]. Here, we confer the potential attacks associated with NFVI, bearing in mind some potential threat scenarios [69,70].

- *VM Escape Attack*: This attack imposes high risk if launched successfully. It is probably due to the improper isolation between and VNFs. In this attack, the attacker hypervisor the VNFs running on the UAV system, which is perhaps due to separation between VNFs and hypervisors. In this attack scenario, the attacker initially compromises any single VNF to admittance to its operating

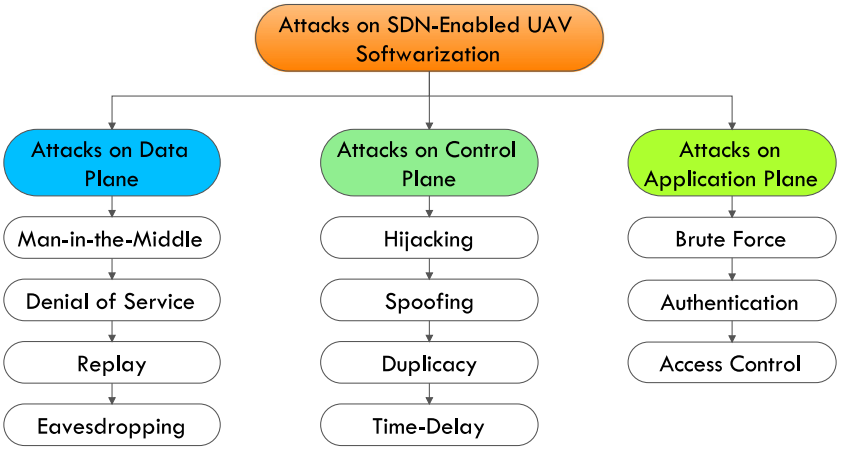


Fig. 6. Security and privacy issues in SDN-Enabled UAV softwarization [62,63].

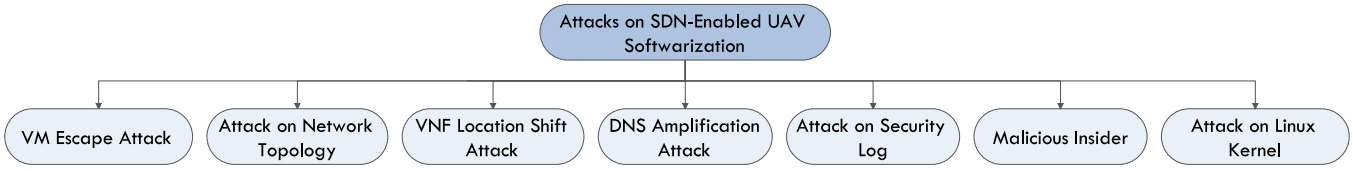


Fig. 7. Security and privacy issues in NFV-Enabled UAV softwarization.

system. Then, the attacker accesses the hypervisor management API using VNF network connectivity and tools. At last, the hypervisor is accessed by the attacker to impact the entire UAV system. For example, UAV application running in a VNF and sending constructed network packets to handle heap overflow with a conceded virtualization process [71]. This caused to arbitrary execution of code to access the host. Another way, the VNFs compose other VNFs as attacks get access to the virtualization infrastructure to compose new VNFs. Here, attacks can get full control over the infrastructure resources.

- *Attack on Network Topology*: In the UAV system, virtual networking components (e.g., virtual networks and VMs) can be easily fashioned using the NFV technique. Dynamic service choices can prone to attack when a virtual router is used to communicate between virtual networks without using any firewall. While comparing with the physical network, the dynamicity of the virtual network and its connectivity can lead to inadequate separation between the subnets and network. An attacker can compromise on virtual firewalls to restrict the functionality of the firewall, which raises the chances of attack. Another way, an attacker can obtain knowledge of multi-site network infrastructure based on the elastic nature of NFVI. Due to which, an attacker would be able to trigger VNF migration or instantiation in another NFVI without any deep packet inspection (DPI), i.e., with lower security protection within the UAV network [72].
- *VNF Location Shift Attack*: In traditional infrastructure, migration of workload beyond the legal boundaries is not possible amid strict regulations and laws. In the case of NFV, violation of laws and regulatory policies is possible by placing any VNF from a legal place to another illegal place. This can cause by violating regulatory policies, which resulted in the banning of service or putting financial penalty to the service provider. The main aim of the attacker is to harm the service provider only. Here, the attacker accomplished the insecure VNF API to access the user's personal data to violate user privacy policy. For example, the user belongs to the USA, but the attacker can shift his location as to Russia with the help of a VNF location shift attack.
- *DNS Amplification Attack*: DoS attacks may impact service availability and deplete network resources by engaged to VNFs' public interfaces or virtual networks. Enormous traffic from a compromised VNF is generated and forwarded to other VNFs working on either the same or different hypervisors. Likewise, a few VNF applications can consume high memory resources, hard disk, more CPU to exhaust the hypervisor [89]. In this scenario of a DNS amplification attack, an NFVI hosts a virtual DNS server component of a virtually evolved packet core. Then, the orchestrator in NFVI infrastructure deploys additional virtual DNS servers in case of heavy traffic load. Here, an attacker may spoof IP addresses and launches malicious DNS queries by using the spoofed IP addresses. To handle this attack, orchestrator will initiate new VMs to accommodate more DNS queries. Consequently, multiple DNS servers will reply to the victims, which will eventually receive amplified DNS query replies and result in service unavailability or disruption.
- *Attack on Security Log*: In this type of security attack, compromised VNFs generate a huge amount of security logs at the hypervisor, which makes it difficult to analyze logs. It becomes to be more difficult to analyze logs from other VNFs if initial entries are deleted in the log files. This also raises the risk of sensitive information in case infrastructure logs are leaked that enables cross relating of logs from one VNF operator to another.
- *Malicious Insider*: These types of attacks are caused by spiteful actions of internal admin users and raise internal security risks. Here, a malicious administrator records the memory dump of a VM user. From this memory dump, the attacker extracts the SSH keys, userId, password, and violates user data confidentiality and data privacy. In another scenario, an internal attacker can extract sensitive data of the user from the hard-drive volume, which is accomplished by the cloud storage devices [90,91]. Here, to extract sensitive data, the attacker first makes a backup copy of the VM drive then uses open source tools like vgscan and kpartx to access user data [92].
- *Attack on Linux Kernel*: In softwarized platforms, the kernel is an important component of the host systems to provide isolation between the UAV applications. The Secure virtualization (sVirt)

Table 3
Relative comparison of existing SDN-based security solutions.

SDN-based Solutions	Description	Merits	Demerits	Attack Mitigation
Moradi M. et al. [73]	Large scale UAV network softwarization using SDN	• Reduced network overhead due to controller placement • Support multi-path TCP communication in heterogeneous networks • More reliable network in terms of handling rapid handoffs in the network • Enable SDN controller to identify the dynamic locations of UAV nodes and handle link congestions with high bandwidth	• Packet communication overhead • End-to-end delay need to be control	Availability attack
Zhao et al. [74]	Heterogeneous multi-tier UAV networks management to handle availability issues	• Support multi-path TCP communication using heterogeneous networks • High reliable network • Enable SDN controller to identify the dynamic locations of UAV nodes • Handles link congestions with high bandwidth	• Need to handle network overhead and security issues	Availability attack
Bindra N. et al. [75]	Network parameter analysis to handle jamming attack	• Support fault free services • Handles attack mitigation and its detection	• It works well known type of attacks only • Lacks in protocol flexibility	Jamming
Secinti G. et al. [76]	Network management protocol to handle jamming attack	• Provide resiliency to the UAV network • Reduces outage rate during end-to-end communication	• Lacks in mobility • Different traffic patterns forced enhanced network energy sources utilization	Jamming attack
Li et al. [77]	Dyna-Q: A reinforcement learning algorithm	• Provide collaborative decision for UAVs using the SDN controller • Upsurge learning rate of attack detection • Jamming attack optimization	• Proposed Dyna-Q environment is quite complex to implementing and build • Increases the network communication overhead	Jamming attacks, availability attack
Sedjelmaci et al. [78]	Hierarchical detection system for UAV network	• Provides high detection rate for large scale UAV network with low number of false positive • Attack resilient model	• Need to handle network overhead, energy efficiency and security issues	Availability, spoofing and jamming attacks
Conti et al. [79]	Collaborative RED Protocol using SDN	• Efficient memory management and communication • Support attack detection in real-time scenarios	• Need to handle network overhead	Duplicacy attacks
Roy et al. [80]	Collaborative rule enforcement using SDN to handle energy consumption and duplicacy	• Given an efficient threat detection mechanism compare to existing approaches • Support robust communication using multi-path routing approach	• Need to handle network overhead and latency score	Energy consumption and duplicacy attacks
Ashraf et al. [81]	ANN based algorithm to handle DDoS attack	• Learning capabilities are efficient for small data samples • Capable to handle redundant and noisy data	• Real-time efficiency glitches and learning rate of algorithm is very low	DDoS
Giotis et al. [82]	Packet flow analysis	• Achieved optimal network and effective detection of DoS attack	• Overhead to network access and network usage performance	DDoS
Wang et al. [83]	It is a tool uses overlay based on vSwitch	• Supports third party integration • Ensure maximum network utilization with high data plane capacity • Increased control plane capacity	• Real-time efficiency glitches and Learning rate of algorithm is very low	DDoS
Kirichek et al. [84]	Packet flow analysis and filtering	• Routing traffic reduction and predict the change in network structure	• Offers low flexibility in network • Requires more additional resources which increase the cost	DDoS
Gillani et al. [85]	An approach for resilient control network	• Ensure network resiliency • Reduce critical resource sharing over the network • Reduce control traffic • Support dynamic feedback facility for each individual node	• Need to improve the network security	DDoS
Mousavi et al. [86]	A machine learning algorithms	• Efficiently detect packet flow rate • Uses the light weight protocol to detect the packet flow using entropy variation analysis	• Need multi-host support mechanism to target attacks	DDoS
Afek et al. [87]	A model for node configuration restoration	• Proposed model enables the system to handle the known definitions of attacks • Prevents the saturation of network controller • Also prevents the controller from cache misses attacks	• Need to improve the attack type detection and mitigation process	Spoofing attack

(*continued on next page*)

Table 3 (*continued*).

