# Privacy-Preserving and Security in SDN-based IoT

## A Survey

Ahmadvand, Hossein; Lal, Chhagan; Hemmati, Hadi; Sookhak, Mehdi; Conti, Mauro

**DOI**
10.1109/ACCESS.2023.3267764

**Publication date**
2023

**Document Version**
Final published version

**Published in**
IEEE Access

**Citation (APA)**
Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-Preserving and Security in SDN-based IoT: A Survey. *IEEE Access*, *11*, 44772-44786. https://doi.org/10.1109/ACCESS.2023.3267764

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 March 2023, accepted 11 April 2023, date of publication 17 April 2023, date of current version 11 May 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3267764*

SURVEY

# Privacy-Preserving and Security in SDN-Based IoT: A Survey

**HOSSEIN AHMADVAND[1], CHHAGAN LAL[2], HADI HEMMATI[1,3], MEHDI SOOKHAK[4], (Senior Member, IEEE), AND MAURO CONTI[2,5], (Fellow, IEEE)**

[1]University of Calgary, Calgary, AB T2N 1N4, Canada
[2]Delft University of Technology (TU Delft), 2628 CD Delft, The Netherlands
[3]York University, Toronto, ON M3J 1P3, Canada
[4]Texas A&M University-Corpus Christi, Corpus Christi, TX 78412, USA
[5]University of Padua, 35122 Padua, Italy

Corresponding author: Hossein Ahmadvand (hossein.ahmadvand@ucalgary.ca)

**ABSTRACT** In recent years, the use of Software Defined Networking (SDN) has increased due to various network management requirements. Using SDN in computer network applications has brought several benefits to users, including lower operational costs, better hardware management, flexibility, and centralized network deployment. On the other hand, the Internet of Things (IoT) is another rapidly growing technology. Distributed and dynamic infrastructures are two critical characteristics of IoT. These characteristics lead to some challenges while using SDN in IoT in terms of security and privacy. In this paper, we address security and privacy issues and solutions for SDN-based IoT systems. We analyze the techniques used for defense in previous works to achieve an acceptable level of security and privacy protection in SDN-based IoT systems. In the data plane, SDN-based IoT papers have considered hashing and encryption techniques, in the control plane, certificate authority and access control have been analyzed, and in the application plane, attack detection, and authentication have been discussed. We also provide a statistical analysis of the existing work. This analysis shows that researchers have focused on certain areas more than others in recent years. The final analysis also highlights issues that previous researchers have ignored.

**INDEX TERMS** Software-defined network, privacy-preserving, security, cloud computing.

## I. INTRODUCTION

Due to the new requirements for networks, such as network programmability, logical centralization of intelligence and control, network abstraction, and openness, the use of SDNs has increased dramatically. This technology adds dynamism to the network architecture. SDN abstracts network functions to virtualize or control them through software. SDN combines the operational part (operating system and software) with the existing role of deciding the destination of the traffic. This is done with a lower-level system that is mainly composed of different hardware. SDNs, through their dynamic management, allow users to be more agile in their applications and activities in a virtualization environment. This approach can provide benefits such as flexibility, scalability, redundancy, and less hardware to manage powerful cloud computing systems. By using SDN, users can add flexibility to their operations and architecture. This is especially important regarding the system architecture in IoT, due to limited resources and distributed infrastructure. Also, with the widespread use of IOT applications and the use of SDN in them, this issue has become more important. Due to the software design and various applications used in this field, security, and privacy challenges are essential in SDN-based IoT. Therefore, in this article, we provide an overview of the research in the field of security and privacy in SDN-based IoT. To this end, we present the following contributions in this article.

- Presenting the main categories of previous works on the security and privacy of SDN-based IoT systems. Existing surveys for SDN-based IoT, dealing with

The associate editor coordinating the review of this manuscript and approving it for publication was Renato Ferrero.

security attacks, using blockchain for security and privacy, and various deep learning techniques for security and privacy are among our categorizations. The important thing about these works is that, in addition to security and privacy, they consider important aspects of IoT (limitation of processing resources, distribution, limited power consumption, and the existence of a deadline for the completion of processes). Based on these categories, the researcher can find the main exciting research direction.

- Presenting a categorization of previous work based on the different layers of SDNs in IoT systems. In SDN-based IoT, due to the nature of IoT processing and its applications, the controller and data layers differ from other SDN-based systems in addition to the application layer. In each layer, we analyze the work done and show the future directions of research.
- Presentation of the main techniques used in previous works. The common denominator of these techniques is that they consider the constraints of resources and their distribution in the IoT. One of these techniques is the use of blockchain to record transactions. Since IoT systems are decentralized, this solution helps increase the level of security and privacy. Due to the severe resource constraints in SDN-based IoT, some work have also been done to detect and reduce the impacts of denial-of-service attacks using deep learning techniques. These techniques could be further extended by researchers. We also explain the advantages and disadvantages of each technique.

First, in Section III, we divide the existing work into some categories based on considered issues. In Section III, we present various works based on the target layers. In Section IV, we discuss the statistical discussions and the number of existing works based on the publication year, scope, and topic. We examined the articles mentioned in this survey and examined them from different aspects in Section V. In section VI, we summarize the issues raised in the article and presented existing directions for future research.

## II. BACKGROUND

In this section, in the first sub-section (II-A), we will examine the market size of SDN and the Internet of Things. In the second subsection (II-B), we introduce and review the technologies mentioned in this article.

### A. ANALYSIS IN SDN AND IoT MARKET SIZE

One of our motivations for preparing this article is the rapid growth of the SDN and IOT market size. Fig. 1 and Fig. 2 show the significant growth of SDNs and the size of the IoT market, respectively. Due to the advantages that this technology brings, its use is increasing rapidly, especially in the IoT sector. SDNs are also being deployed to meet different requirements in various other applications, including vehicular networks, healthcare applications, and other critical applications.

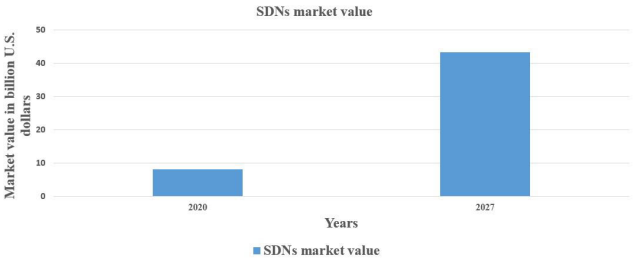


**FIGURE 1.** SDN market size in 2020 and 2027 (worldwide) [1].

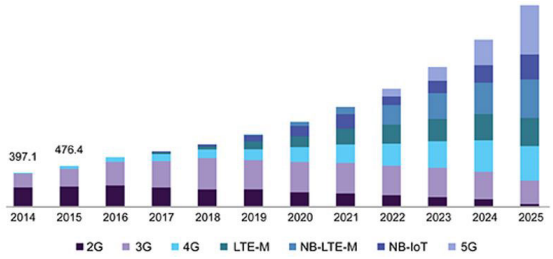


**FIGURE 2.** U.S. cellular IoT Market, by type, 2012-2025 (USD Million) [2].

### B. TECHNOLOGIES AND CONCEPTS

We are dealing with technologies and new numerous concepts in this article. In this section, we introduce The IoT, blockchain, and the difference between security and privacy.

#### 1) INTERNET OF THINGS

The Internet of Things is a term used to describe the billions of devices connected to the Internet around the world. These devices are connected thanks to the many small computers embedded in them and have the ability to send and receive information [3], [4], [5], [6].

One of the most important features of the IoT is the limitation of processing resources. IoT data processing usually is needed at the edge. Devices that are at the edge usually are kind of embedded systems. Embedded systems have low and limited processing power. For this reason, some solutions should be found to perform complex and heavy IoT processing at the edge [7], [8], [9], [10], [11], [12].

#### 2) BLOCKCHAIN

Blockchain is a technology that enables the secure sharing of information. Data, obviously, is stored in a database. Transactions are recorded in an account book called a ledger. A blockchain is a type of distributed database or ledger—one of today's top tech trends—which means the power to update a blockchain is distributed between the nodes, or participants, of a public or private computer network. This is known as distributed ledger technology or DLT. Nodes are incentivized with digital tokens or currency to make updates to blockchains. Bitcoin is the first application of this technology, but this revolutionary technology can be used for any system that needs to reduce trust in intermediaries and third parties [13], [14], [15], [16], [17].

#### 3) THE DIFFERENCE BETWEEN SECURITY AND PRIVACY

In this article, we will explore the issues of security and privacy in an SDN-based IoT system. In this section, we will define the difference between these two concepts. Security prevents unauthorized access to data [18], [19], [20].

- Security prevents unauthorized access to data. While privacy is concerned with protecting users' identifiable information.
- Security protects all data at all levels. Privacy, on the other hand, protects the sensitive data of individuals and organizations (leading to their identification).
- Security can be achieved without privacy. Privacy cannot be achieved without security.

## III. CATEGORIES OF EXISTING WORKS IN SECURITY AND PRIVACY OF SDN-BASED IoT

In this section, we present existing studies in the area of SDN-based IoT security and privacy. We have divided the existing work in this area into below categories: Surveys on security and privacy issues in SDN-based IoT, DDoS issues in SDN-based IoT, the use of blockchain in SDN for security and privacy issues, the use of deep learning techniques to increase the level of privacy and security in SDN, and other topics related to SDN-based security and privacy.

