Wiley
International Journal of Distributed Sensor Networks
Volume 2024, Article ID 9006405, 26 pages
https://doi.org/10.1155/2024/9006405

Review Article

A Review on Software-Defined Networking for Internet of Things Inclusive of Distributed Computing, Blockchain, and Mobile Network Technology: Basics, Trends, Challenges, and Future Research Potentials

Shakila Shafiq,[1,2] Md. Sazzadur Rahman,[1] Shamim Ahmed Shaon,[1] Imtiaz Mahmud,[3] and A. S. M. Sanwar Hosen[4]

[1]*Institute of Information Technology, Jahangirnagar University, Savar, 1342 Dhaka, Bangladesh*
[2]*Department of Computer Science & Engineering, National Institute of Textile Engineering and Research, Nayarhat, Savar 1350, Bangladesh*
[3]*Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA*
[4]*Department of Artificial Intelligence and Big Data, Woosong University, Daejeon 34606, Republic of Korea*

Correspondence should be addressed to Md. Sazzadur Rahman; sazzad@juniv.edu and A. S. M. Sanwar Hosen; sanwar@wsu.ac.kr

Received 8 October 2023; Revised 28 January 2024; Accepted 12 June 2024

Academic Editor: Francesco Longo

Internet of things (IoT) and software-defined networking (SDN) are two relatively recent developments in the field of communication technology that have emerged in response to the growing demand for more efficient, flexible, and dynamic network architectures. As both of these concepts are new, they have received increasing attention from academic or industrial sources to emphasize their potential for integration. This study is aimed at reviewing the literature on SDN for IoT (SDN-IoT) published from 2014 to 2022 and presenting insights and directions for future research, with a particular focus on cloud, fog, and edge computing. The study collects data from Science Direct, IEEE Explore, and Google Scholar and objectively selects 126 papers and conducts metadata analysis. The study articulates the challenges of managing and orchestrating IoT systems and how SDN can be used to address these challenges by enabling dynamic and flexible network configurations. It delineates not only the function of blockchain (BC) technology in securing and managing IoT networks but also how SDN can be utilized to incorporate BC-based solutions. Additionally, the potential of SDN for mobile networks is explored, which are increasingly being used to support IoT devices. Finally, this study outlines the issues, challenges, and potential future research directions that may present opportunities for the researchers working in this field, underscoring the demand for more in-depth investigation and advancement.

Keywords: blockchain; cloud computing; edge computing; fog computing; mobile network; SDN-IoT

1. Introduction

The network of physical "things" that are equipped with sensors, software, and other technologies to communicate, compute, and exchange data with other devices and systems through the internet is referred to as the internet of things (IoT) [1]. It was first presented by Kevin Ashton 17 years ago and has since become a cornerstone of the second digital revolution [2]. All facets of human life are covered by the services provided by IoT applications, for instance, home and building automation, smart industry, smart cities, smart health, intelligent traffic management, smart health monitoring, emergency and surveillance services, retail, and supply chain. Sensors play a significant role in communication between users and intelligent devices by sensing and gathering information. According to a Cisco survey, 1 trillion networked sensors are anticipated to be embedded worldwide by 2022, with up to 45 trillion in 20 years [3] and 500 billion

intelligent devices predicted to be linked on Earth by 2030 [4]. IoT systems will contain a significant share of these connected devices with many integrated sensors and actuators. IoT technology enables everyday physical objects to communicate electronically, enabling them to be cautious about distant events or act to an event they cannot physically perceive. However, the maintenance and scalability of such a variety of connected devices are a matter of challenge. Moreover, several active IoT devices are drastically increasing day by day. Figure 1 shows that the active IoT devices are getting more prominent from 2010 to 2022, but the non-IoT devices are the same in number [5]. These IoT devices generate large amounts of data, and traditional network infrastructure can become overwhelmed. To provide a scalable solution to manage and control the flow of data in the network, integration of Software-Defined Networking (SDN) has been introduced. With SDN, network administrators can manage and configure the entire network from a single location, reducing the complexity of managing multiple devices. Thus, SDN for IoT (SDN-IoT) architecture has been developed for efficient administration due to the global growth of IoT and its administration complexity [6–9]. Figure 2 illustrates the focuses of research studies published from 2014 to 2023, presented as retrieved keywords from the titles of articles, conference papers, book chapters, reviews, and conference reviews. This figure highlights the key areas and trends in the field, with significant emphasis on the SDN-IoT topics, and their integration with other emerging technologies.

By establishing the method of software implementation on the IoT network, SDN regulates, controls, and upgrades network behaviors dynamically [11]. In the modern digital world, communication networks are the fabric that holds everything together. Metcalfe's law asserts that the value of a communication network is proportional to the number of connected devices [12]. As a result, SDN has gained prominence as a network service technology due to its programmability and flexible maintenance [13, 14]. SDN offers a layered structure involving three planes, namely, the data, control, and application planes, where each plane operates independently [15]. Data and control plane separation enables runtime network administration, traffic control, network expansion, and flexible system programmability. Figure 3 illustrates the published research works in SDN-IoT systems from 2014 to 2023, encompassing articles, conference papers, book chapters, reviews, and conference reviews. This visualization provides an overview of the extensive literature available in the field over the specified period, offering valuable insights into the evolution and scope of research in SDN-IoT systems.

Cloud computing (CC) [16], fog computing (FC) [17], and edge computing (EC) [18] were introduced in the context of SDN and the IoT to address the challenges of data processing and management in large-scale, distributed networks. CC provides a centralized, scalable computing infrastructure that can be accessed over the internet, making it ideal for large-scale data processing and storage. This enables real-time data analysis and decision-making, which increases the effectiveness and efficiency of IoT systems. In addition, CC allows remote management and control of IoT devices, which is particularly useful for large-scale IoT device deployments. However, the reliance on CC for IoT data processing can result in high latency and network traffic, as well as security and privacy concerns associated with transmitting sensitive data over the internet. EC could be a solution to these challenges by bringing processing and storage capabilities closer to IoT devices and reducing latency and network traffic. It involves data processing on IoT devices themselves or nearby edge devices such as gateways. It reduces the amount of data that must be transmitted to the cloud and can also improve the responsiveness of IoT systems. It enables real-time analysis and decision-making, reduced latency, increased scalability, enhanced security, decreased costs, and compliance with specific regulations, which is more advantageous for IoT systems. However, it can still be limited in terms of processing and storage capabilities, especially in large-scale IoT deployments; EC would need more resources, such as processing power, bandwidth, and storage, and using FC can help with this issue.