SDN-based Solutions	Description	Merits	Demerits	Attack Mitigation
Sriramulu et al. [88]	GPS position finder algorithm	• Supports SDN protocols and wireless mesh network • Reduces the network congestion and balances the nodes load	• No identification of optimal specifications	Spoofing attack
Ali et al. [23]	SDN-based secure architecture to protect UAVs against attack	• Provide higher adaptability of the system • Support easier reprogramming	• Field evaluations of the proposed architecture is required on a group of UAVs.	Blackhole and wormhole attack

is developed to integrate the required access control security mechanism using hypervisors based on Linux. It delivers isolation between data files and VM processes. To secure Linux kernel, other tools such as hidepd and GRSecurity can be used to provide protection [93].

5. Softwarization security solutions

This section describes the SDN nd NFV-based security solutions .

5.1. SDN-based security solutions

This section presents a security solution to secure SDNs infrastructure in the UAV system. Nevertheless, security is needed to be measured as part of the initial design of SDNs. Table 3 presents a comparative summary of the present SDN security solutions. A few of the security solutions to secure SDNs are as follows.

5.1.1. Secure design of SDN

The energies of researchers applied to the secure design of SDN are tremendously limited. Shinet al. put forward a security-specific framework FRESCO for OpenFlow Networks [94]. FRESCO enables the application programming interface (API) that permits security experts to cultivate threat detection logic and provide security monitoring libraries. This framework uses a security enforcement kernel FortNox, which avoids conflict of rule arises from different security authorizations. FRESCO has an impact on the control layer, application layer, and the interfaces between these two layers, excluding the data layer [95]. FortNox has an impact on authorization and rule conflict on the southbound interfaces, northbound interfaces, and control layers. It improves the security of the infrastructure and application layer.

5.1.2. Security analysis

Wang et al. [96] recommends a systematic approach to detect the conflicts and resolve them in the SDN firewall by checking authorization and flow space. This approach searches the flow path in the entire network and checks the paths against the firewall. The efficacy of the proposed approach is examined via header space analysis [97]. Shin et al. [98] presented noteworthy changes in SDN during the attacks. One of the changes is connection migration that expressively reduces the data-to-control plane communications, which increases on the southbound interface during an attack. Another is the actuating trigger to accelerate the openness of SDN data plane flow dynamics. Then, an adaptive method to detect anomalies in the SDN system refers to OpenWatch has been proposed [99].

5.1.3. Implementation of suitable audit

Skowyra et al. [100] developed a scheme that satisfies system design requirements. Here, an infrastructure tool is highlighted to analyze real-time environment without relying on preceding knowledge of formal logic—this scheme studies network correctness verification and specification modeling along with consideration of scalability issues of OpenFlow systems. Further, in [101], a packet back-trace scheme is proposed for software developers of the SDN to find the root cause of bugs via reconstruction of the series of events. It assists SDN programmers in handling logical errors, protocol compatibility errors, and simplifies network operators to generate a complete bug report.

5.1.4. Security enhancement

To enhance security in SDN infrastructure plays an important role, and various research works have been done so far in this regard. For example, FleXam has been proposed to get packet-level information [102]. It reduces the control plane load and eliminates flow setup time. Other noticeable solutions for security enhancement are learning intrusion detection systems (L-IDS) [18] and CloudWatcher to monitor clouds [103].

5.1.5. Security policy enforcement

The enforcement of security policy is one of the critical issues for the research community due to the dynamic nature of SDNs. Son et al. [104] presented a model FLOVER to verifies the policies running against the system's security policies. Another contribution in this area, D. Kreutzer et al. [18] verify the real-time invariants using the VeriFlow scheme. This study presents the verification of the program traffic isolation and handles the misconfiguration of intra-switch. Further, a fine-grained permission system PermOF [105] has been proposed to comprises a runtime isolation mechanism and OF-specific permissions to apply for the permissions.

5.2. NFV-based security solutions

In this section, we highlight the existing security solutions in order to achieve rationally enhanced security protection against attacks on the NFV environment. These practices do not assure the complete security of NFVI, but then again provide better resiliency in case of an attack. Table 4 presents the relative comparison of some of the existing NFV-based security solutions.

5.2.1. Kernel security

The kernel security is of utmost importance in a virtualization system; it provides detention between the applications. There are various tools and software's available to ensure the kernel security in different aspect; few of the examples are hidepd (prevent from unauthorized user to see process information), GRSecurity (protect against corrupted memory attacks), SELinux (integrate access control security with hypervisors) and sVirt (secure virtualization provides isolation between data files and VM processes) [69].

5.2.2. Remote verification

In this technique, the trust status of the NFV platform is verified remotely. It can be used by either user or the platform owner to verify that the platform has booted securely [117]. The practical implementations include the open-source software refers as open cloud integrity tool (openCIT) hosted on GitHub.

5.2.3. Security zoning

It is a good practice to dispersed management traffic and VM traffic to prevent a VM from impacting other VMs or hosts in case of attack. This will help to prevent management infrastructure from any attacks on VMs. More separation of the VLAN into groups that are in use and which are not in use. Correspondingly, VMs of equivalent functionalities can be grouped into zones. Here, a dedicated firewall and access control policies are used in every zone to increase the security level; a demilitarized zone is one of the examples of it.

Table 4
Relative comparison of existing NFV-based security solutions.

NFV-based solutions	Short description	Merits	Demerits	**Application area**
CloudSafetyNet [106]	Data leakage detection	A cost effective approach and support scalability	Need to improve communication overhead	Data security
Williams et al. [107]	An approach to facilitate virtual private network as a service	The proposed approach apply one or more TCP optimizations, effective, easy-on, global and cost saver.	–	Data security
CloudMonatt [108]	Security health Monitoring	Proposed approach is easy to implement, flexible, cost effective approach and support specific function with scalability	Require to improve security and single point of failure issue.	Intrusion detection and its prevention
CryptVMI [109]	Encrypted virtual machine introspection	Proposed approach is flexible, cost saving approach, effective and support scalability	Need to handle centralized control and management	Intrusion detection and its prevention
CloudSec [110]	Security monitoring appliance	CloudSec is flexible, scalable and cost effective in nature	Does not support specific function and need to handle centralized control and management	Intrusion detection and its prevention
Yan et al. [111]	A secure and trust framework for network virtualization	Proposed framework support flexibility, generality, security, integrity and trustworthiness	Require to improve quality of service and reliability	Network isolation security
Lango et al. [112]	Security management in the trusted virtual data center	Support trusted and reliable virtual network, enhancing guest utilization of virtual data center resources for instance virtual storage and virtual machines and low implementation cost	–	Network security
MANOaaS [113]	Isolation of network virtualization	DCPortal is easy to implement, efficient, scalable and cost-effective	Having single point failure issue due to centralized control	Network isolation security
Radiant Logic [114]	Virtualized solution using federated identity service	It is Cost effective and scalable	Need to handle dependability and flexibility issue	Authentication and access control management
SecMANO [115]	Identity and access management in virtual environment	The proposed approach is effective as it support various features like scalability and complexity of lifecycle	Need to make the approach more secure and handle dependability issue	Authentication and access control management
Jacob et al. [116]	Deploying access control on virtual network function	The proposed approach is cost effective, scalable and support lifecycle management complexity	The lacking of flexibility and dependability feature makes the proposed approach less effective	Authentication and access control management
Aguero et al. [6]	Virtualized Environment for Multi-UAV Network Emulation (i.e., VENUE)	Integration of VENUE platform and real softwares, evaluates routing protocols, and validates network service functionality	Developments of different mobility models is required to cover multiple UAV	Data and Network security

5.2.4. Hypervisor introspection

It can be used to inspect software residing inside VMs to find anomalous activities. It works as host-based IDS, which has access to all VMs; thus, the bootkit and rootkit inside VMs cannot hide easily. This helps to enhance the functionalities of hypervisor by access files in storage, monitor network traffic, and read memory execution. The APIs used in hypervisor introspection are powerful tools to accomplish deep VM analysis and possibly upsurge VM security. Though, APIs can also be exploited, possible to break and bypass the separation between hypervisor and VMs. LibVMI (developed in C language with Python) is one of the libraries for hypervisor introspection. It gives the hypervisor to accomplish an in-depth inspection of VMs such as vCPU register inspection, memory checking, and recording trapping events [118].