The reason for this classification of subjects is the number of articles on these subjects. By reviewing the articles published in the field of privacy and security in SDN-based IOT applications, we concluded that the articles in this field with the mentioned positions have the largest number. These topics are not limited to the type of attacks (such as DDoS) or the type of attack prevention (such as blockchain) or the type of attack detection (using deep learning solutions). Rather, the general approach of existing articles in the field of privacy and security in SDN-based IOT applications.

We first examine existing studies to show how our work differs from them. Since processing resources in SDN-based IoT are severely limited, DoS and DDoS attacks can cause great damage to these systems. For this reason, much work has been done on this topic. We have also studied this category and investigated these works. In this article, we have examined several works in this area. Deep learning techniques are widely used to detect suspicious threats to security and privacy. However, due to limited resources in SDN-based IoT systems, special considerations should be made for the use of deep learning. Finally, we take a look at other issues that have been addressed in the area of security and privacy of SDN-based IoT systems.

### A. SURVEYS ON SDN SECURITY AND PRIVACY ISSUES

In this section, we look at work that addresses security and privacy in SDN-based IoT. Most of these works only address the security issues of SDN-based IoT.

The authors in [29] and [30] considered the three layers of SDNs, the data plane, the control plane, and the application plane. In each layer, they have analyzed the existing vulnerabilities and risks. They have concluded that the greatest risks are in the control plane. Various vulnerabilities and cyberattacks are examined in [31]. The authors also present the defense approaches and solutions to these vulnerabilities. The authors in [21] have presented several existing vulnerabilities and potential attacks in the IoT domain. They have concluded that SDN security plays a very important role in the security of IoT. They have presented the various open areas to enhance the approach to SDN security.

Various DDoS attacks in SDN were analyzed in [32], [33], [34], and [35]. Researchers mentioned that SDN could fall victim to such attacks due to its centralization. Referece [36] has divided SDN security into two areas: control and data. The researchers focused on the data area in their paper. The authors divided DDoS detection techniques into a few categories: Machine Learning, Traffic Analysis, and Connection Analysis in [22].

The authors in [26] have analyzed various attacks in all layers of SDN. They have considered attack types such as network tampering, data leakage, DDoS attacks, and unauthorized applications. Different attack types and anomaly detection in three SDN layers were presented in [37]. The authors in [27] divided the attack types such as switch and controller resource saturation, control and data channel saturation, east-west channel saturation, and north channel saturation into three layers of SDNs. In [38], flow graph, traffic analysis monitoring, and IP-MAC address monitoring-based solutions are used to overcome SDN ARP cache poisoning attacks. In [39], the authors used an advanced support vector machine method to detect two flooding-based DDoS attacks. In [40], the authors classified existing DoS/DDoS models in SDN. They consider three layers, including the protocol, device resources, and the network, for their analysis of the damage caused by Dos/DDoS attacks in three layers. The protocol, device, and network layers include Transmission Control Protocol-TCP, bandwidth, CPU, storage, and infection and recovery time. In [36], the authors consider the data plane environment and analyze a stateful SDN-based system. They presented the impact and range of impact for existing vulnerabilities. [24] have considered blockchain as the main way to make SDN environments secure and private. They discuss the advantages and disadvantages of using Blockchain.

#### 1) THE DIFFERENCE BETWEEN OUR WORK AND EXISTING WORKS

In this article, we do not address security and privacy issues in SDN in general. We address security and privacy issues in SDN-based IoT systems. Due to the limited processing resources in IoT, the DOS attack is essential. This type of attack can exacerbate the problem of limited processing resources. The limitation of processing resources also prevents us from using complex algorithms such as deep learning techniques to ensure security and privacy. Since the distributed architecture of IoT, the use of blockchain can increase the level of privacy and security in IoT applications.

**TABLE 1. Existing surveys in security and privacy of SDN-based IoT and the difference between our work and them.**

| Paper | Data plane | Control plane | Application plane | Security | Privacy | Description | Differences with our work |
|---|---|---|---|---|---|---|---|
| [21] | x | x | x | ✓ | ✓ | A survey on using SDN and NFV for IoT security | This article examines securing techniques in SDN and NFV and their use in IoT. We review previous works in the field of security and privacy in SDN-based IoT. We do not address security and privacy issues in IoT |
| [22] | ✓ | x | x | ✓ | x | Categorization of DDoS attacks | We address security and privacy issues on IoT-based SDN systems including DDoS. |
| [23] | x | x | x | ✓ | x | The authors have addressed DoS and DDoS in the IoT. | We address all security and privacy issues in IoT-based SDN systems, including DDoS. |
| [24] | x | x | x | ✓ | ✓ | A survey on using blockchain in SDN | We address all security and privacy issues on IoT-based SDN systems including blockchain. |
| [25] | x | x | x | ✓ | x | Leveraging Blockchain in Vehicle IoT Environment to Achieve Desirable Level of Security | We address all security and privacy issues in IoT-based SDN systems, including vehicle networks and Blockchain. |
| [26] | ✓ | ✓ | ✓ | ✓ | x | Manipulation of the network, data leakage, DDoS attack, and unauthorized application | We have examined the security and privacy in SDN-based IoT. |
| [27] | ✓ | ✓ | x | ✓ | x | Resource saturation of switch and controller, control, and data channels | This is one of the topics we are working on. Our work is more general about security and privacy in SDN-based IoT |
| [28] | x | x | x | ✓ | ✓ | general survey on SDN-based IoT | This article deals with security and provision superficially and ignores the details. We only focus on security and privacy issues. We cover aspects of security and privacy in IoT. |
| Our work | ✓ | ✓ | ✓ | ✓ | ✓ | We present a survey on security and privacy issues in SDN-based IoT systems. We consider the main problem and solutions in the security and privacy of SDN-based IoT. We consider issues related to the limitation of the resources in SDN-based IoT in previous works. | NA |

Due to these differences, in addition to general security and privacy issues, we focus on the above issues and explore them in SDN-based IoT systems. We have also compared our work with other surveys in this area in Table 1.

### B. ATTACK ISSUES IN SDN-BASED IoT

One of the major security issues in SDN-based IoT is the DoS and DDoS attacks. Due to the limitation of resources in SDN-based IoT, DDoS causes major problems, especially in the SDN controller layer. This type of attack wastes system resources. This problem is especially important in IoT, where processing resources are limited. For this reason, we review the previous works in this area as a dedicated subsection, here. In [41], researchers address a variety of issues related to the use of SDN in the vehicular network. Security is one of the important issues that researchers have addressed. SDN-based security for Ship-IoT has been considered in [42]. In [23], the researchers have described a stateful SDN solution that can detect and mitigate DoS and DDoS attacks in IoT networks. Their approach has a great impact on reducing the terrific data plane in SDN-Based IoT. In [43] the authors have considered DDoS attacks in IoT environments. They have analyzed and classified the various existing approaches and tools in this area. They clarified the open direction and issues for future studies. The authors in [44] present an approach for detecting the DDoS attack on SDN. This method is based on collecting data and analyzing the type of traffic. In this analysis, data entropy is considered. In [45], the authors have presented an approach including analysis of the IP and traffic anomaly behaviors to detect DDoS attacks. In [46], The destructive effect of the DDoS attack on the controller layer in SDN and the extent of violations in the performance of the entire SDN system are investigated. Reduction of damage and defending against the DDoS attack has been considered in [47]. The authors have presented a low-cost approach to reducing the controller's overhead. This solution allows the user to respond to the attack in real time. The authors in [48] have presented a multi-layer classifier that detects the DDoS attack. This multi layers classifier used Support Vector Machine (SVM) for classification.

In [23], the authors have used an approach to detect and prevent DDoS attacks. They have used an extension of OpenFlow. This extension can detect and prevent malicious packets in switches and prevent sending them to the control panel. [49] presents the security issues in software-defined wireless networking. This work [50] has used SDN for detecting and defending DDoS attacks in the IoT environment. The idea of this paper is to integrate controllers including SDN controllers. By using this approach, the operator can monitor and apply the detection and defense algorithm easier. In [51], the researchers have presented an approach to detect malicious traffic to overcome the problem of DDoS attacks. In this approach, the SDN's controller analysis the session IPs and their payload. This approach can analyze large volume traffic that is generated by IoT devices. Security of IoT environment has been considered in [52]. The authors have limited access to IoT devices via the network. They also have used an approach for the authentication of IoT devices. For using this approach, the authors have added a lightweight layer to the IoT system. This approach can prevent malicious IoT devices from to adding the network. In table 2, we compare the works done in the field of DoS and DDoS.

### C. USING BLOCKCHAIN IN SDN FOR SECURITY AND PRIVACY ISSUES

One of the most important technologies based on the blockchain platform is cryptocurrency. Due to distributed architecture of blockchain, it is a good candidate for the IoT environment. In this section, we examine the use of blockchain in creating privacy and security in SDN.

In [53], the researcher established an approach for routing in cluster IoT-based SDN using blockchain. By this approach, they can increase the privacy level of SDN. One of the uses of the blockchain is to record interactions as evidence for future use. Another advantage of blockchain is its use in authentication. In [54] proposes a decentralized access control mechanism based on blockchain for SDN-based IoT. In [55] a combination of blockchain and SDN has been considered. The authors also have considered the important challenges for IoT processing including energy consumption and real-time processing. This approach is a suitable approach to use in smart cities due to the considering functional techniques, security, and privacy issues. The authors in [56] have used the blockchain for data management and saving transactions and records in IoT clusters. In recent years, the use of blockchain for privacy-preserving and improving the level of security in SDN has increased. The authors in [24] have surveyed various works in the area of using blockchain in SDN. They have predicted that due to the rapid development of using blockchain in industry and economy, using blockchain in technologies like SDN will grow significantly.