FC is introduced as an intermediary layer between the edge and the cloud, providing additional processing and storage resources to support the edge and offloading some of the processing and storage workloads from the cloud. It enables the creation of local instances of virtualized network functions and applications that can communicate with the cloud. It uses a network of fog nodes, which are intermediate devices located between the edge devices and the cloud. These fog nodes have more resources than edge devices and are responsible for performing some of the computing tasks and data processing on behalf of the edge devices. This can help to reduce the workload on edge devices and improve the performance of real-time applications. CC, EC, and FC each have their benefits, and the optimal solution will depend on the application's requirements. Depending on the use case, these three types of computing can also be combined in a hybrid approach. As they represent different aspects of distributed computing (DC), where resources are spread across different nodes in a network, for reading simplicity, we will address these three terms as DC here.

Additional challenges in the SDN-IoT environment include device security, reliability, and confidentiality [19, 20]. The capabilities of blockchain (BC) along with the SDN controller allow us to build a safe network that overcomes these security issues. It provides a secure, tamper-proof way to store and transfer data, ensuring the integrity and confidentiality of data in these networks. Integrating mobile networks with SDN-IoT can provide a more flexible and scalable solution for supporting the rapidly growing number of connected devices in the IoT and help ensure that these devices have reliable and secure access to the network. It refers to the integration of cellular communication technologies such as 5G/6G with the principles of SDN to create a unified, efficient, and scalable network for supporting IoT devices. Therefore, the present study is aimed at exploring the SDN-IoT architectures, benefits of DC and BC technology, and integration of mobile networks in this paradigm and at solving the aforementioned problems by providing a taxonomy of existing systems and future directions. To our

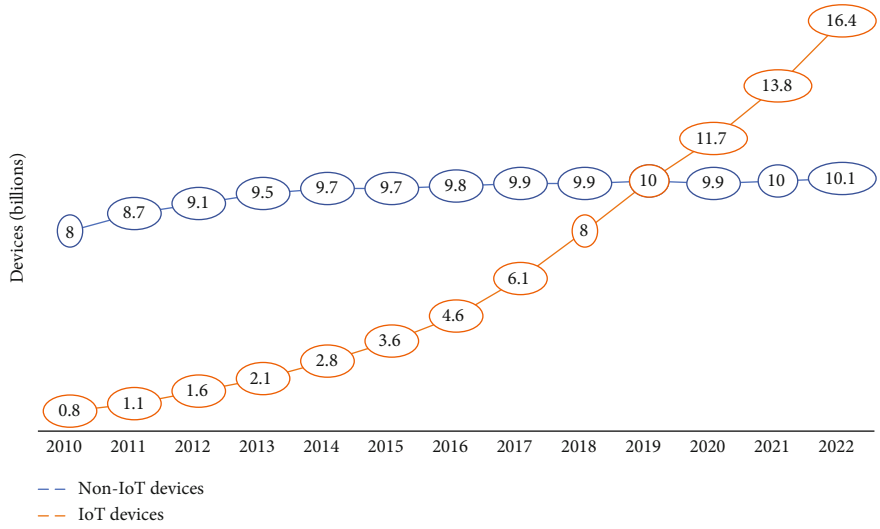

FIGURE 1: Non-IoT and IoT devices active from 2010 to 2022.

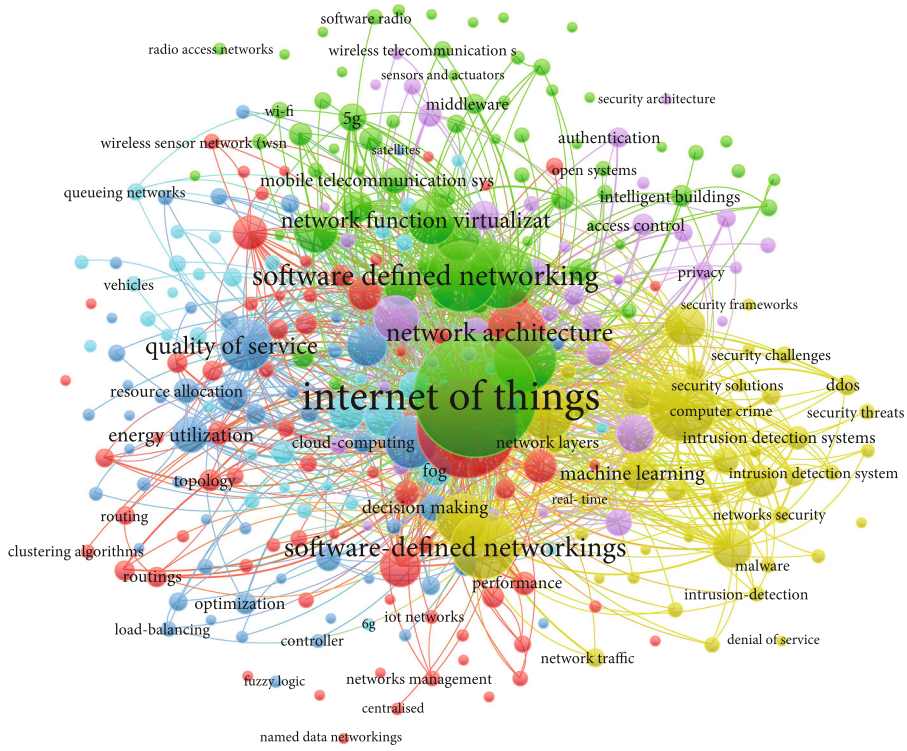

FIGURE 2: The focus of research studies published from 2014 to 2023, presented as retrieved keywords from the titles of papers (articles, conference papers, book chapters, reviews, and conference reviews) [10].

knowledge, this is the first assessment that comprehensively examines the critical facets of the SDN-IoT and its deployment with DC, BC, and 5G/6G technologies from needs to almost all working areas. The following are the study's main contributions:

- This research provides comprehensive insights into the development of SDN-IoT by citing and reviewing relevant papers on a range of subjects that have previously been studied separately.
- The fundamental specifications of the underlying technologies, such as SDN, IoT, DC, BC, and mobile networks along with an overview of how each plays a part in enabling IoT applications are discussed.
- The main SDN-IoT scenario is in depth studied with emphasis on the current SDN-IoT deployment, which includes DC, BC, and 5G/6G technologies.
- This study systematically selects 50 research articles and evaluates based on their model proposals, contributions,

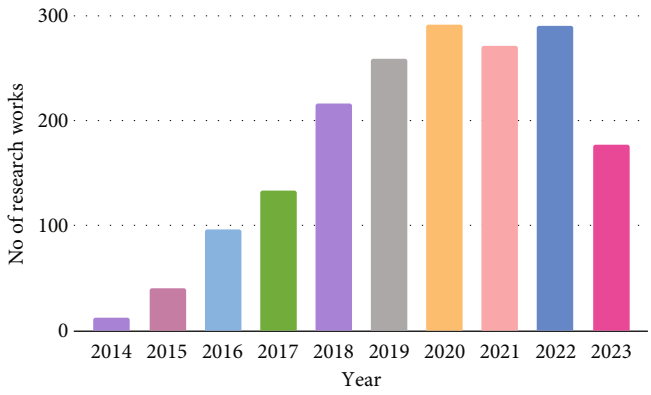

FIGURE 3: Published research works including articles, conference papers, book chapters, review, and conference review in SDN-IoT systems from 2014 to 2023 [10].

and possible future applications. Ten popular working areas, including security and privacy, reliability, mobility, scalability, latency, traffic management, resource management, IoT services, mobile network, and wireless sensor network (WSN) are covered. The deployments are examined, assessed, and debated in detail.

- This study offers a detailed categorization of the reviewed papers, encompassing multiple fronts such as architecture, models, frameworks, and solutions and examines how SDN-IoT systems are deployed in conjunction with DC, BC, and 5G/6G technologies, facilitating a comprehensive understanding of the topic.
- This study presents novel open research questions, issues, challenges, and future research instructions that offer a road map for the researchers to develop new approaches regarding integration of SDN and IoT.

2. Methodology

In this section, the methodology for the topical review of SDN-IoT is presented. The research selection procedures and analysis are outlined. This study provides an overview of recent research conducted on SDN orchestration for IoT interplay, with a specific focus on the role of CC, EC, FC, or BC as crucial facilitators. To comprehend the central theme of the study, we begin by providing background information on related terms. Subsequently, we explore several studies in the SDN-IoT paradigm. Lastly, we discuss the issues, challenges, and future directions in this scope. The organization of the study is given in the last subsection of this section.

2.1. Research Selection Method. We conduct a comprehensive search on Google Scholar, IEEE Xplore, Scopus, and ScienceDirect databases to identify papers that are most relevant to our inquiry. We utilize the following keywords and phrases when doing a search for articles that encompass the topics of (i) "SDN + IoT", "SDN + IoT + Architecture", "SDN + IoT + Framework", and "SDN + IoT + Solution"; (ii) "SDN + IoT + Edge computing"; (iii) "SDN + IoT + Cloud computing"; (iv) "SDN + IoT + Fog computing"; (v) "SDN + IoT + Edge + Cloud", "SDN + IoT + Fog + Cloud", "SDN + IoT + Edge + Fog", and "SDN + IoT + Edge + Fog + Cloud"; (vi) "SDN + IoT + Blockchain"; and (vii) "SDN + IoT + 5G/6G + mobile network". This methodical technique yields a total of 182 articles. After removing the identical papers, we get 126 articles. Of those, we carefully choose 92 articles using the following criteria for the inclusion process:

- Research articles available online of the last decade
- Studies include the advantages of combining EC and/or FC and/or CC and SDN technology in IoT environment
- Studies that use BC-based solutions for SDN-IoT
- 5G/6G enabled network for SDN-IoT

The following are the steps of the exclusion process that are applied to the articles:

- Studies that have inadequate descriptions of the proposed model
- Articles that are not written in English
- Studies that do not include SDN-IoT solutions

A methodology for selecting the papers through inclusion/exclusion phases is presented in Figure 4, where it is seen that 59 full-text articles can be accessed among the 92 screened articles, of which 50 articles are selected for this study. Figure 5 provides a taxonomy of related SDN-IoT works in different orchestration, including SDN-IoT, CC, FC, EC, BC, and mobile network. This taxonomy visually categorizes the various aspects of SDN-IoT research, emphasizing the diverse areas of interest and the integration of SDN-IoT with other emerging technologies. Figure 6 presents the published articles in SDN-IoT systems based on the year included in this study after being filtered by inclusion and exclusion criteria.

2.2. Organization of the Study. This article is organized as follows. Section 3 describes some related review studies and their limitations. Section 4 gives the definition of IoT, SDN, DC, BC, and next-generation cellular technologies with fundamental specifications. Moreover, it presents the architecture of the SDN-IoT environment, after a thorough analysis on these platforms. Section 5 investigates on SDN-IoT systems based on architectures and other variety of fronts (e.g., models, frameworks, and solutions). Section 6 presents studies on SDN-IoT with DC where separate subsections for CC, EC, and FC are included. Section 7 looks into the studies conducted on SDN-IoT with BC. Lastly, very few works that involve 5G/6G mobile networks in this scope are looked over in Section 8. Section 9 explains current challenges and future study directions, and lastly, Section 10 concludes the article. The acronyms and abbreviations used in this paper are summarized in Table 1 to ensure clear understanding of the terminology.