5.2.5. Orchestration and security management

The right designing of the NFV orchestrator incorporates the trust and security requirements of NFVI. It requires an integration of the VNF manager, security orchestrator, and the element management systems. This protection can be achieved by network service descriptor or setting scaling boundaries to protect from various attacks like DNS amplification attack and the others attack.

5.2.6. Virtual network security

The VMs and underlying hardware need to be secure to protect the entire infrastructure [119]. The regular update of the hypervisor by applying the released security patches is one the best solution. On the contrary, the entire infrastructure would expose to security risks. Further, we need to disable all services, which are not in use like remote access services and SSH require for a short duration, not all the time. The administrator is the caretaker of the entire infrastructure by using their accounts as keys. The administrator account should be secure by using a strong password accompanied by strictly following security guidelines.

5.2.7. Trusted platform module

The Trusted platform module (TPM) measures the profound system components of hardware root-like platform firmware, OS kernel,

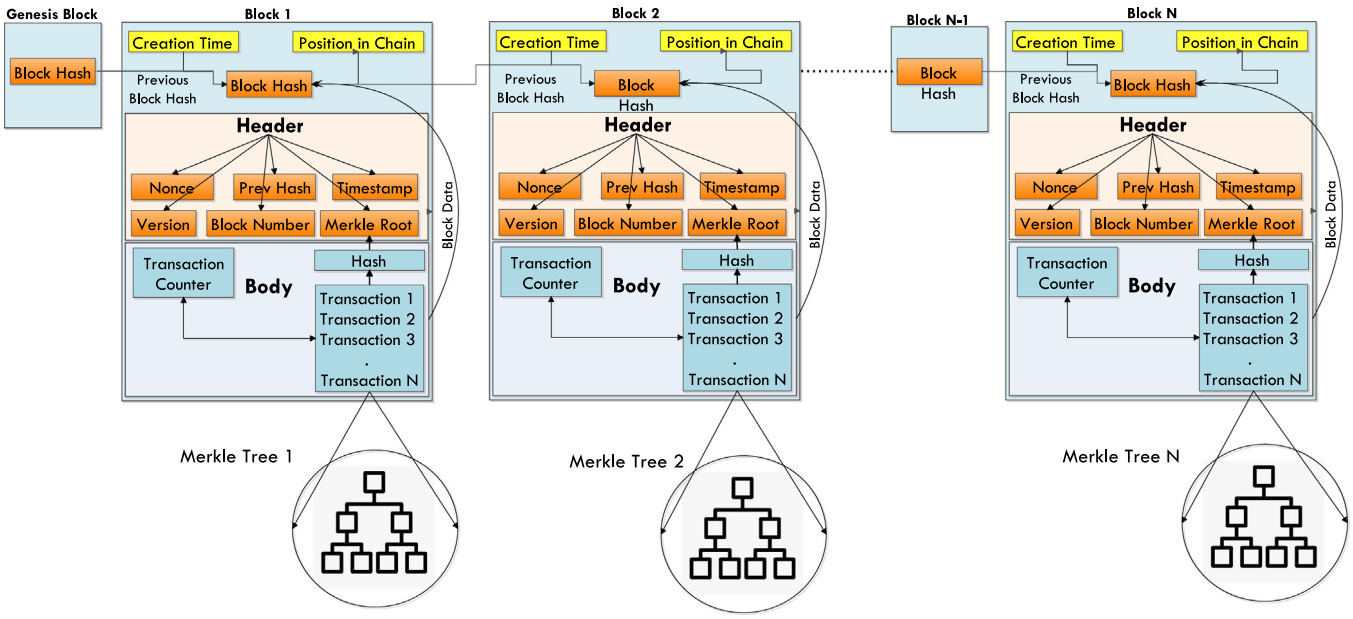


Fig. 8. Structure of blockchain.

bootloader, BIOS, and others that securely verified and stored. The TPM works when the system is rebooted or reset during system runtime; new platform measurement is not possible. Then, the validation of the platform measurements can be achieved using a remote attestation server or launch control policy of TPM [120,121].

5.2.8. VNF swap area encryption

The virtual disks accompanying VNFs encompasses sensitive data, which need to be protected. This can be achieved by storing cryptographic keys and encryption of VNF volume. Besides, to prevent VNF from unauthorized access, the hypervisor should be securely configured. The memory management technique VM swapping is used as secondary memory (transfer memory segments between main memory and disk) to upsurge system performance in the event system runs out of memory. The data resides in the transferred memory segment can be sensitive data such as certificates and passwords, which remain determined even after rebooting the system and create an attack scenario. This can be handle by encrypting VM swap areas or using Linux based tools like dm-crypt [122].

6. Blockchain technology: The concept

6.1. Overview of blockchain

The traditional centralized systems like cloud and fog are always under the influence of data security and privacy issues [123]. Nevertheless, blockchain, a distributed ledger, an emergent technology, provide data security and privacy. It record all transaction data in distributed manner and has potential to overcome centralized storage issues such as single point of failure, security and privacy issues [124].

The blockchain was first introduced by an anonymous researcher (referred to as Satoshi Nakamoto) in the year 2008 (presented bitcoin framework) [125]. It is a chain of blocks group together with a hash value of the previous block within the network [126]. A single block consists of a block header, block hash, and block body, as shown in Fig. 8. Here, block header comprises various information such as version, previous block hash, Merkle root, timestamp, nonce (for proof-of-work (PoW)), and block number [127]. The every $(N+1)$th block hash value is calculated using the hash value of Nth block to ensure the immutability of data. The hash function used to calculate hash values are needed to be strong like a Message-Digest Algorithm (MDA) and the Secure Hashing Algorithm (SHA) [128,129]. Then the body of block stores the other information such as data hash values, transactions, and transactions counter [130].

The blockchain ensures data security using cryptographic primitives, where each participant can use their digital signature (private key generation for the corresponding transaction). In case any mischievous user updates the transaction of Nth participant over BC, then its digital signature becomes invalid. Therefore, the cryptographic primitives secure the data immutability and participant's identity too. The digital agreement between two parties over BC is called the smart contract (SC), which eliminates the need for a third-party for digital agreement [131]. SC is a programming code, which can be written in a specific language like C++, javascript, solidity, simplicity, and rholang [132]. SC cannot be negated or modified once it is signed. It reduces the transaction processing time and execution overhead over the blockchain network.

6.2. Blockchain environments

Further, the BC is categories into three diverse types such as private, public, and consortium blockchains.

- *Public Blockchain:* The public blockchain is entirely decentralized, distributed, and permissionless, where everyone can join the blockchain network, for example, Bitcoin and Ethereum. A new block creation in public blockchain is computationally expensive [133] and requires a specific amount of processing fee.
- *Private Blockchain:* This type of blockchain can be managed by a single organization, where every member is well-known to the organization. It is a permissioned-blockchain and does not involve any processing fee for the transaction.
- *Consortium Blockchain:* It is quite similar to private blockchain (permissioned), but the difference lies as it involves multiple organizations to build the blockchain network [134]. It also does not encompass any processing fee for the transaction and not computationally expensive.

6.3. Security and privacy aspects of blockchain

The widespread of UAV system requires efficient service delivery models, which involve new actors in the ecology. The cloud and virtualization infrastructures leveraged to provide scalability, flexibility, and

the capability to deliver services quickly. Though this paradigm shift enables innovative capabilities but produces complex security issues. In line with this, the BC technology can suffice this security problem; also, handle a few more issues pertaining to the UAV system such as identity management, air traffic control, and insurance. The UAV system requires to be provisioned with cryptographic data, which supports authenticated, confidential, and secure communications between UAVs using blockchain [135]. This will ensure that the secure data transmission as it is encrypted (UAV carry out sensitive task or mission). For example, In the case of UAVs are being used for package delivery using blockchain technology, it enables UAV owners to log information of the time, location, delivery date, and resources. It makes the UAV data accessible to legitimate users and stakeholder's along with the route information of the package.

Several research works focus on security aspects in UAVs using BC. To secure UAV communication, the authors Aggarwal et al. [136] have presented a game theory-based approach for block creation, i.e., forger node using a specific UAV and rest UAVs participate in block verification and validation using proof of stake (PoS) consensus mechanism [137]. This study shows that the BC-based security model provides better performance compared to other existing security systems for the UAV ecosystem in terms of communication cost and latency. This approach also shows the securing UAV data dissemination among end-users [138]. Further, Kuzmin et al. [139] shows how BC protects the integrity of data and secure data storage by writing them inside a block. They have implemented flight route control and its schedule using SC based on a particular condition. The implementation of blockchain is a very critical task as it requires rigorous simulations. Though it has been carried out by Lei et al. [140] with effective results, more robust testing is needed for complex UAV environment. Blockchain helps to avoid mid-air collision of UAVs as route information of peer UAV is shared with the other UAV, which allows the UAVs to maintain a safe distance from each other. More, to secure the UAV networks blockchain mitigates the jamming of UAV signals due to its decentralized architecture, detect UAV hijack using various consensus mechanism such as PoW, PoS and many more [141].