The current communication channel between IoT devices is unencrypted. This issue caused serious vulnerabilities in data transfer between IoT and cloud devices. In [57], the authors suggest using the blockchain to deal with this issue, so that the data is encrypted using the blockchain and vulnerabilities are prevented. The current vehicular IoT environment is insecure since a compromised vehicle can go undetected and spread incorrect road information. Due to the critical applications and real-time processing in vehicular networks, this issue has a great impact on the functionality of the vehicular network. The researcher in [25] has considered this issue and suggested using blockchain to overcome it. The authors in [58] have used a combination of SDN and distributed blockchain to improve the security level of IoT. The authors in [59] have used threat prevention, data protection, and access control, and mitigate network attacks such as cache poising/ARP spoofing, DDoS/DoS attacks, and detect security threats for large-scale SDN-based IoT systems.

Lack of trust between different vendors has been considered in [60]. The Authors have tried to resolve this issue by using blockchain in the SDN structure. The current SDN architecture is insecure and vulnerable and lacks data privacy, authentication, and availability. combining the SDN and blockchain can improve the level of trust and security between different nodes [61]. Blockchain nodes are insecure, especially in the public Blockchain network. Some novel approach has been presented in [62], [63], and [64] for using SDN in blockchain for filtering the packets, NS amplification attack in the private Blockchain, and adding the efficient capability of handling a group of sub-flows together. The proposed approach in [65], has used smart contracts to improve the security and privacy of SDN-based IoT. The authors have used a public blockchain using Ethereum. The main objective of [66] is to use a Cyber Threat Intelligence (CTI) sharing platform based on a private blockchain. By this Cyber Threat Intelligence sharing, this approach can reduce the impact of attacks. A secure IoT architecture based on the blockchain is presented in [67]. By using this approach, the security, performance, and functionality of Network Function Virtualization (NFV) and SDN will increase. Energy-aware and blockchain-based architecture have been presented in [55]. Due to the features of this approach, it can be used in IoT applications like smart cities. Using blockchain causes removing the single point of failure. In this paper [68], the authors propose that in an SDN-based IoT network, the identities, public keys, and trust indices of IoT devices, can be stored on a blockchain to ensure immutability and tamper-resistance.

This paper [69] proposes a lightweight blockchain-based authentication mechanism where ordinary sensors' credentials are stored. This lightweight approach is implemented in SDN's controller. The authors have considered the limitation of IoT processing capabilities and energy consumption. The authors in [70] utilize two emerging technologies blockchain and SDN as a sustainable solution. They have used transaction records to improve the level of privacy and security in the SDN environment. This paper [71] presents an approach to using blockchain for distributed control strategy and network attack detection. Blockchain-based multi-controller architecture has been in [72] for SDN-based networks. One master controller and multiple redundant controllers are assigned to

**TABLE 2.** Comparison of the existing works on security and privacy of SDN-IoT (Dos&DDoS).

| Paper | Data plane | Control plane | Application plane | Security | Privacy | Description |
|---|---|---|---|---|---|---|
| [23] | x | ✓ | x | ✓ | ✓ | Mitigate DoS and DDoS attacks in IoT networks |
| [41] | x | x | x | ✓ | x | Security of SDN in the vehicular network |
| [42] | x | x | x | ✓ | x | SDN-based security for Ship-IoT |
| [43] | x | x | x | ✓ | x | DDoS attack mitigation strategies featured by SDN technologies |
| [44] | ✓ | x | x | ✓ | x | Analysis the data to detect and mitigate DDoS |
| [45] | ✓ | x | x | ✓ | x | Analysis the IPs and traffic to detect and prevent DDoS |
| [46] | x | ✓ | x | ✓ | x | Performance monitoring for detect DDoS |
| [47] | x | ✓ | x | ✓ | x | Low overhead approach to detect DDoS |
| [48] | ✓ | x | ✓ | ✓ | x | Traffic classification to detect DDoS |
| [49] | x | x | x | ✓ | x | security issues in Software defined wireless networking |
| [50] | x | ✓ | x | ✓ | x | Detect DDoS attack in controller |
| [51] | ✓ | | ✓ | ✓ | | Detect malicious IPs and traffic |
| [52] | ✓ | | | ✓ | ✓ | Prevent DDoS by enable authentication |

**TABLE 3.** Comparison of the existing works on security and privacy of SDN-IoT (blockchain).

| Paper | Data plane | Control plane | Application plane | Security | Privacy | Description |
|---|---|---|---|---|---|---|
| [53] | ✓ | ✓ | x | ✓ | x | Secure routing in cluster IoT-SDN by using blockchain |
| [54] | x | ✓ | ✓ | ✓ | ✓ | Secure access control by blockchain in IoT-SDN |
| [55] | x | x | ✓ | ✓ | ✓ | energy-aware secure IoT-SDN-based on blockchain |
| [56] | x | x | x | x | x | record the transactions in blockchain in IoT-SDN environment |
| [57] | x | x | x | ✓ | ✓ | Secure communication channel between IoT devices and the cloud using Blockchain |
| [58] | x | x | x | ✓ | x | Botnet prevention system for IoT-SDN and Distributed Blockchain |
| [59] | ✓ | ✓ | x | ✓ | x | General solution for security in SDN for large scale IoT systems |
| [60] | x | x | x | ✓ | ✓ | Improving level of trust between different vendors by using blockchain for SDN solutions |
| [61] | x | x | x | ✓ | ✓ | Improving level of trust between different nodes by using blockchain for SDN solutions |
| [62] | x | x | x | ✓ | ✓ | Improving level of security in blockchain by using SDN in its network for filtering the packets |
| [63] | x | x | x | ✓ | ✓ | Using SDN to prevent DNS amplification attack in the private Blockchain |
| [64] | x | x | x | ✓ | ✓ | Using SDN to add the efficient capability of handling a group of sub-flows together |
| [65] | x | ✓ | ✓ | ✓ | ✓ | using smart contract in IoT-SDN to provide security and privacy |
| [66] | ✓ | ✓ | ✓ | ✓ | ✓ | Cyber Threat Intelligence sharing platform based on a private blockchain |
| [67] | x | x | ✓ | ✓ | x | secure IoT-SDN-NFV architecture based on the blockchain |
| [68] | x | ✓ | ✓ | ✓ | x | Using blockchain for identification and sharing the public key in IoT-SDN |
| [69] | x | ✓ | ✓ | ✓ | x | resource limitation aware approach for authentication in IoT-SDN |
| [70] | x | ✓ | ✓ | ✓ | ✓ | record the transaction in blockchain in IoT-SDN |
| [71] | x | x | x | ✓ | ✓ | energy aware and distributed approach based on the blockchain to increase the security and privacy |
| [72] | ✓ | ✓ | ✓ | ✓ | ✓ | using blockchain to make redundancy and increase the level of security and privacy |

each SDN domain. They have used a blockchain where the master controller creates blocks of network flow updates, and redundant controllers validate the blocks.

In table 3 we have compared the researchers that used blockchain in their approaches.

### *D. USING DEEP LEARNING FOR IMPROVING THE SECURITY AND PRIVACY IN SDN-IoT*

The use of deep learning in improving privacy and security has grown exponentially in recent years. The use of machine learning is used to identify anomalies, intrusions, and other destructive factors. The use of deep learning in the SDN-based IoT environment is complex. Processing resources in the IT environment are very limited. In contrast, deep learning is a very heavy and complex process. For this reason, appropriate solutions should be found to use deep learning in this environment.

Machine learning and deep learning approaches for intrusion detection and monitoring the vulnerabilities are presented in [73]. The authors in [74] present an approach for

selecting optimal processing resources without any reduction in the result. Due to the limited processing resources in IoT, one of the most important issues in the IoT processor is deep learning. An SDN-based framework for processing deep learning techniques in IoT is presented in [75]. Their SDN-enabled, hybrid DL-driven architecture is proposed to protect the IoT environment against malware and cyberattacks, i.e., DDoS, brute-force, bot, and infiltration. In [76], the authors present an approach for communicating between the controllers and switches in the SDN-based networks to increase performance and usability. A deep learning approach for intrusion detection and prevention system against brute-force and distributed DDoS attacks and malicious packets in SDN has been presented in [77]. In [78], the author has considered increasing the capabilities in terms of privacy preservation. They have used deep learning approaches to utilize the more sensitive data to reduce their risk. Deep learning techniques are used in [79]. the authors have used resource-constrained aware deep learning approaches to detect threats and attacks. These approaches are a good candidates for the IoT environment due to their awareness of the limitation of resources. The authors in [80] have used a deep learning approach for classification to detect anomaly detection in an IoT environment. Due to resource limitation awareness, this approach can be used in IoT devices. The authors in [81] have employed A deep learning approach to detect and mitigate the malware in a medical IoT environment based on the SDN. The authors in [82] have used deep learning techniques like RNNs (recurrent neural networks) and LSTM (long short-term memory) to detect and reduce the impact of DDoS in SDN controllers. We have compared the works in deep learning concepts in SDN-IoT in table 4.