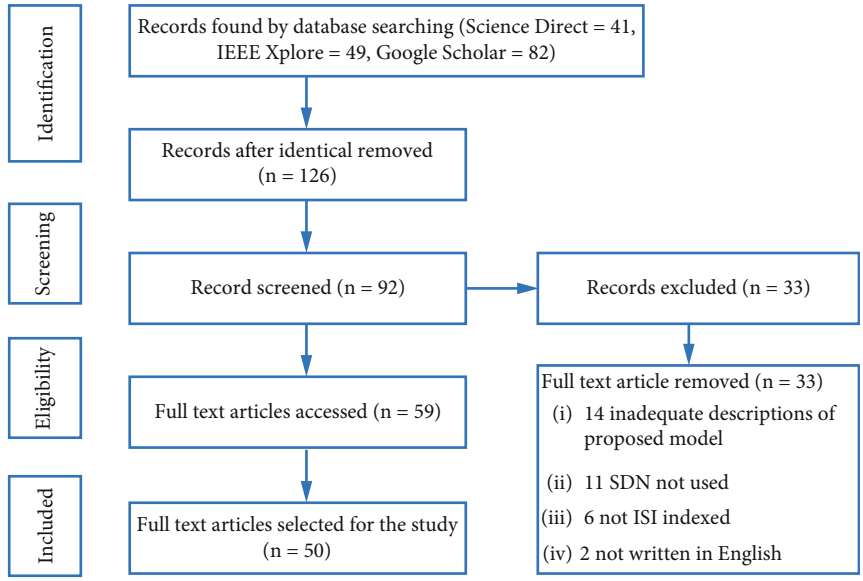

FIGURE 4: PRISMA diagram of the selection procedure and literature search of the research papers of this study. The search string used in this study is ("Cloud computing" or "Fog computing" or "Edge computing" or "Blockchain" or "mobile network" or "5G" or "6G") and ("Software Defined Networking") and ("Internet of Things").

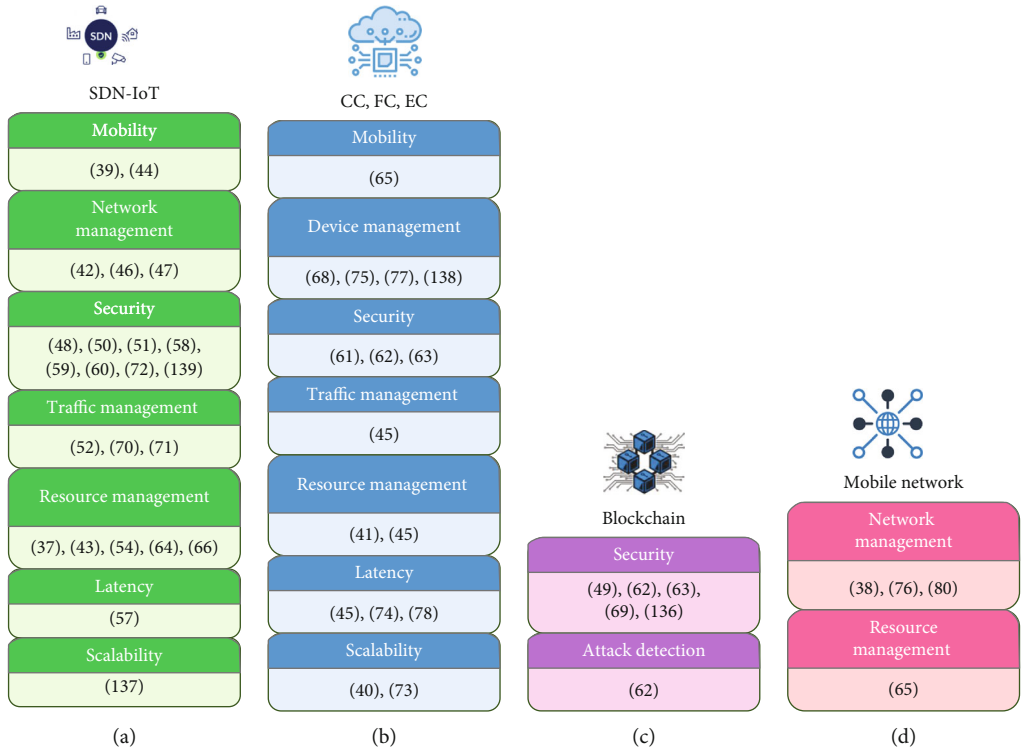

FIGURE 5: Taxonomy of related SDN-IoT works in different orchestration: (a) SDN-IoT; (b) cloud, fog, and edge computing; (c) blockchain; and (d) mobile network.

This research includes 50 articles that proposed SDN-IoT systems and other technologies with it to enhance the system performance. The articles are classified by the underlying working area, such as security, access control, resource management, traffic management, mobility, latency, and IoT services, and grouped by DC, BC, any combination of these, and mobile networks. The statistical measurements of working areas in the analyzed articles are shown in Figure 7. It is clear that most of the researches are conducted in security area. After that, mobile network, traffic management, and resource management are dominant areas.

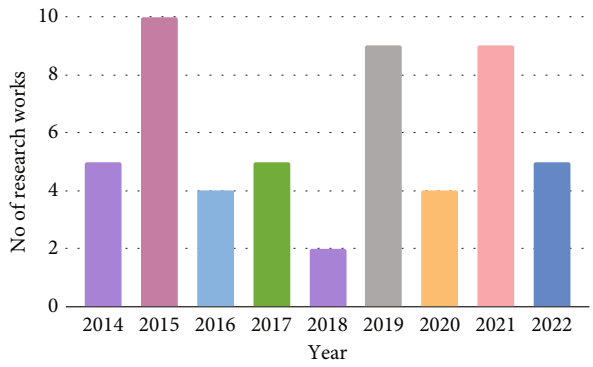

Figure 6: Published articles in SDN-IoT systems based on year included in this study.

Table 1: Acronyms and abbreviations.