6.4. Integration of blockchain with softwarization techniques

SDN employs flexible, efficient, and innovative deployment of network applications by separating the network control from the forwarding plane. It is a propitious solution to enhance the scalability and versatility of UAV network. A major issue with the centralized SDN controller is a single point failure, which can disrupt working of entire UAV network [142]. To overcome such issue, the integration blockchain with SDN controller is a perfect solution. Apart from single point failure, a blockchain-based SDN controller resists against various cyber-security attacks such as insider attack, man-in-the-middle attack, and hijacking attack.

7. The proposed solution: Blockchain-based softwarized architecture

Fig. 9 presents the proposed blockchain-based softwarization framework for UAV network management using blockchain technology, SDN, and NFV techniques. It provides flexibility to the network function management, security, and efficiency in data UAV communication (between UAV-to-UAV and UAV-to-ground station). This proposed framework is conceptually divided into four different layers (i) infrastructure layer, (ii) blockchain middleware layer, (iii) control layer, and (iv) application layer. The functionality of each layer is as follows.

7.1. Infrastructure layer

It is also known as a data plane with virtualization that encompasses both physical and virtual instances (created by VIM) of the network hardware devices such as routers, switches, and access points. There exists N number of UAVs are operating in the sky to serve different application scenarios such as military operations, battlefield surveillance, healthcare, package delivery, and search & rescue. So, it is quite complex to manage the huge number of heterogeneous devices and also vulnerable to various security issues, as mentioned in Section 2. If any malicious UAV can join the network or the existing UAV becomes compromised can either affect the system efficiency or disrupt the communication completely. Blockchain is a viable solution to this issue and protects the entry of malicious UAV into the network.

VIM component of this layer is responsible for virtualization and orchestration of resources. The entire physical network is virtually partitioned to serve the different application scenarios without investing much on the installation of new dedicated hardware. It makes the UAV network cost-effective, scalable, and efficient. Each virtualized network and SDN controller is connected to the blockchain network for security and transparency of data communication. The data in a blockchain is authenticated using algorithms such as message-digest, SHA256, Kerberos, and password authentication protocols [144]. It obliterates the possibility of any malicious activity in the UAV network and also protects against MiM, spoofing, and eavesdropping attacks.

The communication infrastructure to be used for UAV communication is 5G-enabled Tactile Internet (5G-TI) [145]. It is able to achieve the radio latency of < 1 ms and the device latency of < 5 ms, which is suitable for mission-critical UAV network [146]. It also makes the UAV network reliable (99.999%) with 10^{-7} or 3.17 s system outage per year [147].

7.2. Control plane

It is also known as the brain of the UAV communication network, where all functional decisions related to the network hardware are taken. It is logically separated from the data plane or forwarding plane with the benefit of translating SDN application requirements to the UAV data paths, and providing an abstract view of the entire network to the SDN applications [7]. The separation also helps to manage the large UAV network efficiently [148]. This layer is in the middle of the other layers and is communicating with them via the agent-driver interfaces. It transmits the UAV control related information to the infrastructure layer via controller-data plane interface (CDPI) driver and the infrastructure layer receives the information through their CDPI agent. Likewise, the northbound interface (NBI) driver at the application layer passes the information to the control plane vita NBI agent. These interfaces are open-source interfaces for inter-layer communication.

This layer comprises of NFs and the SDN controllers. NFs would be dynamic routing, access control, network monitoring, path selection, device discovery, hop calculation, switching, and topology estimation. Table 5 shows the exhaustive list of existing SDN controllers. All controllers are connected to the public blockchain network via Ethereum client to form a P2P network after satisfying rules/instructions mentioned in the SC so that they can communicate in a fully-decentralized way. Controllers are responsible for collecting the UAV parameters and network statistics in order to manage it properly and efficiently. The SDN controllers at the control plane are more vulnerable to the cyberattacks and the blockchain helps to preserve the controller data security as well as UAV network system integrity.

The public blockchain is open and fully decentralized in which any SDN controller can join the blockchain network without any additional computational overhead. The controller captures the network statistics and develops a flow table for the data movement from source to destination. It is then passed to the infrastructure layer via a southbound open interface.

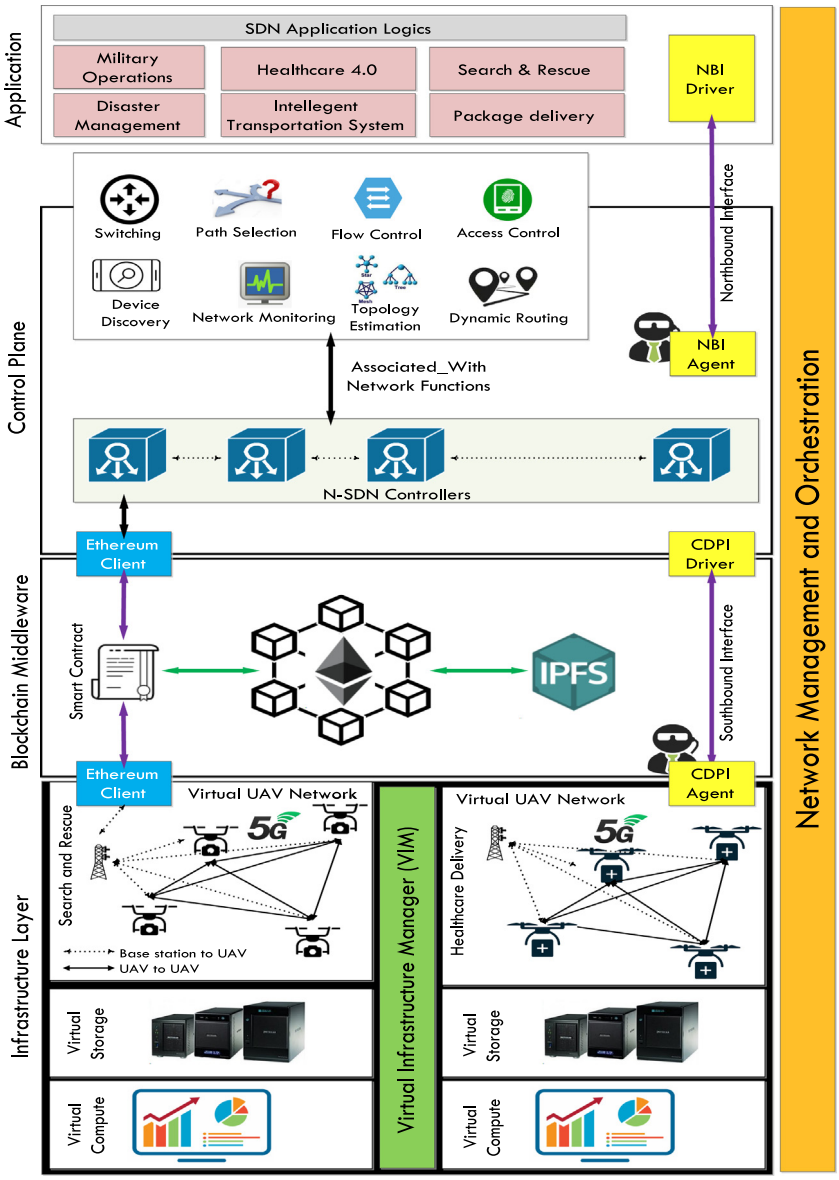


Fig. 9. Proposed blockchain-enabled UAV softwarization architecture [105,143].

7.3. Application plane

These are the software programs (written in Java, Python, REST, and JSON programming languages) that directly intimate their network functional requirements and behavior to the SDN controller via NBI. This layer consists of application logic and the NBI driver. It is an open platform for software developers to design any innovative applications to communicate with the SDN controller via the NBI agent in order to collect the network statistics for efficient decision making. Such applications could be military operations, healthcare 4.0, disaster management, intelligent transport system, search and rescue, and package delivery.

7.4. Blockchain layer

It acts as a security layer between the infrastructure and the control layers. Here, we consider an Ethereum (public) blockchain to store the UAV communication and SDN controller information as a transaction (hash value). Both the control and infrastructure layer communicates with the blockchain layer via the Ethereum client [151]. The data in a blockchain is to be stored only after it satisfies the SC conditions. The benefits of using blockchain in a softwarized UAV architecture are as follows.

- *Data Immutability:* Once the UAV communication data is stored in the blockchain. It does not entertain any kind of modification in it. If any malicious or compromised UAV forcefully tries to modify the block transaction, all its consecutive block hashes would become invalid, and this activity can be stored into the blockchain [152]. It helps to track the malicious intruder and take necessary action against it. This characteristic of blockchain makes the UAV communication secure.
- *Traceability:* Blockchain keeps every single activity that happened in the UAV communication as a transaction that is immutable in nature [153]. This feature helps to easily track the UAV malicious activities.
- *Transparency:* Blockchain is a distributed and decentralized ledger, where each participant node has a copy of the entire ledger. This brings transparency in the UAV softwarized network system.
- *Data Reliability:* Blockchain eliminated the issue of single-point failure and ensures the data and system reliability.