### E. OTHER ISSUES IN PRIVACY AND SECURITY OF SDN-IoT

The use of SDN in various IoT applications is widespread. One of important IoT applications in which the use of SDN is the vehicular network. Due to the large number of security applications in vehicular networks and the need for real-time processing, privacy and security in this application are of great importance. The use of SDN in other IoT applications such as smart cities and smart homes is also very common. In this section, we will discuss other issues related to privacy and security in IoT-SDN including smart cities and homes, energy-aware architecture, and edge-fog architecture of SDN-based IoT. The authors in [83] consider the VANET environment for analysis of existing security threads in SDN-based architecture. The authors in [84] have considered energy efficiency for detecting the anomalies. They have considered a dynamic strategy selection and lightweight detection module. Because we face limited resources in IoT. This solution can be used in an IT processing environment. In [85], SDN-based fog computing is presented for vehicular computation. This architecture considers critical functionalities of the vehicular network includes: vehicle-to-vehicle and vehicle-to-infrastructure communications. Smart grids and smart homes are important parts of the IoT ecosystem. Privacy preserving in an SDN-based smart grid is considered in [86] and [87]. These papers consider privacy in communication, authentication, and data aspects. The authors in [88], [89], and [90] consider using SDN architecture to reduce energy consumption in smart cities and industries. In [91] the authors, establish hybrid proactive defense mechanisms combining moving target defense techniques with cyber deception to spread camouflage information to confuse attackers. Based on these mechanisms, they introduce a defender-led signaling game model to formalize defense scenarios and depict the interactions between the defender and the attacker. Anomaly behavior detection of various applications in IoT has been considered in [92]. The authors have analyzed distributed rules in SDNs to find their relationship and impact. Abnormal detection in various IoT applications including smart homes, healthcare, and other application in IoT has been considered in [93]. The authors detect and reduce the impacts of attacks in the IoT environment by using SDNs. In this article [94], the authors have presented an architecture to be used in SDN-based IOTs to prevent unusual traffic. The authors in [95] have considered traffic management in an IoT environment. The authors predict and manage malicious traffic in IoT gateways. The combination of fog and SDN in IoT to meet the security requirements has been considered in [96]. Smart homes are one of the important applications of the Internet of Things. There are many sensors in these houses. The Internet of Things is used to connect these sensors. For this reason, issues related to security and privacy become important in this type of application. This article [97] examines the work done in the field of security and privacy of SDN-based IOT in smart homes. A roadmap to smart homes security-aided SDN and ML has been presented in [98]. This article [99] also considers the same approach in the field of smart health applications and edge processing for smart health. We have presented other previous works in the field of security and privacy in SDN-IoT in table 5.

## IV. SDN LAYERS AND INTERFACES

In this section, we will categorize previous works based on the SDN layers.

Major previous works in this area have considered SDNs into the following three categories: data plane, control plane, and application plane, and considered some techniques in these layers. Fig. 3 presents three layers of SDNs and related vulnerabilities of each of them [100], [101], [102].

#### 1) DATA PLANE

This Layer aligns with the controller rules and routes the packets. Data plane includes physical devices and infrastructure-related network [101], [103], [104], [105]. In [106], the authors examine the security issues in the SDN data layer. They have drawn the community's attention to solving security issues in the data layer.

The authors in [107] have analyzed the new multi-hop link (MHL) fabrication attack and its prevention approach in

**TABLE 4.** Comparison of the existing works on security and privacy of SDN-IoT (Deep Learning).

| Paper | Data plane | Control plane | Application plane | Security | Privacy | Description |
|---|---|---|---|---|---|---|
| [73] | ✓ | ✓ | ✓ | x | x | Intrusion detection and monitoring the vulnerabilities |
| [74] | ✓ | ✓ | x | ✓ | x | security aware approach for using deep learning to select suitable processing resource in IoT-SDN environment |
| [75] | ✓ | ✓ | ✓ | ✓ | x | a framework for processing deep learning in IoT-SDN |
| [76] | ✓ | ✓ | x | ✓ | x | communication between controller and switches |
| [77] | ✓ | ✓ | ✓ | ✓ | x | using deep learning to detect and prevent the malicious packets, brute-force, and DDoS |
| [78] | ✓ | ✓ | ✓ | x | ✓ | using deep learning approach for authentication process for increasing the level of privacy |
| [79] | ✓ | ✓ | ✓ | ✓ | x | resource limitation aware approach based on deep learning in IoT-SDN |
| [80] | ✓ | ✓ | ✓ | ✓ | x | using deep learning to detect and classify the anomalies |
| [81] | ✓ | ✓ | ✓ | ✓ | x | deep learning approach to detect and mitigate the malware in medical IoT environment based on the SDN |
| [82] | ✓ | ✓ | ✓ | ✓ | ✓ | using deep learning approaches to detect and reduce the impact of DDoS in SDN controller |

**TABLE 5.** Comparison of the existing works on security and privacy of SDN-IoT (other).

| Paper | Data plane | Control plane | Application plane | Security | Privacy | Description |
|---|---|---|---|---|---|---|
| [83] | ✓ | ✓ | ✓ | ✓ | ✓ | Consider the VANET environment for analysis of existing security thread in SDN-based architecture |
| [84] | ✓ | ✓ | ✓ | ✓ | x | Energy aware approach to anomaly detection in vehicular network |
| [85] | ✓ | ✓ | ✓ | ✓ | x | SDN-based fog computing for vehicular network |
| [86], [87] | ✓ | ✓ | ✓ | x | ✓ | Privacy preserving in smart home and smart grids |
| [91] | x | ✓ | | ✓ | x | Proactive defense mechanisms |
| [92] | x | ✓ | ✓ | ✓ | x | Anomaly behavior detection of various applications in IoT |
| [93], [94] | x | ✓ | ✓ | ✓ | x | Abnormal detection (and prevention) in various IoT applications based on SDN |
| [95] | ✓ | ✓ | ✓ | ✓ | x | Traffic management in IoT-SDN environment. |
| [96] | ✓ | ✓ | ✓ | ✓ | x | Combination of fog and SDN in IoT to meet the security |
| [97] | ✓ | ✓ | ✓ | ✓ | x | Reviewing the work done in the field of security and privacy of SDN-based IOT in smart homes |
| [98] | ✓ | ✓ | ✓ | ✓ | ✓ | Smart homes security aided SDN and ML |
| [99] | ✓ | ✓ | ✓ | ✓ | ✓ | Reviewing the work done in the field of security and privacy of SDN-based IOT in smart homes |
| [100] | ✓ | ✓ | ✓ | ✓ | x | SDN-based secure and privacy-preserving for vehicular networks |
| [101] | ✓ | ✓ | ✓ | ✓ | x | An overview of SDN layered architecture along with its strengths to DDoS attacks and its vulnerabilities which lead to new DDoS attacks. |
| [102] | ✓ | ✓ | ✓ | ✓ | ✓ | SDN-Based Privacy Preserving Cross Domain Routing protocol |
| [103] | ✓ | ✓ | | ✓ | | Security issues in data and control plane |
| [104] | x | ✓ | x | ✓ | | Security of routing in SDN |
| [105] | x | ✓ | x | ✓ | x | Using OpenFlow for SDN security |
| [106] | ✓ | x | x | ✓ | x | Security issues and vulnerabilities in data plane |
| [107] | x | ✓ | | ✓ | x | Security issues in hybrid SDNs |
| [108] | x | ✓ | x | ✓ | | Using blockchain to improve security in SDN structure of IoT |
| [109] | ✓ | ✓ | x | ✓ | | The denial of services attacks against the control plane in 5G networks has been addressed |
| [110] | ✓ | ✓ | x | ✓ | x | Detect and prevent attacks from malicious end hosts in SDNs |
| [111] | x | ✓ | x | ✓ | x | Layer communicates with a lower layer using the north-bound application interfaces |

the hybrid SDN. The authors have presented an approach to prevent the injection MHLs in the control and data plane.

Because this layer is the closest part of the SDN to the physical layer. This layer has the most connection with the distribution function and the limitation of processing resources in the physical layer. For this reason, it should be adjusted with this infrastructure.

### 2) CONTROL PLANE

The control plane manages and controls the network and infrastructure in SDN architecture. Many vendors have considered this layer as their target in their products. This layer is responsible for the different business logic and rule from various vendors. This layer communicates with the application plane via the northbound interface and with the data plane via the southbound interface.

**Northbound interface**: The control and application plane communicate with each other via the northbound interface. This layer prepares APIs for the applications to communicate with the controller.