IoT	Internet of things
SDN	Software-defined networking
FC	Fog computing
EC	Edge computing
CC	Cloud computing
DC	Distributed computing
BC	Blockchain
SDN-IoT	SDN for IoT
SD	Software defined
WSN	Wireless sensor network
DDS	Data Distribution Service
DoS	Denial-of-service
SaaS	Software as a Service
OF	OpenFlow
IIoT	Industrial IoT
QoS	Quality of services
E2E	End to end
PC	Principal controllers
SC	Secondary controllers
LC	Local controllers
ICN	Information-centric networking
ICMP	Internet Control Message Protocol
TCP	Transmission Control Protocol
ONF	Open Networking Foundation
RFID	Radio frequency identification
REST	Representational state transfer
NFV	Network function virtualization
API	Application programming interface
NETCF	Network Configuration Protocol

3. Literature Survey and Comparison

The past few years have seen the completion of numerous reviews on various topics related to SDN-IoT [13, 21, 22]. A comprehensive examination of the key obstacles that need to be addressed to ensure the effective support of IoT systems was presented in [22]. The authors also proposed an IoT architecture associated with SDN and Data Distribution Service (DDS) middleware, which introduces adaptability to the network when SDN is used for IoT system. In the later year, an extensive survey of various SDN solutions that are valuable for meeting the specific needs of IoT across various networking domains, including core, access, edge, and data center networking, was offered in [22]. The authors in [23] walked in the same manner, providing a comprehensive overview of the significant SDN-IoT frameworks. They focused on four trends, namely, network function virtualization (NFV), OpenFlow (OF), middleware, and BC. Again, there is no association of cloud or FC, 4G, or beyond mobile network technologies in SDN-IoT. The study in [24, 25] provided a thorough analysis of the solutions based on SDN that aim to address the primary difficulties of the IoT associated with FC. In the following year, the emergence of EC to address the obstacles of IoT systems while processing, filtering, and storing huge amounts of data was focused on in [26], where the authors concluded that the complexity of the EC architectures could be reduced by the SDN in IoT scenarios. Afterwards, the same concept was presented in [27], where the survey suggested the use of SDN and EC to efficiently orchestrate IoT services and manage the infrastructure. Some studies presented the security features offered by SDN-IoT.

The security measures implemented by SDN, outlining the various approaches that can be employed to oversee, maintain, and respond to security risks in the context of IoT, were surveyed in [13]. Later in [28], the authors highlighted the same role of SDN-IoT network security. The authors also surveyed different proposed NFV, SDN/NFV, and BC-based solutions for ensuring the security of the IoT network against newly developing threats. BC enables the secure exchange of data and ensures the integrity of records, which is essential for handling sensitive IoT data, which is rarely studied in the found literature. For example, the article [29] outlined the potential opportunities and significant obstacles that need to be addressed when contemplating the use of SDN in hybrid cloud-fog systems to facilitate 5G and future-enabled IoT devices and applications but the authors missed analyzing the significant role of BC. The authors in [28] reviewed another study where the importance of integrating SDN and IoT was highlighted [30]. Recently, like the study in [26], the authors in [31] provided a survey on SDN-based architectures in edge-IoT systems. Like most studies found in the literature, the authors did not mention the significance of fog- and cloud-associated systems.

The convergence of edge, fog, and cloud in SDN-IoT is aimed at overcoming obstacles. The edge serves as the local filter and initial responder, while the fog enhances processing capabilities for preprocessing. The cloud, on the other hand, offers storage, analysis, and orchestration capabilities. This trio of components guarantees effective and immediate management of data, while BC technology ensures the protection of data transmission, thereby establishing a secure and efficient pathway for the interconnected future. Several

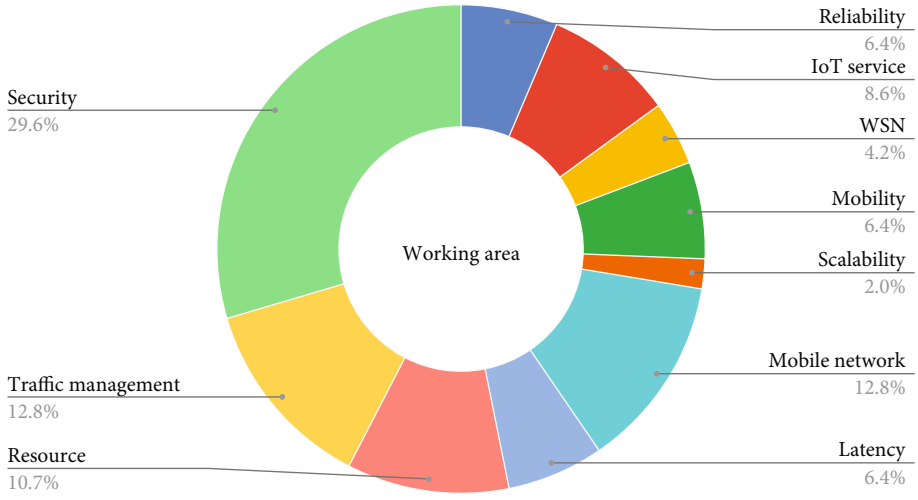

Figure 7: Distribution of the SDN-IoT research papers according to their working area.

studies discussed the integrated perspective of SDN-IoT and associated application domains. The majority of these studies focused on a specific SDN-IoT environment in the literature. Security issues were significantly focused on many studies [32, 33] and some studies included CC [34], EC [35], EC and CC [36], FC [37], DC [38], and mobile networks [39] for IoT, but they were not associated with SDN. Though the authors in [21] covered all these areas related to SDN, the outstanding role of BC in the SDN-IoT paradigm was uncovered. The studies that are now accessible offer a view of how SDN-IoT integrates with DC. Still, the majority of them ignore the significant topic of 5G/6G technology and BC, which is addressed in this study. This study is a unique model that exists at the convergence of SDN, IoT, DC, BC, and mobile networks; there are not any survey papers on the SDN-IoT, DC, BC, and mobile networks from a complete viewpoint encompassing the architecture, management, security, and many more. Table 2 compares the current study with other review studies that have already been conducted under this paradigm and shows that the existing literature falls short of offering a thorough analysis of the SDN-IoT and its deployment with DC, BC, and next-generation cellular technologies.

4. Background

The rapid growth of IoT devices has led to the emergence of new technologies and paradigms to manage and process the vast amount of data generated by these devices. SDN is a networking paradigm that allows for efficient and flexible network management and control, while CC provides a scalable and cost effective platform for data storage and processing. However, the traditional cloud-based architecture may not be able to provide the low latency and real-time processing required by many IoT applications. To address this challenge, FC and EC have been proposed as complementary paradigms that bring the computing resources closer to the IoT devices and applications. Furthermore, the emergence of BC technology has provided a secure and transparent way of managing IoT devices and data. Finally, the upcoming 5G/6G networks promise to bring even faster and more reliable communication capabilities, enabling new use cases and applications for IoT. In this section, we will define and explore the fundamental specifications of SDN, IoT, SDN-IoT, CC, FC, EC, BC, and 5G/6G and their respective roles in supporting IoT applications in individual subsection.