Table 5
Open source SDN controllers [149,150].

Controller Name	Language	License	Developer	Purpose
Project Calico	–	Apache 2	Tigera	Provide the network connectivity between workloads and enforce network security.
The Fast Data Project (fd.io)	–	Apache 2	LF Networking Fund (LFN)	–
vneio/sdnc	Intel DPDK technology	Apache 2	vne.io	It has the fast packet processing capabilities compared to other JAVA, Python or Ruby based controllers.
Faucet	Python	Apache 2	faucet-dev	OpenFlow controller for multi table OpenFlow 1.3 switches
NOX	C++ & Python	GPLv3	Nicira/ Vmware	To manage and develop network control related applications
Open vSwitch	C	Apache 2.0	Nicira	It supports virtual distribution of switches across the network
Beacon	Java	Stanford	Stanford University	Used to check the performance benchmarks
OpenDay- light	Java	EPLv1	OpenDaylight Project	Exposes Northbound application programming interfaces
Floodlight	Java	Apache 2.0	Big Switch Networks / Cisco	To orchestrate traffic flow in SDN environment
Open Contrail	Python	Apache 2.0	Juniper Networks	It is used to deploy the cloud to automate NFV
Ryu	Python	Apache 2.0	NTT Communications	It is used to enhance the network agility
Onos	Java	Apache 2.0	Open Networking Lab	To increase the performance, scalability
Runos	C++	Apache 2.0	Applied Research Center for Computer Networks	It helps to run multiple applications independently
Cherry	Python	Creative-Commons-Licence	CherryPy Team	To circulate the information related to the security and policy of an enterprise
Open Kilda	Python & Java	Apache 2.0	Telstra	It solved the problem of latency in distributed SDN controller environment

To store data directly as a transaction in a blockchain is quite costly, i.e., ≈ $ 550 per 1 MB of data, which is not affordable. The alternative to this is to store the data in the distributed and immutable storage called Interplanetary File System (IPFS), which returns the hash value of the data as a token. Then, store this hash value as a transaction in the chain of blocks. IPFS does not charge anything to store the data distributively in it. The other benefit of using IPFS is speedup downloading speed with minimum bandwidth utilization.

8. Open issues and research challenges

Although the blockchain-based secure, decentralized, and scalable and softwarized UAV network offers various welfares in terms of privacy, security, and anonymity, it brings various advancing obstacles during implementation. These open research issues and challenges are needed to be addressed while integrating blockchain, NFV, SDN, and UAVs effectively and efficiently. This section highlights the challenges of blockchain-based softwarized UAV networks to secure data and communication networks with scalability as shown in Fig. 10.

8.1. Interoperability

The softwarized UAV system is embedded with network hardware pieces of equipment like switches and routers that are not vendor-specific, which raises the interoperability issues. This needed to be handling effectively and carefully using the proper solutions. The interoperability issues need attention, while the proposed blockchain-based softwarized UAV system is deployed in real-time.

Fig. 10. Open issues and research challenges associated blockchain-enabled UAV softwarization.

8.2. Data processing latency

UAV systems are entrenched with multiple sensors that generate a massive amount of data, and the processing of such enormous data on the dynamic environment of UAVs would produce partial solutions for decision making. Softwarization permits the data transfer

to the centralized SDN controller, where after processing of data, an optimal solution can be achieved but with an extra delay. So, the proposed blockchain-based softwarization architecture for UAV could reduce delay during data offloading. This facilitated due to distributed data storage techniques in the blockchain, where each member of the blockchain network has a copy of the ledger.

8.3. Real-time deployment

There few researchers around the world have worked in the UAV softwarization domain [5,15,27,31,60,154]. The existing literature mostly dedicated on survey, review, or development on a testbed. The blockchain-based secure UAV softwarization has not been explored yet by the researchers. Conversely, real-time deployment is still a challenge for highly movable UAVs. Hence, its real-time deployment is indispensable to mitigate privacy and security issues.

8.4. Data security

In Softwarized UAV system, data security is the prime concern. Softwarized UAV system suffers from security issues due to various attacks such as DDoS and spoofing, which makes its deployment, UAV routing, and its monitoring difficult through the APIs at the control layer. Therefore, the proposed blockchain-based architecture can solve these security issues, but then again, real-time deployment is in the embryonic stage.

8.5. Single point failure

The existing UAV softwarized architecture may have a single-point failure issue, i.e., a centralized SDN controller takes all decisions about the entire communication network of UAV. The proposed architecture emphasizes handling this issue by storing the decision data of the controller in a distributed manner at different nodes, which is reachable even after the failure of any node. Nevertheless, in the proposed architecture, there is only one SDN controller for decision making for each application. So, in the scenario, the SDN controller fails, then the complete application-specific decision making gets impacted. The probable solution to this is to add more redundant controllers, which increases the implementation cost of the proposed architecture. The selection of the optimal number of controllers is noteworthy for further investigation in the UAV network.

8.6. Quality of service (QoS)

The primary objective of the softwarization of the UAV network is to reduce operational and management complexity while preserving the network service's quality. Hence, it needs great significance to study QoS in different scenarios and use cases, specifically when security is a crucial requirement. The network performance issue and the reliability of services play an essential role to configure, deploy, and scale multiple VNF in the real-time environment of UAV. Though NFV has great potential, there are still some challenging issues such as network performance issues with respect to various parameters like queuing capabilities, throughput, latency, and security, designing of the efficiently enable network and hardware support for the virtualization. Further, the uses of VNFs may associate with the network services reliability over the UAV environment. The deployment of VNF and network services depends on low-cost hardware, whereas using orchestrates software and manages complex network services. The use of low-cost commodity hardware may increase risks such as VNF instance and network services unreliable due to various factors like hardware failure, server overloaded performance degradation, and many more. To handle these issues, pool managers can be used for resource pooling to manage VNF instances and interact with the service control entities to reach the desired reliability level over the UAV network [155].

8.7. Computational complexity of controller

The controller computational complexity increases due to block mining, authentication, UAV validation, and verification of a new controller in the UAV system. Separately from access control techniques and validation, the controller has to pay attention to numerous Network control functions (NCFs), for instance, device discovery, network routing, monitoring, and topology estimation [124].

8.8. Resource pooling

In softwarized UAV network, multiple applications use the concept of resource sharing or virtual resource pooling to increase the scalability and efficiency of the UAV system. A single attack on any virtual function can affect the other virtual functions, which need excessive attention in future research work [156].

8.9. Smart contract security

SC is a piece of software code, which is used to establish the trust between the peer nodes of the blockchain without the involvement of any central entity. It is susceptible to man-in-the-middle, eavesdropping, fabrication, and spoofing attacks. So, there is a need to devise the proper testing mechanism for validating the SC security vulnerabilities before deploying it into the blockchain network.

8.10. Blockchain standardization

The acceptable standards of blockchain has not been developed yet by the renowned organizations such as IEEE and ITU. Thus, the smooth and efficient integration of blockchain with UAV communication needs proper rules and regulations for real-time deployment. So, this arises the need to frame technical standards with proper guidelines that make its deployment in UAV network simple and efficient.

9. Conclusion

Despite the well-recognized benefits and potentials of softwarized UAV networks, security remains a key challenge for network service providers as well as customers. Secure and scalable softwarized UAVs network using SDN/NFV still remains a faraway goal. To meet the UAV network security requirements, this study presented a blockchain-based security implications on softwarized UAV network. In this paper, firstly, we analyze the potential vulnerabilities, threats, and attacks on softwarized UAV network, and then identify the corresponding security solution for counter-mining attacks during softwarization. We also highlight how softwarization can facilitate the UAV network to satisfy the operational, design, and security challenges. We have emphasized the critical network security issues in SDN and NFV-based UAV systems along with attack taxonomy. Then, we presented secure blockchain-based softwarization architecture for the UAV network using 5G-TI to mitigate the aforesaid security issues and provide efficient communication. The proposed architecture not only provides data and network security, but it also protects data from being tampered once captured in the blockchain. Then, the 5G-TI enables the reduction in communication delay for its efficient operation. Finally, we underlined several open research challenges and future directions for UAV softwarization. In short, blockchain-based softwarization is a key enabler to meet the secure, scalable, and efficient UAV communication network. Though numerous research efforts have been taken in this study on blockchain-based UAV softwarization, several issues remain open for future research.

In the future, we would explore the proposed architecture in the different scenario for UAV-based healthcare application.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work is supported by Visvesvaraya Ph.D. Scheme for Electronics and IT by Department of Electronics and Information Technology (DeiTY), Ministry of Communications and Information Technology, Government of India.

References

[1] S. Tanwar, S. Tyagi, S. Kumar, The role of internet of things and smart grid for the development of a smart city, in: Y.-C. Hu, S. Tiwari, K.K. Mishra, M.C. Trivedi (Eds.), Intelligent Communication and Computational Technologies, Springer Singapore, Singapore, 2018, pp. 23–33.

[2] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0, in: 2019 International Conference on Computer, Information and Telecommunication Systems, CITS, 2019, pp. 1–5.