**Southbound interface**: This layer is responsible for connecting to network equipment, including switches and other

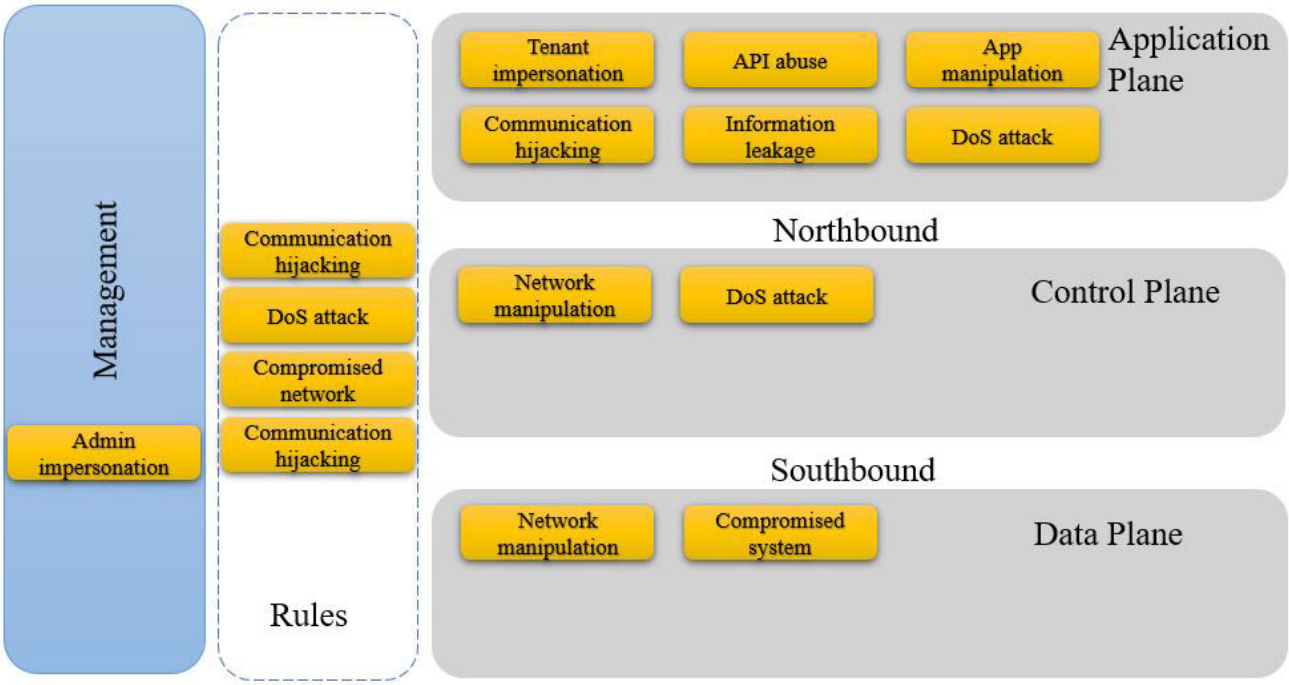


**FIGURE 3.** Vulnerabilities in SDN-based IoT.

nodes. This layer should be aware of the network topology and its connections. This layer also has APIs that allow the user to interact with and control network equipment. Some of the popular southbound APIs are OpenFlow, Cisco, and OpFlex.

- **Modules in controller** The controller includes following sub-modules [100]:
  - **Authentication Module.** This module is partially executed at Certificate Authority (CA) and partially on the cluster head. The modules help to validate the authenticity of CA, and cluster heads [100].
  - **Intrusion Detection Module.** This module prevents insider attackers or intruders who pass the first layer of security, authentication [100].
- **Using Blockchain in controller** The authors in [108] have merged the SDN and blockchain technology to overcome the security and privacy challenges in the SDN-based IoT systems. They have designed a routing protocol in the SDN controller for IoT devices and removed the PoW (Proof of Work). This approach can reduce energy consumption and increase security between IoT devices.
- **Other approach in controller** The authors have considered DDoS attacks in the controller plane in [109]. They have considered 5G as their benchmark for their experiments. Researchers in [110] have presented a security solution that detects and prevents attacks from malicious end hosts in an SDN. They have added s Security Management Application (SMA) in the SDN Controller and Switch Security Components (SSC) in the switches for enforcing the security policies on network flows. In [112] the authors have presented an approach for DDoS threat and SDN mitigation architecture for attack detection. Their approach has used a discrete scalable memory-based support vector machine algorithm. The author was able to predict the reduced attack in traffic and traffic dropping. The authors in [82] have used deep learning techniques like RNNs and LSTM to detect and reduce the impact of DDoS in SDN controllers. The authors in [27] have divided the attack types such as switch's and controller's resource saturation, control, and data channel saturation, east–westbound channel saturation, and northbound channel saturation, into three layers of SDNs. In [46], The destructive effect of the DDoS attack on the controller layer in SDN and the extent of violations in the performance of the entire SDN system are investigated. Due to the sensitivity of this layer and its greater impact on the overall performance of SDN-based IoT, this layer is more important to attackers. Therefore, most of the previous works have been done in this layer.

### 3) APPLICATION PLANE

This layer is the top layer in SDN architecture. The application plane communicates with the control plane with northbound interfaces. This layer manages various applications in SDN architecture. The application includes critical equipment like Intrusion Prevention System (IPS), Intrusion Detection System (IDS), load balancers, and firewalls [101], [111].

Given the widespread use of SDNs in IoT applications, much work has been done to create privacy and security in SDN-based IoT. Due to the limitations of SDN-based IoT, protocols and appropriate solutions to maintain privacy and security are presented in these works [113], [114], [115], [116].

This layer is most relevant to IoT applications. For this reason, most of the risks and solutions to deal with them are related to these applications.

## V. DISCUSSION

In this article, we have considered various works existing in the security and privacy of SDN-based IoT. For a clear analysis of the publications and research directions, we should consider various aspects of the existing works on the mentioned issues.

### A. NUMERICAL REVIEW OF EXISTING WORKS

We perusing publications over time in the area of privacy and security of SDNs. By this analysis, the research directions over previous and recent years could be detected. Then, we have to consider the statistical analysis of the research subjects of the existing papers.

**Publication over time** Figure 4, presents the number of published papers based on the different years. As can be seen, the number of articles is decreasing. But it should be noted that the number of security articles was much higher than the number of privacy articles. Most of the articles have dealt with security issues, and because their issues have been resolved, their number has decreased.

**Previous works' subject** Figure 5, presents the number of published papers based on the different subjects. As shown in Figure 5, the least work has been done in privacy-preserving. Very important applications now and in the future need to be processed in SDN-based IoT systems' privacy. Therefore, privacy in SDN-based IoT is a very important path for research.

**Privacy over time.** Figure 6, presents the number of published papers related to privacy-preserving over time. As can be seen in the figure, the number of articles is increasing. This position reflects an increase in attention to privacy issues in recent years. Therefore, there are many more unresolved issues in this area.

**Security over time.** Figure 7, presents the number of published papers related to security over time. From the content of the figure, it can be concluded that security issues have been resolved in recent years and fewer issues remain. This indicates that in this area, security problems have been identified as a more fundamental issue and a solution has been devised for it. Therefore, researchers should go to other paths besides security to find a suitable path for research.

**Applications' domain-counts.** Figure 8, presents the number of published papers based on the different application domains. As expected, the number of articles on new technologies such as blockchain, 5G, and vehicular networks is higher than others. However, due to the nature of SDN-based IoT, its use in all industries and applications is increasing rapidly. Therefore, its use in all new applications in the field of information technology and cloud computing is expected to increase significantly.

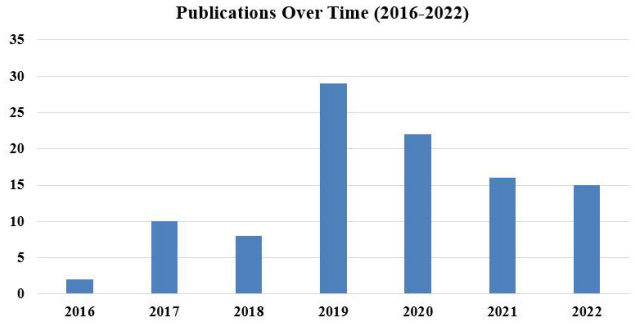


**FIGURE 4.** Publications over time.

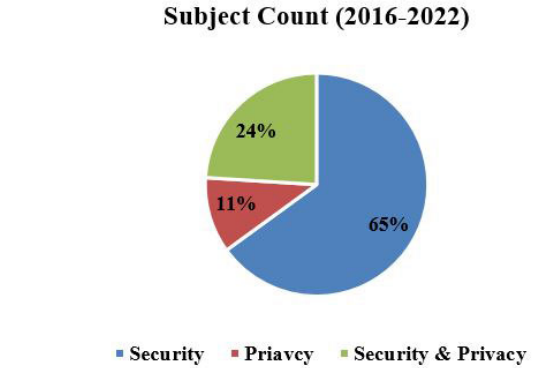


**FIGURE 5.** Subject count.

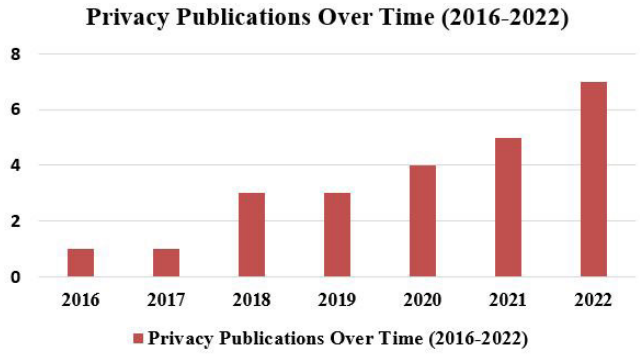


**FIGURE 6.** Privacy publications over time.

**Considered Layers-counts.** Figure 9, presents the number of published papers based on the considered layer. Most articles cover security and privacy issues at all three levels. This indicates that the authors of the articles believed that to achieve an acceptable level of security and privacy, the issues in all three layers should be considered. Therefore, it seems that researchers should consider all three layers simultaneously to achieve an acceptable level of security and privacy.