4.1. SDN. The term "SDN" was first used to describe the concepts and work surrounding OF at Stanford University in Stanford, California, United States [44]. Open Networking Foundation (ONF) [45] is devoted to creating, standardizing, and commercializing SDN for the transport and IP network layers. Three layers [46–50] make up the SDN architecture, and they all communicate with one another via northbound and southbound application programming interfaces (APIs). The division of the control plane and data plan is the core of SDN. There is also an application plane, which informs the control plane of its requirements. The OF or network configuration (NETCONF) protocols standardize the southbound interface, which the controller uses to program the data plane [51]. However, OF cannot be the only SDN protocol because there are other protocols like BGP [52], ForCES [53], LISP [54], NETCONF [55], OVSDB [56], and OpenState [57]. But they are less traditional protocols. There is currently no standard for the northbound interface. Still, a representational state transfer (REST) API, for instance, may be developed to allow applications to communicate their needs to the network [58]. The network management orchestration of SDN is shown in Figure 8.

4.2. IoT. When it comes to the IoT, everything from cars to refrigerators is linked to the web in novel ways that go beyond what humans can accomplish. Identifiable and interconnected things can take the shape of either real or digital entities [50]. The data is collected, managed, communicated, stored, and processed by the IoT devices and objects. IoT's application extends across diverse industries and scenarios, presenting inventive solutions to enhance efficiency, connectivity, and

Table 2: A comparison of previous surveys on SDN-IoT systems.

References	Author	Publication year	SDN	IoT	CC	FC	EC	Mobile networks	BC
[13]	Farris et al.	2019		✓	✓			✓	
[21]	Jazaeri et al.	2021	✓	✓	✓	✓	✓	✓	
[36]	Yu et al.	2018		✓	✓		✓		
[40]	Pan and McElhannon	2018	✓	✓	✓		✓		
[34]	Botta et al.	2016		✓	✓				
[38]	Elazhary	2019		✓	✓	✓	✓		
[37]	Mukherjee, Shu, and Wang	2018		✓		✓			
[39]	Javed et al.	2018		✓				✓	
[22]	Hakiri et al.	2015	✓	✓					
[41]	Alam et al.	2020	✓	✓					
[42]	Panarello et al.	2018		✓					✓
[43]	Wang et al.	2019		✓					✓
This study			✓	✓	✓	✓	✓	✓	✓

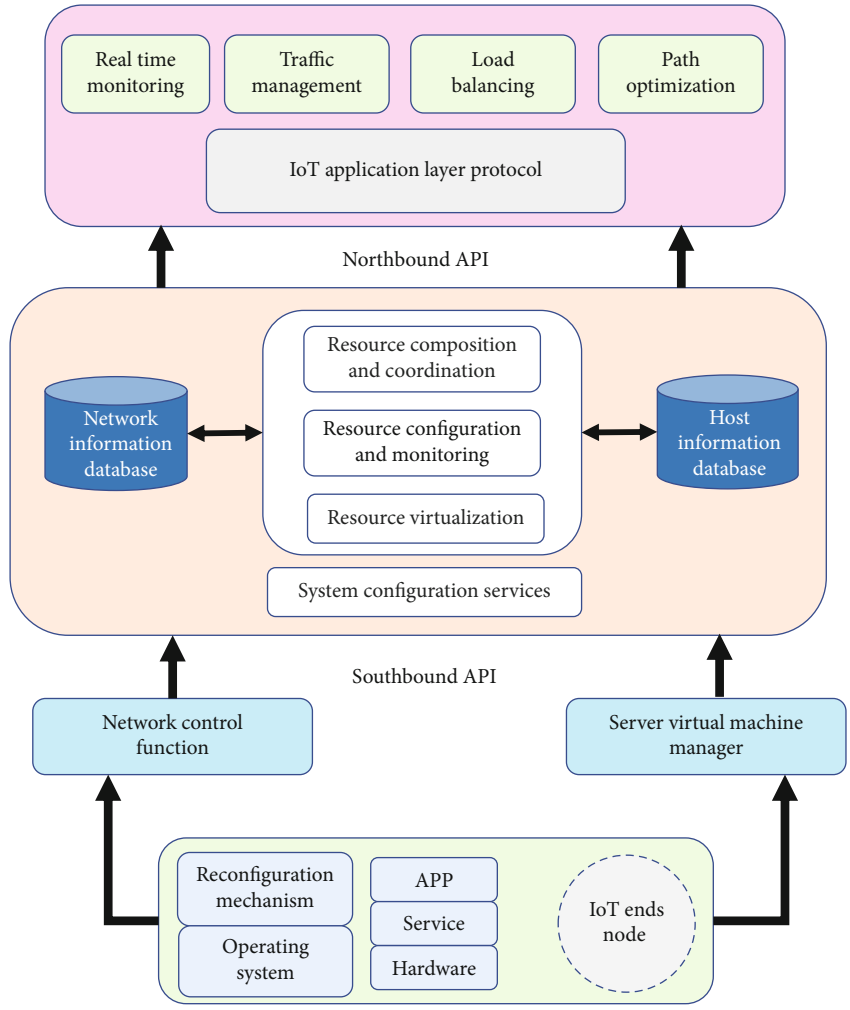

Figure 8: SDN orchestration.

decision-making. IoT integration is crucial for the evolution of smart cities, empowering them to boost efficiency, connectivity, and data-driven decision-making across diverse urban sectors. Whether optimizing transportation systems, managing energy intelligently, or enhancing urban infrastructure, IoT deployment fosters the creation of agile, sustainable urban

environments that respond effectively to evolving needs [59]. In addition to the inherent difficulty of coordinating a wide variety of disparate sensing devices, the IoT is complicated by the sheer number of objects that can connect to the network and exchange data with one another under the umbrella of a wide variety of different protocols and network models [60].