[3] Make in India for unmanned aircraft systems, 2019, http://ficci.in/spdocument/23003/Make-in-India-for-UAS.pdf, (Accessed 2019).

[4] The state of drone market in India, 2019, https://www.expresscomputer.in/news/the-state-of-drone-market-in-india/44529/, (Accessed 2019).

[5] S. Mahmoud, I. Jawhar, N. Mohamed, J. Wu, UAV and WSN softwarization and collaboration using cloud computing, in: 2016 3rd Smart Cloud Networks Systems SCNS, Dubai, United Arab Emirates, 2016, pp. 1–8.

[6] V. Sanchez-Aguero, F. Valera, B. Nogales, L.F. Gonzalez, I. Vidal, VENUE: Virtualized environment for multi-UAV network emulation, IEEE Access 7 (2019) 154659–154671.

[7] Wikipedia, Software-defined networking, 2014, https://en.wikipedia.org/wiki/Software-defined_networking, (Accessed 2014).

[8] SDN architecture overview, 2019, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf, (Accessed 2019).

[9] Open Networking Foundation, OpenDaylight (ODL), 2013, https://www.opendaylight.org/, (Accessed 2013.

[10] G. Verticale, A. Capone, Softwarization and virtualization, 2019, https://www.5gitaly.eu/2018/wp-content/uploads/2019/01/5G-Italy-White-eBook-Softwarization-and-virtualization.pdf, (Accessed 2019).

[11] I. Zacarias, J. Schwarzrock, L.P. Gaspary, A. Kohl, R.Q. de Araujo Fernandes, J.M. Stocchero, E.P. de Freitas, Enhancing mobile military surveillance based on video streaming by employing software defined networks, Wirel. Commun. Mob. Comput. 2018 (2018) 1–12.

[12] Exclusive: Iran hijacked US drone, says Iranian engineer, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer, (Accessed 2011).

[13] Hak5 1520 – pineapple drone, rooftop packet sniffing and offline archival backup, 2014, https://www.hak5.org/episodes/hak5-1520, (Accessed 2014).

[14] G. Sanders, The very real dangers of hacked drones, 2019, https://tractica.omdia.com/robotics/the-very-real-dangers-of-hacked-drones/, (Accessed 2019.

[15] J. McCoy, D.B. Rawat, Software-defined networking for unmanned aerial vehicular networking and security: A survey, Electronics 8 (12) (2019) 1–25.

[16] S. Fichera, L. Galluccio, S.C. Grancagnolo, G. Morabito, S. Palazzo, OPERETTA: An openflow-based remedy to mitigate TCP SYNFLOOD attacks against web servers, Comput. Netw. 92 (2015) 89–100.

[17] R. Mohammadi, R. Javidan, M. Conti, SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks, IEEE Trans. Netw. Serv. Manag. 14 (2) (2017) 487–497.

[18] D. Kreutz, F.M. Ramos, P. Verissimo, Towards secure and dependable software-defined networks, in: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, HotSDN '13, Association for Computing Machinery, New York, NY, USA, 2013, pp. 55–60.

[19] J.H. Lam, S.-G. Lee, H.-J. Lee, Y. Oktian, Securing SDN southbound and data plane communication with IBC, Mob. Inf. Syst. 2016 (2016) 1–13.

[20] S. Matsumoto, S. Hitz, A. Perrig, Fleet: Defending SDNs from malicious administrators, in: Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, HotSDN '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 103–108.

[21] A. Bates, K. Butler, A. Haeberlen, M. Sherr, W. Zhou, Let SDN be your eyes: Secure forensics in data center networks, ISBN: 1-891562-36-3, 2014, http://dx.doi.org/10.14722/sent.2014.23002.

[22] A. Lara, B. Ramamurthy, OpenSec: Policy-based security using software-defined networking, IEEE Trans. Netw. Serv. Manag. 13 (1) (2016) 30–42.

[23] C. Guerber, N. Larrieu, M. Royer, Software defined network based architecture to improve security in a swarm of drones, in: 2019 International Conference on Unmanned Aircraft Systems ICUAS, Atlanta, GA, USA, 2019, pp. 51–60.

[24] R. Sairam, S.S. Bhunia, V. Thangavelu, M. Gurusamy, NETRA: Enhancing IoT security using NFV-based edge traffic analysis, IEEE Sens. J. 19 (12) (2019) 4660–4671.

[25] R. Gupta, A. Kumari, S. Tanwar, A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles, Trans. Emerg. Telecommun. Technol. n/a (n/a) e4009.

[26] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, BloHosT: Blockchain enabled smart tourism and hospitality management, in: 2019 International Conference on Computer, Information and Telecommunication Systems CITS, Beijing, China, 2019, pp. 1–5.

[27] M. Sara, I. Jawhar, M. Nader, A softwarization architecture for UAVs and WSNs as part of the cloud environment, in: 2016 IEEE International Conference on Cloud Engineering Workshop IC2EW, Berlin, Germany, 2016, pp. 13–18.

[28] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in UAV communication networks, IEEE Commun. Surv. Tutor. 18 (2) (2016) 1123–1152.

[29] C. Rametta, G. Schembra, Designing a softwarized network deployed on a fleet of drones for rural zone monitoring, Future Internet 9 (1) (2017).

[30] B. Nogales, V. Sanchez-Aguero, I. Vidal, F. Valera, Adaptable and automated small UAV deployments via virtualization, Sensors 18 (12) (2018) 1–16.

[31] F. Al-Turjman, M. Abujubbeh, A. Malekloo, L. Mostarda, UAVs assessment in software-defined IoT networks: An overview, Comput. Commun. 150 (2020) 519–536.

[32] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, M. Debbah, A tutorial on UAVs for wireless networks: Applications, challenges, and open problems, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2334–2360.

[33] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile internet and its applications in 5G era: A comprehensive review, Int. J. Commun. Syst. 32 (14) (2019) e3981, e3981 dac.3981.

[34] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, J.J. Rodrigues, Tactile internet for smart communities in 5G: An insight for NOMA-based solutions, IEEE Trans. Ind. Inf. (2019) 1.

[35] K. Hartmann, K. Giles, UAV exploitation: A new domain for cyber power, in: 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2016, pp. 205–221.

[36] P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned UAV networks: Challenges, solutions, and comparisons, Comput. Commun. 151 (2020) 518–538.

[37] M.P. Arthur, Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS, in: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, 2019, pp. 1–5.

[38] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M.S. Obaidat, A systematic review on security issues in VANET, Secur. Priv. 1 (5) (2018) e39.

[39] N. Sharma, A.S. Bisen, Detection as well as removal of black hole and gray hole attack in MANET, in: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016, pp. 3736–3739.

[40] S.U. Patil, Gray hole attack detection in MANETs, in: 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 2017, pp. 20–26.

[41] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, E. Ghanbari Parmehr, Spoofing detection of civilian UAVs using visual odometry, ISPRS Int. J. Geo-Inf. 9 (1) (2020) 1–23.

[42] J. Grover, V. Laxmi, M.S. Gaur, Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks, CSI Trans. ICT 1 (2013) 261–279.

[43] K. Patel, D. Mehta, C. Mistry, R. Gupta, S. Tanwar, N. Kumar, M. Alazab, Facial sentiment analysis using AI techniques: State-of-the-art, taxonomies, and challenges, IEEE Access (2020) 1.

[44] T.M. Hoang, N.M. Nguyen, T.Q. Duong, Detection of eavesdropping attack in UAV-aided wireless systems: unsupervised learning with one-class SVM and K-means clustering, IEEE Wirel. Commun. Lett. 9 (2) (2020) 139–142.

[45] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi, I. Jawhar, UAVs for smart cities: Opportunities and challenges, in: 2014 International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, 2014, pp. 267–273.

[46] Wikipedia, Software-defined networking, 2014, https://en.wikipedia.org/wiki/Software-defined_networking, (Accessed 2014).

[47] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, H. Flinck, Network slicing and softwarization: A survey on principles, enabling technologies, and solutions, IEEE Commun. Surv. Tutor. 20 (3) (2018) 2429–2453.

[48] J. Bhatia, Y. Modi, S. Tanwar, M. Bhavsar, Software defined vehicular networks: A comprehensive review, Int. J. Commun. Syst. 32 (12) (2019) e4005, e4005 dac.4005.

[49] C. Rametta, G. Schembra, Designing a softwarized network deployed on a fleet of drones for rural zone monitoring, Future Internet 9 (1) (2017) 1–21.

[50] S. Rao, SDN series part one: Defining software defined networking, 2014, https://thenewstack.io/defining-software-defined-networking-part-1/, (Accessed 2014).

[51] J. Bhatia, R. Dave, H. Bhayani, S. Tanwar, A. Nayyar, SDN-based real-time urban traffic analysis in VANET environment, Comput. Commun. 149 (2019) 162–175.

[52] Cisco, Software defined networking, 2013, https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/SDN/SDN.html, (Accessed 2013).

[53] S. Hassas Yeganeh, Y. Ganjali, Kandoo: A framework for efficient and scalable offloading of control applications, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 19–24.

[54] R. Ahmed, R. Boutaba, Design considerations for managing wide area software defined networks, IEEE Commun. Mag. 52 (7) (2014) 116–123.