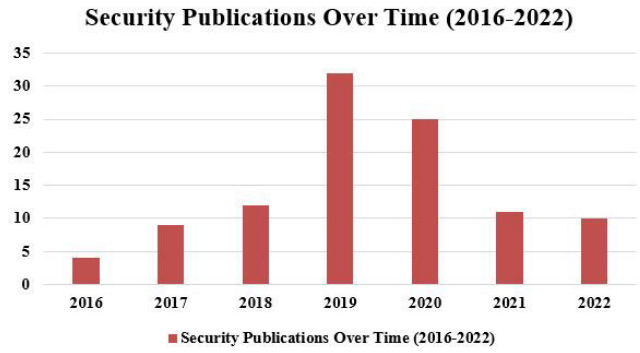


**FIGURE 7.** Security publications over time.

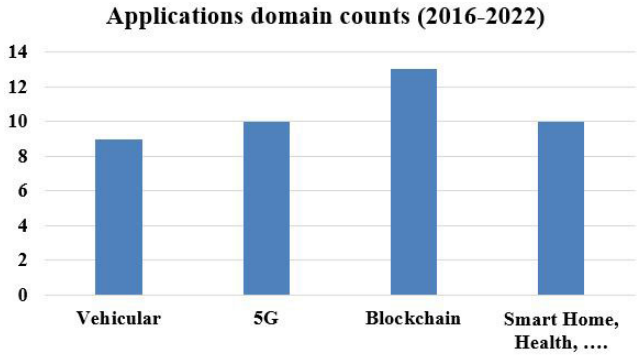


**FIGURE 8.** Applications domain count.

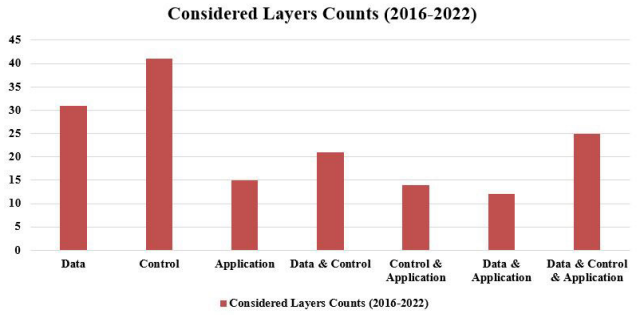


**FIGURE 9.** Considered layers count.

### B. TECHNICAL REVIEW OF PREVIOUS WORKS

Here, we review technical issues with previous work. SDNs are used for various applications. These applications include blockchain, vehicular networks, and 5G. considering these areas can be used for detecting various research directions.

**DDoS attacks.** Due to the limited processing resources in SDN-based IoT, this type of attack seems to be one of the most important and destructive types of attacks for this system. So although a lot of previous work has addressed this issue, it can still be one of the most important topics for continued research.

**Using blockchain to achieve an acceptable level of privacy security in SDN-based IoT.** The use of blockchain to achieve an acceptable level of privacy and security in SDN-based IoT has been considered in many previous works. The use of blockchain can be much more widespread, given the multiple uses of SDN-based IoT. For example, in this article [117], blockchain is used to record smart contract information and the type of driver behavior in the connected autonomous vehicles network. Therefore, more use of blockchain in the application layer and the controller layer can be one of the future research directions.

**Using deep learning techniques for security and privacy in SDN-based IoT** Due to the limited processing resources in SDN-based IoT, complex applications such as deep learning are complex and difficult. On the other hand, given that identifying many threats requires deep learning processing. So, some approaches should be found to process deep learning applications on limited processing resources of SDN-based IoT. It seems that this issue can also be one of the paths for future research. It seems that for this purpose, solutions such as federated learning or SNNs (Spiking Neural Networks) should be used [118], [119].

## VI. CONCLUSION AND FUTURE WORKS

In this work, we have analyzed the approaches and techniques in privacy-preserving and security of SDN-based IoT systems. Due to the dynamic nature of SDNs, constraints in IoT processing resources, and the existence of real-time applications in this type of processing, security, and privacy issues are essential. As far as we know, this is the first work in reviewing the existing works in the field of security and privacy-preserving SDN-based IoT systems. We have categorized existing works based on the main subjects, targeted layer, and application types in them. We also have analyzed the existing works based on their subject, application domains, publishing year, and considered layers. We have also provided statistical analyzes based on the considered subjects, layers, applications, and the year in which the research was conducted.

Due to the presented information in this research, unlike security, which has attracted a lot of attention, privacy still needs more attention and research in SDN-based IoT. Therefore, researchers should pay more attention to this issue and consider it. It also seems that to achieve an acceptable level of security and privacy, the issues in all three layers should be considered simultaneously. Also, due to the distributed nature of the infrastructure in IoT systems, the use of blockchain should be considered more to maintain privacy and security. Also, given the importance of machine learning and deep learning to identify suspicious and attack streams, low-overhead solutions should be found for processing machine learning and deep learning on the limited SDN-based IoT infrastructures. Due to the emergence of a new generation of communications such as 5G and the use of new applications in it, it seems that to coordinate and comply with these applications, some research should be considered in the application layer of SDN-based IoT.

## DECLARATIONS

### ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

### CONSENT FOR PUBLICATION

Not applicable.

### AVAILABILITY OF DATA AND MATERIALS

Not applicable.

### COMPETING INTERESTS

The authors declare that they have no competing interests.

### FUNDING

Not applicable.

### AUTHORS' CONTRIBUTIONS

Hossein has collected the contents of the article and written it. Chhagan has read the article and has given his comment to Hossein in several rounds. Mauro and Mehdi read the article several times and gave their comments to Hossein and Chhagan for improvement. Mauro has also led and managed Research.

## REFERENCES

[1] *Software-Defined Networking (SDN) Market Size Worldwide in 2020 and 2027*. Accessed: Aug. 20, 2021. [Online]. Available: https://sites.google.com/site/technologiesmarketnews/cellular-iot-market-worth-9-65-billion-by-2025-key-industry-players-zte-corporation-gemalto-nv

[2] *IoT Market 2012–2025*. Accessed: Jan. 4, 2022. [Online]. Available: https://www.statista.com/statistics/468636/global-sdn-market-size/

[3] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[4] F. Wortmann and K. Flüchter, "Internet of Things," *Bus. Inf. Syst. Eng.*, vol. 57, no. 3, pp. 221–224, 2015.

[5] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of Things," *Int. J. Commun. Syst.*, vol. 25, no. 9, p. 1101, Sep. 2012.

[6] R. H. Weber and R. Weber, *Internet of Things*, vol. 12. Heidelberg, Germany: Springer, 2010.

[7] Y. Li and H. Takada, "ISotEE: A hypervisor middleware for IoT-enabled resource-constrained reliable systems," *IEEE Access*, vol. 10, pp. 8566–8576, 2022.

[8] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to IoT," *Int. Adv. Res. J. Sci., Eng. Technol.*, vol. 5, no. 1, pp. 41–44, 2018.

[9] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, pp. 77–89, Apr. 2022.

[10] M. O. Arowolo et al., "K-nearest neighbour algorithm for classification of IoT-based edge computing device," in *Artificial Intelligence for Cloud and Edge Computing*. Cham, Switzerland: Springer, 2022, pp. 161–179.

[11] I. Zualkernan, S. Dhou, J. Judas, A. R. Sajun, B. R. Gomez, and L. A. Hussain, "An IoT system using deep learning to classify camera trap images on the edge," *Computers*, vol. 11, no. 1, p. 13, 2022.

[12] H. Ahmadvand, T. Dargahi, F. Foroutan, P. Okorie, and F. Esposito, "Big data processing at the edge with data skew aware resource allocation," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2021, pp. 81–86.

[13] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[14] S. S. Gupta. (2017). *Blockchain*. [Online]. Available: http://www.IBM.COM

[15] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[16] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 45–54.

[17] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," 2019, *arXiv:1906.11078*.

[18] D. J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT, USA: Yale Univ. Press, 2011.

[19] D. E. Pozen, "Privacy-privacy tradeoffs," *Univ. Chicago Law Rev.*, vol. 83, no. 1, pp. 221–247, 2016.

[20] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, Art. no. e3677.

[21] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.

[22] P. J. B. Pajila and E. G. Julie, "Detection of DDoS attack using SDN in IoT: A survey," in *Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019*. Springer, 2020.

[23] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and mitigation of dos and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors*, vol. 20, no. 3, p. 816, 2020.

[24] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.

[25] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[26] M. Parashar, A. Poonia, and K. Satish, "A survey of attacks and their mitigations in software defined networks," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–8.

[27] M. P. Singh and A. Bhandari, "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges," *Comput. Commun.*, vol. 154, pp. 509–527, Mar. 2020.

[28] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1994–2008, Dec. 2017.

[29] K. Slavov, D. Migault, and M. Pourzandi, "Identifying and addressing the vulnerabilities and security issues of SDN," *Ericsson Technol. Rev.*, vol. 92, no. 7, 2015.

[30] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 159, Jun. 2020, Art. no. 102595.

[31] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey," *Future Gener. Comput. Syst.*, vol. 115, pp. 126–149, Feb. 2021.

[32] R. Swami, M. Dave, and V. Ranga, "Software-defined networking-based DDoS defense mechanisms," *ACM Comput. Surv.*, vol. 52, no. 2, pp. 1–36, Mar. 2020.

[33] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," *IEEE Access*, vol. 7, pp. 80813–80828, 2019.

[34] X. Xiaoqiong, Y. Hongfang, and Y. Kun, "DDoS attack in software defined networks: A survey," *ZTE Commun.*, vol. 15, no. 3, pp. 13–19, 2019.

[35] R. M. A. Ujjan, Z. Pervez, K. Dahal, W. A. Khan, A. M. Khattak, and B. Hayat, "Entropy based features distribution for anti-DDoS model in SDN," *Sustainability*, vol. 13, no. 3, p. 1522, Feb. 2021.