4.2.1. IoT Architecture and Layers. Numerous paradigms and frameworks for IoT have been presented in literature. Some proposed architectures have three layers/domains [22, 48, 50, 60–63], while others have four [22, 63] which are discussed below.

4.2.1.1. Sensing Layer. The sensing layer is the layer that contains physical objects and devices like sensors and actuators. This is the "perception and device layer/domain," among other names. Edge nodes (sensors) are in charge of sensing, collecting, and delivering data to other network devices (sink or gateway).

4.2.1.2. Network Layer. The network layer is where we see examples of the various protocols used for exchanging data in the IoT, such as ZigBee, Bluetooth, Wi-Fi, and cellular. The network domain/layer is responsible for transmitting information gathered at the sensing layer from the actual physical objects.

4.2.1.3. Application and Service Layer. The data gathered by the devices is sent to the next tier, the application and service layer, where it is evaluated and stored in the cloud or on servers. This domain/layer encompasses all services and applications related to the IoT that are necessary to the end user or the system.

4.2.1.4. Middleware Layer. To provide bidirectional communication between objects and devices in the IoT provided by different suppliers without regard to hardware and vendor details, a "middleware layer" provides addressing and service management. The IoT architecture and its layers provide a scalable and flexible framework for integrating devices, data, and applications in the IoT ecosystem. By leveraging this architecture, organizations can develop innovative IoT solutions that enhance efficiency, productivity, and customer experiences.

4.2.2. IoT Components. As we discussed previously, the IoT layers serve as a classification system for the various components that make up the IoT. There are specialized parts for each layer's tasks. Sensors, WSNs, radio frequency identification (RFID) tags [3], edge node machines, mobile devices, and actuators are all part of the sensing layer [63]. Aggregation components, represented by things like sink nodes, WSN services tailored to the needs of the client and the system, process and analyze the data as it passes through the application/service layer. One of the biggest problems with the IoT is all the variety of gadgets, services, apps, technology, etc. Examples of such heterogeneity include the sensing layer's use of Bluetooth, ZigBee, and other technologies [48]. It is important to note that different communication technologies are utilized to guarantee connectivity at different tiers, including the network layer and the application layer. Wi-Fi, cellular, and similar technologies are all supplied by various suppliers and manufacturers. Service providers evaluate virtualization options to enhance resource use and decrease management headaches. The fundamental difficulties of the middleware layer are the efficient and rapid installation of services and applications and the utilization of data resulting from the IoT [22].

4.3. SDN-IoT. SDN-IoT refers to the convergence of SDN and IoT technologies. It is an architecture that uses SDN principles to manage and control IoT devices, allowing network administrators to centrally manage and automate the deployment, configuration, and maintenance of IoT networks. IoT constitutes some issues like unpredictable network circumstances, varied communication technologies, application specific quality-of-service (QoS) needs, and tremendous data influx that SDN can handle, as it is a potential strategy for unifying network control through rule-based administration. SDN's abstractions make it possible to govern the network holistically using high-level policies without worrying about low-level setup concerns. Therefore, it is advantageous to handle the heterogeneity and application-specific needs of IoT. The integration of IoT with SDN enhances IoT performance and security by enabling complete remote control of NETCONF without necessitating close proximity to IoT devices. The SDN controller in the IoT with SDN framework empowers the network to be divided into discrete subnets. The SDN controller uses the northbound API to connect with the IoT application. This analyzes the network traffic and acts in accordance with the established rules. On the other hand, the controller interacts with network switches using southbound API following configured rules. The general architecture of SDN-IoT is illustrated in Figure 9, which supports IoT applications.

4.4. EC. EC refers to a DC paradigm where computing resources and application services are deployed at the edge of the network, closer to the end-users and IoT devices, to enable faster data processing, real-time decision-making and reduce network latency and bandwidth consumption. The combination of EC and SDN has helped to address numerous issues and uncertainties. Using EC on open-source platforms with SDN management results in a simplification of dependability, real-time, and secure operations, with the added benefit of growing the number of linked entities and valuable data that IoT devices provide. EC and SDN can assist in handling IoT big data [18]. In the past several years, edge-enabled devices, including smart phones and health wristbands, have been extensively released on the market. These cutting-edge gadgets execute multiple services, generate and transfer data to the network, and continually build data logs. Even so, the majority of IoT devices still have little computational power and constantly require intermediate computational power from outside the IoT. The incorporation of EC into SDN-IoT seamlessly facilitates network administration and enhances mobility. Within