[55] B. Heller, R. Sherwood, N. McKeown, The controller placement problem, in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 7–12.

[56] A.L. DeCarlo, The application tier of a software-defined networking architecture, 2012, https://searchnetworking.techtarget.com/feature/The-application-tier-of-a-software-defined-networking-architecture, (Accessed 2012).

[57] E. Haleplidis, Overview of RFC7426: SDN layers and architecture terminology, 2017, https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology, (Accessed 2017).

[58] ETSI, Network functions virtualisation (NFV), 2020, https://www.etsi.org/technologies/nfv, (Accessed 2020).

[59] What is network function virtualization (NFV)? 2016, https://www.blueplanet.com/resources/What-is-NFV-prx.html, (Accessed 2016).

[60] C. Tipantuña, X. Hesselbach, V. Sanchez-Agüero, F. Valera, I. Vidal, B. Nogales, An NFV-based energy scheduling algorithm for a 5G enabled fleet of programmable unmanned aerial vehicles, Wirel. Commun. Mob. Comput. 2019 (2019) 1–20.

[61] A. Leonhardt, Defining the elements of NFV architectures, 2019, https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/, (Accessed 2019).

[62] A. Shaghaghi, M.A. Kaafar, R. Buyya, S. Jha, Software-defined network (SDN) data plane security: Issues, solutions, and future directions, in: B.B. Gupta, G.M. Perez, D.P. Agrawal, D. Gupta (Eds.), Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Springer International Publishing, Cham, 2020, pp. 341–387.

[63] E.B. Eskca, O. Abuzaghleh, P. Joshi, S. Bondugula, T. Nakayama, A. Sultana, Software defined networks' security: An analysis of issues and solutions, 2015.

[64] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, F. Ahamd, Security issues in software defined networking (SDN): Risks, challenges and potential solutions, 2019.

[65] Core Networking, Software-defined networking (SDN): Layers and architecture terminology, 2014, SDN Security Attack Vectors and SDN Hardening, (Accessed 2014).

[66] J. Vora, P. DevMurari, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, Blind signatures based secured E-healthcare system, in: 2018 International Conference on Computer, Information and Telecommunication Systems, CITS, 2018, pp. 1–5.

[67] S. Gao, Z. Peng, B. Xiao, ACM, A. Hu, Y. Song, K. Ren, Detection and mitigation of DoS attacks in software defined networks, IEEE/ACM Trans. Netw. (2020) 1–15.

[68] W. Yang, C. Fung, A survey on security in network functions virtualization, in: 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, South Korea, 2016, pp. 15–19.

[69] S. Lal, T. Taleb, A. Dutta, NFV: Security threats and best practices, IEEE Commun. Mag. 55 (8) (2017) 211–217.

[70] J. Singh, A. Refaey, A. Shami, Multilevel security framework for NFV based on software dfined perimeter (SDP), IEEE Network (2020) 1–6.

[71] A.A. Ali, Virtual machine escapes, 2013.

[72] K. Jain, Security based on network topology against the wiretapping attack, IEEE Wirel. Commun. 11 (1) (2004) 68–71.

[73] M. Moradi, Software-Driven and Virtualized Architectures for Scalable 5G Networks, (Ph.D. thesis), 2018.

[74] Q. Zhao, P. Du, M. Gerla, A.J. Brown, J.H. Kim, Software defined multi-path TCP solution for mobile wireless tactical networks, in: MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 2018, pp. 1–9.

[75] N. Bindra, M. Sood, Is SDN the real solution to security threats in networks? A security update on various SDN models, Indian J. Sci. Technol. 9 (2016) 1–8.

[76] G. Secinti, P.B. Darian, B. Canberk, K.R. Chowdhury, SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks, IEEE Commun. Mag. 56 (1) (2018) 16–21.

[77] Z. Li, Y. Lu, Y. Shi, Z. Wang, W. Qiao, Y. Liu, A dyna-Q-based solution for UAV networks against smart jamming attacks, Symmetry 11 (5) (2019) 1–19.

[78] H. Sedjelmaci, S.M. Senouci, N. Ansari, A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks, IEEE Trans. Syst. Man Cybern. 48 (9) (2018) 1594–1606.

[79] M. Conti, R. Di Pietro, L. Mancini, A. Mei, Distributed detection of clone attacks in wireless sensor networks, IEEE Trans. Dependable Secure Comput. 8 (5) (2011) 685–698.

[80] S. Roy, M. Conti, S. Setia, S. Jajodia, Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact, IEEE Trans. Inf. Forensics Secur. 9 (4) (2014) 681–694.

[81] J. Ashraf, S. Latif, Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques, in: 2014 National Software Engineering Conference, Rawalpindi, Pakistan, 2014, pp. 55–60.

[82] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris, Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments, Comput. Netw. 62 (2014) 122–136.

[83] A. Wang, Y. Guo, F. Hao, T. Lakshman, S. Chen, Scotch: Elastically scaling up SDN control-plane using vswitch based overlay, in: Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies, CoNEXT '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 403–414.

[84] R. Kirichek, A. Vladyko, A. Paramonov, A. Koucheryavy, Software-defined architecture for flying ubiquitous sensor networking, in: 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, South Korea, 2017, pp. 158–162.

[85] F. Gillani, E. Al-Shaer, Q. Duan, In-design resilient SDN control plane and elastic forwarding against aggressive ddos attacks, in: Proceedings of the 5th ACM Workshop on Moving Target Defense, MTD '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 80–89.

[86] S.M. Mousavi, M. St-Hilaire, Early detection of DDoS attacks against SDN controllers, in: 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015, pp. 77–81.

[87] Y. Afek, A. Bremler-Barr, L. Shafir, Network anti-spoofing with SDN data plane, in: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1–9.

[88] R.K. Sriramulu, Constructing Dynamic Ad-hoc Emergency Networks using Software-Defined Wireless Mesh Networks, (Ph.D. thesis), 2018, pp. 1–62.

[89] M. Han, T.N. Canh, S.C. Noh, J. Yi, M. Park, DAAD: DNS Amplification Attack Defender in SDN, in: 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea (South), 2019, pp. 372–374.

[90] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, J.J.P.C. Rodrigues, Fog computing for smart grid systems in the 5G environment: Challenges and solutions, IEEE Wirel. Commun. 26 (3) (2019) 47–53.

[91] A. Kumari, R. Gupta, S. Tanwar, N. Kumar, Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions, J. Parallel Distrib. Comput. 143 (2020) 148–166.

[92] F. Rocha, M. Correia, Lucy in the sky without diamonds: Stealing confidential data in the cloud, in: 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, DSN-W, 2011, pp. 129–134.

[93] E. Kovacs, Serious vulnerabilities in linux kernel allow remote DoS attacks, 2019, https://www.securityweek.com/serious-vulnerabilities-linux-kernel-allow-remote-dos-attacks, (Accessed 2019).

[94] S. Ellinidou, G. Sharma, T. Rigas, T. Vanspouwen, O. Markowitch, J.-M. Dricot, SSPSoC: A secure SDN-based protocol over MPSoC, Secur. Commun. Netw. 2019 (2019) 4869167:1–4869167:11.

[95] A. Akhunzada, E. Ahmed, A. Gani, M.K. Khan, M. Imran, S. Guizani, Securing software defined networks: taxonomy, requirements, and open issues, IEEE Commun. Mag. 53 (4) (2015) 36–44.

[96] J. Wang, Y. Wang, H. Hu, Q. Sun, H. Shi, L. Zeng, Towards a security-enhanced firewall application for openflow networks, in: G. Wang, I. Ray, D. Feng, M. Rajarajan (Eds.), Cyberspace Safety and Security, Springer International Publishing, Cham, 2013, pp. 92–103.

[97] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Machine learning models for secure data analytics: A taxonomy and threat model, Comput. Commun. 153 (2020) 406–440.

[98] S. Shin, V. Yegneswaran, P. Porras, G. Gu, AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, Association for Computing Machinery, New York, NY, USA, 2013, pp. 413–424.

[99] Y. Zhang, An adaptive flow counting method for anomaly detection in SDN, in: Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, CoNEXT '13, Association for Computing Machinery, New York, NY, USA, 2013, pp. 25–30.