[36] A. Shaghaghi et al., "Software-defined network (SDN) data plane security: issues, solutions, and future directions," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. 2020, pp. 341–387.

[37] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," *Cluster Comput.*, vol. 24, no. 2, pp. 1235–1253, Jun. 2021.

[38] Z. Shah and S. Cosgrove, "Mitigating ARP cache poisoning attack in software-defined networking (SDN): A survey," *Electronics*, vol. 8, no. 10, p. 1095, Sep. 2019.

[39] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced support vector machine- (ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN)," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–12, Mar. 2019.

[40] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, and S. Kandeepan, "A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks," *Eng. Sci. Technol., Int. J.*, vol. 31, Jul. 2022, Art. no. 101065.

[41] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[42] R. Sahay, W. Meng, D. A. S. Estay, C. D. Jensen, and M. B. Barfod, "CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships," *Future Gener. Comput. Syst.*, vol. 100, pp. 736–750, Nov. 2019.

[43] F. S. D. Silva, E. Silva, E. P. Neto, M. Lemos, A. J. V. Neto, and F. Esposito, "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," *Sensors*, vol. 20, no. 11, p. 3078, May 2020.

[44] A. B. Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021.

[45] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments," *Future Gener. Comput. Syst.*, vol. 125, pp. 156–167, Dec. 2021.

[46] R. Swami, M. Dave, and V. Ranga, "DDoS attacks and defense mechanisms using machine learning techniques for SDN," in *Research Anthology on Combating Denial-of-Service Attacks*. Hershey, PA, USA: IGI Global, 2021, pp. 248–264.

[47] Y.-C. Wang and Y.-C. Wang, "Efficient and low-cost defense against distributed denial-of-service attacks in SDN-based networks," *Int. J. Commun. Syst.*, vol. 33, no. 14, p. e4461, Sep. 2020.

[48] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020.

[49] D. He, S. Chan, and M. Guizani, "Securing software defined wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 20–25, Jan. 2016.

[50] K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabir, "Preventive determination and avoidance of DDoS attack with SDN over the IoT networks," in *Proc. Int. Conf. Autom., Control Mechatronics Ind. 4.0 (ACMI)*, Jul. 2021, pp. 1–6.

[51] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, "A time-efficient approach toward DDoS attack detection in IoT network using SDN," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3612–3630, Mar. 2022.

[52] N. Hossain, M. Z. Hossain, and M. A. Hossain, "An ontological security framework to secure the SDN based IoT networks," *Amer. J. Agricult. Sci., Eng. Technol.*, vol. 5, no. 1, pp. 4–18, 2021, doi: 10.54536/ajaset.v5i1.55.

[53] S. A. Latif, F. B. X. Wen, C. Iwendi, F. W. Li-li, S. M. Mohsin, Z. Han, and S. S. Band, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, Jan. 2022.

[54] W. Ren, Y. Sun, H. Luo, and M. Guizani, "SILedger: A blockchain and ABE-based access control for applications in SDN-IoT networks," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 4, pp. 4406–4419, Dec. 2021.

[55] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3850–3864, Mar. 2021.

[56] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, 2008.

[57] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 303–308.

[58] Q. Shafi and A. Basit, "DDoS botnet prevention using blockchain in software defined Internet of Things," in *Proc. 16th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2019, pp. 624–628.

[59] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[60] C. Xue, N. Xu, and Y. Bo, "Research on key technologies of software-defined network based on blockchain," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, p. 239.

[61] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, May 2017, pp. 720–725.

[62] M. Steichen, S. Hommes, and R. State, "ChainGuard—A firewall for blockchain applications using SDN with OpenFlow," in *Proc. Princ., Syst. Appl. IP Telecommun. (IPTComm)*, Sep. 2017, pp. 1–8.

[63] Z. A. El Houda, L. Khoukhi, and A. Hafid, "ChainSecure—A scalable and proactive solution for protecting blockchain applications using SDN," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[64] W. Hou, Z. Ning, L. Guo, and P. Guo, "SDN-based optimizing solutions for multipath data transmission supporting consortium blockchains," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2018, pp. 1–5.

[65] R. Shashidhara, N. Ahuja, M. Lajuvanthi, S. Akhila, A. K. Das, and J. J. P. C. Rodrigues, "SDN-chain: Privacy-preserving protocol for software defined networks using blockchain," *Secur. Privacy*, vol. 4, no. 6, Nov. 2021, Art. no. e178.

[66] M. Hajizadeh, N. Afraz, M. Ruffini, and T. Bauschert, "Collaborative cyber attack defense in SDN networks using blockchain technology," in *Proc. 6th IEEE Conf. Netw. Softw. (NetSoft)*, Jun. 2020, pp. 487–492.

[67] A. Hakiri and B. Dezfouli, "Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks," in *Proc. ACM Int. Workshop Softw. Defined Netw. Netw. Function Virtualization Secur.*, Apr. 2021, pp. 11–18.

[68] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, and D. Draheim, "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors J.*, vol. 21, no. 6, pp. 8716–8733, Jan. 2021.

[69] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.

[70] N. Shukla, C. Gandhi, and T. Choudhury, "Leveraging blockchain and SDN for efficient and secure IoT network," in *Blockchain Applications in IoT Ecosystem*. Cham, Switzerland: Springer, 2020, pp. 151–166.

[71] A. Xiong, H. Tian, W. He, J. Zhang, H. Meng, S. Guo, X. Wang, X. Wu, and M. Kadoch, "A distributed security SDN cluster architecture for smart grid based on blockchain technology," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Nov. 2021.

[72] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: Blockchain-based multicontroller architecture for secure software-defined networks," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–12, Apr. 2021.

[73] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 493–501, Jan. 2019.

[74] S. Javanmardi, M. Shojafar, R. Mohammadi, A. Nazari, V. Persico, and A. Pescapè, "FUPE: A security driven task scheduling approach for SDN-based IoT–fog networks," *J. Inf. Secur. Appl.*, vol. 60, Aug. 2021, Art. no. 102853.

[75] D. Javeed, T. Gao, M. T. Khan, and I. Ahmad, "A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)," *Sensors*, vol. 21, no. 14, p. 4884, Jul. 2021.

[76] Q. Zhou, J. Yu, and D. Li, "A dynamic and lightweight framework to secure source addresses in the SDN-based networks," *Comput. Netw.*, vol. 193, Jul. 2021, Art. no. 108075.

[77] T.-H. Lee, L.-H. Chang, and C.-W. Syu, "Deep learning enabled intrusion detection and prevention system over SDN networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[78] K. D. Joshi and K. Kataoka, "PSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107295.

[79] D. Javeed, T. Gao, and M. T. Khan, "SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT," *Electronics*, vol. 10, no. 8, p. 918, Apr. 2021.

[80] A. Wani, S. Revathi, and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Trans. Intell. Technol.*, vol. 6, no. 3, pp. 281–290, Sep. 2021.

[81] S. Khan and A. Akhunzada, "A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 170, pp. 209–216, Mar. 2021.

[82] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies*, vol. 9, no. 1, p. 14, Feb. 2021.

[83] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Veh. Commun.*, vol. 27, Jan. 2021, Art. no. 100284.

[84] B. Wang, Y. Sun, and X. Xu, "A scalable and energy-efficient anomaly detection scheme in wireless SDN-based mMTC networks for IoT," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1388–1405, Feb. 2021.

[85] M. Arif, G. Wang, V. E. Balas, O. Geman, A. Castiglione, and J. Chen, "SDN based communications privacy-preserving architecture for VANETs using fog computing," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100265.

[86] V. Sivaraman and B. Sikdar, "A game-theoretic approach for enhancing data privacy in SDN-based smart grids," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10583–10595, Jul. 2021.

[87] W. Iqbal, H. Abbas, B. Rauf, Y. A. Bangash, M. F. Amjad, and A. Hemani, "PCSS: Privacy preserving communication scheme for SDN enabled smart homes," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17677–17690, Sep. 2022.

[88] M. Faheem, R. A. Butt, B. Raza, M. W. Ashraf, M. A. Ngadi, and V. C. Gungor, "Energy efficient and reliable data gathering using Internet of Software-defined mobile sinks for WSNs-based smart grid applications," *Comput. Standards Interfaces*, vol. 66, Oct. 2019, Art. no. 103341.

[89] M. Faheem, M. Umar, R. A. Butt, B. Raza, M. A. Ngadi, and V. C. Gungor, "Software defined communication framework for smart grid to meet energy demands in smart cities," in *Proc. 7th Int. Istanbul Smart Grids Cities Congr. Fair (ICSG)*, Apr. 2019, pp. 51–55.

[90] M. Faheem and R. A. Butt, "Big datasets of optical-wireless cyber-physical systems for optimizing manufacturing services in the Internet of Things-enabled industry 4.0," *Data Brief*, vol. 42, Jun. 2022, Art. no. 108026.

[91] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5366–5380, 2021.

[92] R. Kiani and A. Bohlooli, "Distributed rule anomaly detection in SDN-based IoT," in *Proc. 5th Int. Conf. Internet Things Appl. (IoT)*, May 2021, pp. 1–6.

[93] C.-H. Lee, J. S. Park, and J. G. Shon, "An SDN-based distributed identifier locator separation scheme for IoT networks," in *Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 2019*. Singapore: Springer, 2021.