[100] R.W. Skowyra, A. Lapets, A. Bestavros, A. Kfoury, Verifiably-safe software-defined networks for CPS, in: Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, HiCoNS '13, Association for Computing Machinery, New York, NY, USA, 2013, pp. 101–110.
[101] N. Handigol, B. Heller, V. Jeyakumar, D. Maziéres, N. McKeown, Where is the debugger for my software-defined network? in: Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 55–60.
[102] S. Shirali-Shahreza, Y. Ganjali, FleXam: Flexible sampling extension for monitoring and security applications in openflow, in: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, HotSDN '13, Association for Computing Machinery, New York, NY, USA, 2013, pp. 167–168.
[103] S. Shin, G. Gu, CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?) 2012 20th IEEE International Conference on Network Protocols (ICNP), Austin, TX, USA, 2012, pp. 1–6.
[104] S. Son, S. Shin, V. Yegneswaran, P. Porras, G. Gu, Model checking invariant security properties in OpenFlow, in: 2013 IEEE International Conference on Communications (ICC), Budapest, Hungary, 2013, pp. 1974–1979.
[105] F. Xiong, A. Li, H. Wang, L. Tang, An SDN-MQTT based communication system for battlefield UAV swarms, IEEE Commun. Mag. 57 (8) (2019) 41–47.
[106] C. Priebe, D. Muthukumaran, D. O' Keeffe, D. Eyers, B. Shand, R. Kapitza, P. Pietzuch, Cloudsafetynet: Detecting data leakage between cloud tenants, in: Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, CCSW '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 117–128.
[107] B.O. Williams, M.K. Lohner, K. Harmon, J. Bower, Virtual private network (VPN)-as-a-service with delivery optimizations while maintaining end-to-end data security, Google Patents, US Patent 10, 270, 809, 2019.
[108] T. Zhang, R.B. Lee, CloudMonatt: An architecture for security health monitoring and attestation of virtual machines in cloud computing, in: 2015 ACM/IEEE 42nd Annual International Symposium on Computer Architecture (ISCA), Portland, OR, USA, 2015, pp. 362–374.
[109] F. Yao, R. Sprabery, R.H. Campbell, CryptVMI: A flexible and encrypted virtual machine introspection system in the cloud, in: Proceedings of the 2nd International Workshop on Security in Cloud Computing, SCC '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 11–18.
[110] A.S. Ibrahim, J. Hamlyn-Harris, J. Grundy, M. Almorsy, CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model, in: 2011 5th International Conference on Network and System Security, Milan, Italy, 2011, pp. 113–120.
[111] Z. Yan, P. Zhang, A.V. Vasilakos, A security and trust framework for virtualized networks and software-defined networking, Secur. Commun. Netw. 9 (16) (2016) 3059–3069.
[112] J.A. Lango, J.J. Voll, A.G. Tucker, Expansion of services for a virtual data center guest, Google Patents, US Patent 9, 535, 741, 2017.
[113] R.V. Nunes, R.L. Pontes, D. Guedes, Virtualized network isolation using Software Defined Networks, in: 38th Annual IEEE Conference on Local Computer Networks, Sydney, NSW, Australia, 2013, pp. 683–686.
[114] R. Logic, Toward a federated identity service based on virtualization, https://www.ciosummits.com/Online_Asset_Radiant_Logic_Buyers_Guide.pdf.
[115] M. Pattaranantakul, R. He, A. Meddahi, Z. Zhang, SecMANO: Towards network functions virtualization (NFV) based security management and orchestration, in: 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 2016, pp. 598–605.
[116] E. Jacob, J. Matías, A. Mendiola, V. Fuentes, J. Garay, C. Pinedo, Deploying a virtual network function over a software defined network infrastructure: Experiences deploying an access control VNF in the university of the basque country's openflow enabled facility, 2014, pp. 1–5.
[117] ETSIGS NFV-SEC 009, Network functions virtualisation (NFV); NFV security; report on use cases and technical approaches for multi-layer host administration, 2015, https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/009/01.01.01_60/gs_nfv-sec009v010101p.pdf, (Accessed 2015).
[118] T. Tuzel, M. Bridgman, J. Zepf, T.K. Lengyel, K. Temkin, Who watches the watcher? Detecting hypervisor introspection from unprivileged guests, Digit. Investig. 26 (2018) S98 – S106.
[119] E. Siebert, Virtual network security best practices, 2010, https://searchservervirtualization.techtarget.com/tip/Virtual-network-security-best-practices, (Accessed 2010).
[120] IETF, Building blocks towards a trustworthy NFV infrastructure, 2015, https://www.ietf.org/proceedings/93/slides/slides-93-nfvrg-21.pdf, (Accessed 2015).
[121] S. Tanwar, A. Kumari, S. Tyagi, N. Kumar, Verification and validation techniques for streaming big data analytics in internet of things environment, IET Netw. (2018).
[122] M. FanJiao, Z. Jiamin, Y. Xiao, Z. Changyou, T. Yu-An, A high efficiency encryption scheme of dual data partitions for android devices, in: 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing, Vol. 1, EUC, Guangzhou, China, 2017, pp. 823–828.
[123] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R.M. Parizi, K.-K.R. Choo, Fog data analytics: A taxonomy and process model, J. Netw. Comput. Appl. 128 (2019) 90–104.
[124] G.S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, R. Buyya, BlockSDN: Blockchain-as-a-service for software defined networking in smart city applications, IEEE Netw. 34 (2) (2020) 83–91.
[125] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009.
[126] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges, Mech. Syst. Signal Process. 135 (2020) 106382.
[127] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D.H. Nyang, D. Mohaisen, Exploring the attack surface of blockchain: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020) 1.
[128] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, T.-Y. Ni, A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption, in: K. Arai, R. Bhatia (Eds.), Advances in Information and Communication, Springer International Publishing, Cham, 2020, pp. 988–1003.
[129] R. Gupta, S. Tanwar, N. Kumar, S. Tyagi, Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review, Comput. Electr. Eng. 86 (2020) 106717.
[130] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inf. Secur. Appl. 50 (2020) 102407.
[131] J. Hathaliya, P. Sharma, S. Tanwar, R. Gupta, Blockchain-based remote patient monitoring in healthcare 4.0, in: 2019 IEEE 9th International Conference on Advanced Computing, IACC, 2019, pp. 87–91.
[132] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, S.W. Kim, Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges, IEEE Access 8 (2020) 24746–24772.
[133] H. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: A survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.
[134] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for industry 4.0: A comprehensive review, IEEE Access (2020) 1.
[135] I.G.-M. no, R. Lacuesta, M. Rajarajan, J. Lloret, Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain, Ad Hoc Netw. 86 (2019) 72–82.
[136] S. Aggarwal, M. Shojafar, N. Kumar, M. Conti, A new secure data dissemination model in internet of drones, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1–6.
[137] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P.K. Singh, W. Hong, A survey on decentralized consensus mechanisms for cyber physical systems, IEEE Access 8 (2020) 54371–54401.
[138] U. Bodkhe, S. Tanwar, Secure data dissemination techniques for IoT applications: Research challenges and opportunities, Softw.- Pract. Exp. n/a (n/a) 1–23.
[139] A. Kuzmin, E. Znak, Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles, in: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 2018, pp. 32–37.
[140] K. Lei, Q. Zhang, J. Lou, B. Bai, K. Xu, Securing ICN-based UAV ad hoc networks with blockchain, IEEE Commun. Mag. 57 (6) (2019) 26–32.
[141] T. Alladi, V. Chamola, N. Sahu, M. Guizani, Applications of blockchain in unmanned aerial vehicles: A review, Veh. Commun. 23 (2020) 100249.
[142] W. Li, W. Meng, Z. Liu, M.-H. Au, Towards blockchain-based software-defined networking: Security challenges and solutions, IEICE Trans. Inf. Syst. E103.D (2020) 196–203.
[143] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, Q. Zhang, K.R. Choo, An energy-efficient SDN controller architecture for IoT networks with blockchain-based security, IEEE Trans. Serv. Comput. (2020) 1.
[144] S. Banerjee, V. Odelu, A.K. Das, S. Chattopadhyay, N. Kumar, Y. Park, S. Tanwar, Design of an anonymity-preserving group formation based authentication protocol in global mobility networks, IEEE Access 6 (2018) 20673–20693.
[145] S. Tanwar, S. Tyagi, I. Budhiraja, N. Kumar, Tactile internet for autonomous vehicles: Latency and reliability analysis, IEEE Wirel. Commun. 26 (4) (2019) 66–72.
[146] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions, IEEE Network 33 (6) (2019) 22–29.
[147] J. Vora, S. Kaneriya, S. Tanwar, S. Tyagi, N. Kumar, M. Obaidat, TILAA: Tactile internet-based ambient assistant living in fog environment, Future Gener. Comput. Syst. 98 (2019) 635–649.
[148] S. Boukria, M. Guerroumi, I. Romdhani, BCFR: Blockchain-based controller against false flow rule injection in SDN, in: 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1034–1039.
[149] SDN controllers, 2018, http://flowgrammable.org/sdn/ecosystem/#tab_controller, (Accessed 2018).
[150] M. Fakoorrad, Thesis: Application layer of software defined networking- pros and cons in terms of security, 2018, , (Accessed 2018).

[151] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P.K. Singh, W. Hong, Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward, IEEE Access 8 (2020) 474–488.

[152] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, N. Kumar, Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw. Sci. Eng. (2019) 1.

[153] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, J.J.P.C. Rodrigues, BHEEM: A blockchain-based framework for securing electronic health records, in: 2018 IEEE Globecom Workshops, GC Wkshps, 2018, pp. 1–6.

[154] P. Fernando, J. Wei, Blockchain-powered software defined network-enabled networking infrastructure for cloud management, in: 2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1–6.

[155] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, A. Meddahi, NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3330–3368.

[156] M. Casoni, C.A. Grazia, M. Klapez, SDN-based resource pooling to provide transparent multi-path communications, IEEE Commun. Mag. 55 (12) (2017) 172–178.