[94] S. Lahlou, Y. Moukafih, A. Sebbar, K. Zkik, M. Boulmalf, and M. Ghogho, "TD-RA policy-enforcement framework for an SDN-based IoT architecture," *J. Netw. Comput. Appl.*, vol. 204, Aug. 2022, Art. no. 103390.

[95] P. Thorat, N. K. Dubey, K. Khetan, and R. Challa, "SDN-based predictive alarm manager for security attacks detection at the IoT gateways," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–2.

[96] S. Prabavathy and V. Supriya, "SDN based cognitive security system for large-scale Internet of Things using fog computing," in *Proc. Int. Conf. Emerg. Techn. Comput. Intell. (ICETCI)*, Aug. 2021, pp. 129–134.

[97] N. Y.-R. Douha, M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, "A survey on blockchain, SDN and NFV for the smart-home security," *Internet Things*, vol. 20, Nov. 2022, Art. no. 100588.

[98] T. Altaf and R. Braun, "A roadmap to smart homes security aided SDN and ML," in *Proc. 5th Conf. Cloud Internet Things (CIoT)*, Mar. 2022, pp. 129–136.

[99] H. Babbar, S. Rani, and S. A. AlQahtani, "Intelligent edge load migration in SDN-IIoT for smart healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8058–8064, Nov. 2022.

[100] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8421–8434, Sep. 2019.

[101] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, Aug. 2020, Art. no. 100279.

[102] Q. Chen, S. Shi, X. Li, C. Qian, and S. Zhong, "SDN-based privacy preserving cross domain routing," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 6, pp. 930–943, Nov. 2019.

[103] K. Dhamecha and B. Trivedi, "SDN issues—A survey," *Int. J. Comput. Appl.*, vol. 73, no. 18, pp. 30–35, Jul. 2013.

[104] A. Voellmy and P. Hudak, "Nettle: Taking the sting out of programming network routers," in *Practical Aspects of Declarative Languages: 13th International Symposium, PADL 2011, Austin, TX, USA, January 24–25, 2011. Proceedings 13*. Berlin, Germany: Springer, 2011.

[105] W. Stallings, "Software-defined networks and openflow," *Internet Protocol J.*, vol. 16, no. 1, pp. 2–14, 2013.

[106] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, "A survey on the security of stateful SDN data planes," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1701–1725, 3rd Quart., 2017.

[107] P. Shrivastava and K. Kataoka, "Topology poisoning attacks and prevention in hybrid software-defined networks," *IEEE Trans. Netw. Serv. Manage.*, vol. 19, no. 1, pp. 510–523, Mar. 2022.

[108] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K.-R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 625–638, Jul. 2020.

[109] R. S. Silva, C. C. Meixner, R. S. Guimarães, T. Diallo, B. O. Garcia, L. F. M. de Moraes, and M. Martinello, "REPEL: A strategic approach for defending 5G control plane from DDoS signalling attacks," *IEEE Trans. Netw. Serv. Manage.*, vol. 18, no. 3, pp. 3231–3243, Sep. 2021.

[110] V. Varadharajan and U. Tupakula, "Counteracting attacks from malicious end hosts in software defined networks," *IEEE Trans. Netw. Serv. Manage.*, vol. 17, no. 1, pp. 160–174, Mar. 2020.

[111] A. Voellmy, H. Kim, and N. Feamster, "Procera: A language for high-level reactive network control," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, Aug. 2012, pp. 43–48.

[112] M. Revathi, V. V. Ramalingam, and B. Amutha, "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework," *Wireless Pers. Commun.*, vol. 127, pp. 2417–2441, Dec. 2022.

[113] R. Djouani, K. Djouani, F. Boutekkouk, and R. Sahbi, "A security proposal for IoT integrated with SDN and cloud," in *Proc. 6th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2018, pp. 1–5.

[114] U. Gorrepati, P. Zavarsky, and R. Ruhl, "Privacy protection in LTE and 5G networks," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, May 2021, pp. 382–387.

[115] A. Rahman, C. Chakraborty, A. Anwar, M. R. Karim, M. J. Islam, D. Kundu, Z. Rahman, and S. S. Band, "SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic," *Cluster Comput.*, vol. 25, pp. 2351–2368, Aug. 2022.

[116] D. B. Rathnamalala, H. W. P. Milan, K. L. I. Dilshani, and E. H. Jayatunga, "Fully integrated software-defined networking (SDN) testbed using open-source platforms," *Social Netw. Comput. Sci.*, vol. 3, no. 1, pp. 1–15, Jan. 2022.

[117] T. Dargahi, H. Ahmadvand, M. N. Alraja, and C.-M. Yu, "Integration of blockchain with connected and autonomous vehicles: Vision and challenge," *ACM J. Data Inf. Qual.*, vol. 14, no. 1, pp. 1–10, 2021.

[118] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, "Federated learning," *Synth. Lect. Artif. Intell. Mach. Learn.*, vol. 13, no. 3, pp. 1–207, 2019.

[119] S. Ghosh-Dastidar and H. Adeli, "Spiking neural networks," *Int. J. Neural Syst.*, vol. 19, no. 4, pp. 295–308, Aug. 2009.

**HOSSEIN AHMADVAND** received the Ph.D. degree from the Sharif University of Technology, Iran, for his work exploring the use of data variety in the progressive processing of big data in a cloud environment, in 2019. He is currently a Postdoctoral Researcher with the University of Calgary. He is also an experienced researcher, a project manager, and a senior research and development expert. He has many experiences in research and industry. His research interests include edge computing, ML/DL, big data processing, and cloud computing.

**CHHAGAN LAL** received the Ph.D. degree in computer science and engineering from the Malaviya National Institute of Technology, Jaipur, India, in 2014. He was a Research Fellow with Simula Research Laboratories, Oslo, Norway. Before joining Simula, he was a Postdoctoral Fellow with the Department of Mathematics, University of Padova (UNIPD), Italy (https://spritz.math.unipd.it/team.html). He is currently a Researcher with the CyberSecurity Laboratories, Department of Intelligent Systems, Faculty of EEMCS, TU Delft, The Netherlands. During the Ph.D. degree, he was awarded the Canadian Commonwealth Scholarship under the Canadian Commonwealth Scholarship Program to work with the University of Saskatchewan, Saskatoon, SK, Canada. He has wide experience in proposal preparation and execution of EU H2020 projects. His research interests include various aspects of systems and network security and traffic engineering in next-generation networks, such as network security, blockchain technologies and smart contracts, and solutions for secure and reliable communication in networks, such as the IoT, SDN, VANETs, and ICN. He is an active member of the Security and PRIvacy Through Zeal (SPRITZ) Research Group, which is led by Prof. Mauro Conti.

**HADI HEMMATI** received the Ph.D. degree from the University of Oslo, Norway. He was an Associate Professor with the Electrical and Software Engineering Department, University of Calgary, AB, Canada. He was also an Assistant Professor with the University of Manitoba and a Postdoctoral Fellow with the University of Waterloo and Queen's University. He is currently an Associate Professor with Electrical Engineering and Computer Science Department, York University. His research interests include automated software engineering (with a focus on software testing, debugging, and repair), trustworthy AI (with a focus on robustness and explainability), pragmatic software/ML solutions for large-scale systems, and empirically investigating them in practice. He has been a PI on multiple industry research projects in different domains, such as IT, aviation, insurance, urban development, fintech, and beyond.

**MEHDI SOOKHAK** (Senior Member, IEEE) received the Ph.D. degree in computer science, major in information security from the University of Malaya (UM), in 2015. From 2012 to 2015, he was a Research Assistant with the Center of Mobile Cloud Computing Research (C4MCCR), UM. From 2016 to 2017, he was a Postdoctoral Fellow with Carleton University, Canada. In 2017, he joined Arizona State University. In 2019, he joined Illinois State University as an Assistant Professor in cybersecurity. He is currently an Assistant Professor in computer science with Texas A&M University, Corpus Christi, TX, USA. He has authored more than 50 papers in high-ranking journals and conferences. His research interests include cloud and mobile cloud computing, fog/edge computing, vehicular networks, blockchain, computation outsourcing, machine learning, and AI. He is on the editorial board of several ISI journals, including *Vehicular Communications*, *Electronics*, and IEEE Access. He served as the Chair for several conferences, such as IEEE WTS and IEEE ICC.

**MAURO CONTI** (Fellow, IEEE) received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. After the Ph.D. degree, he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor with the University of Padua, where he became an Associate Professor, in 2015, and then a Professor, in 2018. He was a Visiting Researcher with GMU, in 2008 and 2016, UCLA, in 2010, UCI, in 2012, 2013, 2014, and 2017, TU Darmstadt, in 2013, UF, in 2015, and FIU, in 2015 and 2016. He is currently a Professor with the University of Padua, Italy, and an affiliate Professor with the University of Washington. His research interests include security and privacy. In this areas, he has published more than 200 papers in the topmost international peer-reviewed journals and conferences. His research is also funded by companies, including Cisco and Intel. He has been awarded a Marie Curie Fellowship, in 2012, by the European Commission and a Fellowship by the German DAAD, in 2013. He was the Program Chair of TRUST 2015, ICISS 2016, and WiSec 2017, and the General Chair of SecureComm 2012 and ACM SACMAT 2013. He is the Area Editor-in-Chief of IEEE Communications Surveys and Tutorials, and an Associate Editor for several journals, including IEEE Communications Surveys Tutorials, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management.