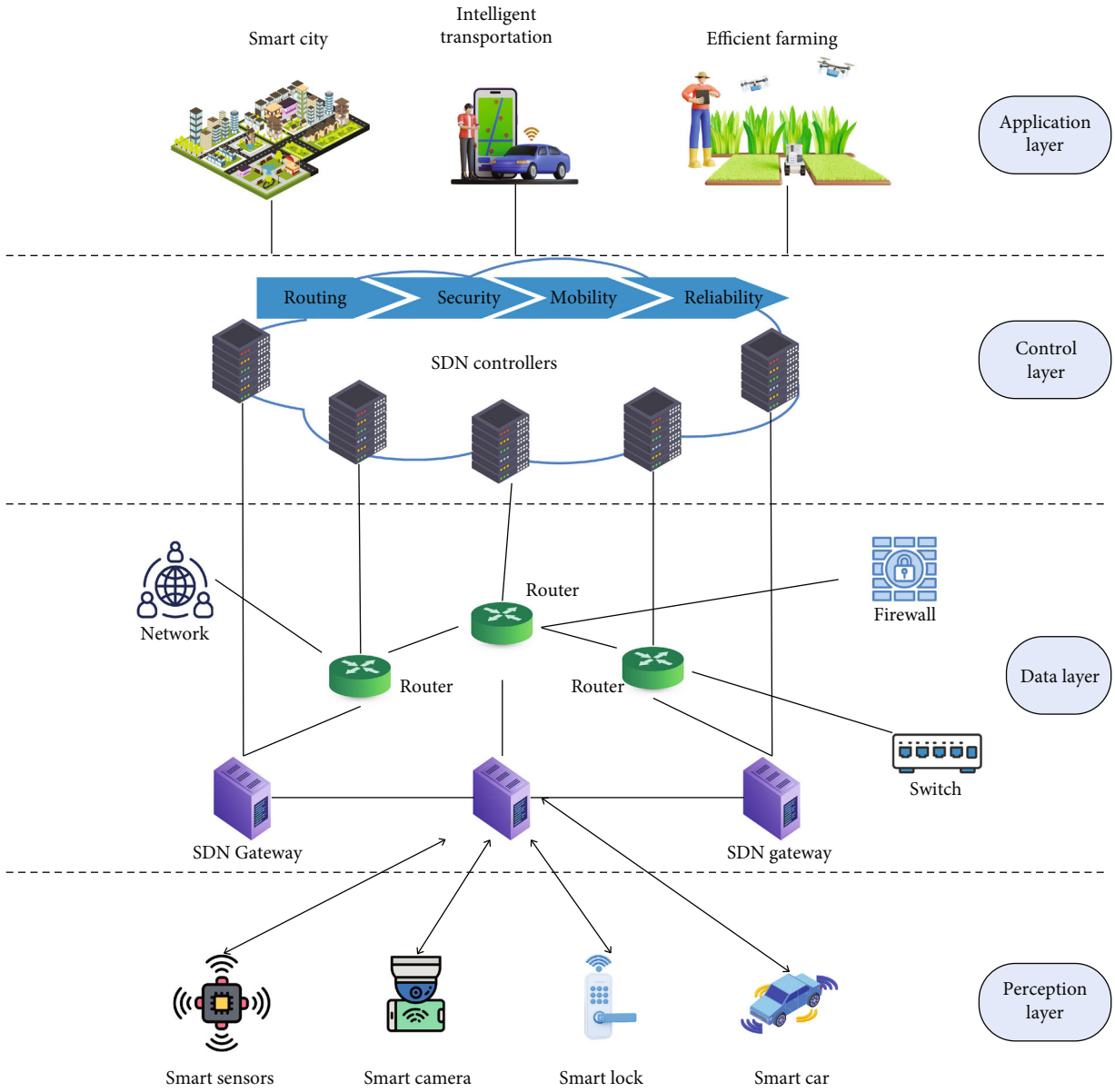

Figure 9: SDN-IoT architecture.

SDN-IoT networks, EC enables streamlined resource management, virtualization, and unified control, thereby optimizing the deployment of IoT devices. Utilizing EC for data offloading mechanisms and flow classification in SDN-IoT significantly enhances network efficiency while concurrently reducing latency [64]. In addition, edge devices can move jobs that require more computing capacity to the cloud infrastructure [65]. Thus, several of the challenges and complexities of IoT systems can be solved by integrating EC with SDN.

4.5. CC. Driven by the ever-expanding network of interconnected devices that generate and process data, the IoT is revolutionizing businesses. Three key technologies are at the center of this revolution: CC, SDN, and EC. CC serves an important supporting role, functioning as the brains and muscles behind the scenes, while EC and SDN take center stage in controlling and processing data at the network edge. CC refers to the use of remote servers and networks to store, manage, and process data and applications, which can be accessed over the internet. It provides users with the ability to access and use these resources as needed, without requiring them to own or manage the underlying infrastructure. Cloud providers use resource pooling to combine multiple computing resources into a single virtual resource. In order to guarantee flawless services all across the communication process, the data centers and users' applications must be balanced by the SDN control layer, which is connected to the cloud [65]. Cloud architectures featuring both a single SDN controller and several controllers were proposed by Mayoral et al. [66]. Through the strategic utilization of CC within SDN-IoT networks, organizations can elevate

network flexibility, optimize resource utilization, and foster the creation of real-time applications. Architectures integrating cloud-based SDN-IoT additionally support the seamless incorporation of EC, empowering data processing and analysis at the network periphery. This results in expedited response times and minimized latency. CC can be utilized to store and display the resulting data for later usage by a wide variety of users and applications [22]. Additionally, cloud-based services can be used to deploy and manage SDN controllers and applications, enhancing the overall efficiency and functionality of SDN-IoT.

4.6. FC. FC is a decentralized computing model that brings computation and data storage closer to the edge of the network, usually at the edge of the LAN or on a gateway device. The concept of FC was inspired by the natural occurrence of fog and clouds where fog is closer to the ground [67]. It relies on low-latency communication between devices and fog nodes, allowing for real-time data processing and decision-making. Fog serves as a bridge between the cloud and the IoT, facilitating communication. As a result, it maximizes the potential of each technology, expanding the CC application space and improving IoT resource availability. SDN has been presented as a potential approach that can manage communication network traffic and is compatible with the FC network architecture [68]. By harnessing the capabilities of SDN for centralized control and programmability and integrating them with the decentralized nature of FC, organizations can establish a more agile and scalable infrastructure tailored for IoT deployments. The synergy of FC in SDN-IoT empowers localized tasks, including on-site data processing, real-time analytics, and immediate decision-making at the network's edge. This approach diminishes the necessity to transmit all data to centralized cloud servers, resulting in diminished latency, reduced bandwidth usage, and an overall enhancement in system performance. Moreover, the amalgamation of FC and SDN within the IoT landscape facilitates the deployment of applications demanding real-time responsiveness, such as industrial automation, smart cities, and healthcare monitoring. The hierarchy of IoT systems with the three types of DC is illustrated in Figure 10.

4.7. BC. BC serves as a decentralized global ledger, housing a set of data records. Operating on a peer-to-peer network, BC technology allows users to conduct transactions directly, eliminating the need for intermediaries [69]. BC is a developing collection of records recorded in the form of a Merkle tree linked to cryptographic rules, with each block containing the cryptographic hash of the block before it. The structure of the BC can be understood by considering the total number of transactions [70, 71]. Peers that are linked to a BC have the ability to cancel any invalid transactions that are submitted to the network. When it comes to IoT security, using BC provides assurance. Information can be transferred using BC technology and the Paillier cryptosystem. The Merkle tree [72] generates hash keys that are then stored in the BC. IoT may be made more secure and scalable using SDN and BC technologies. For security purposes, BC transactions are carried out with as little extra effort as feasible [73]. Third-party authentication methods lack the security features of BC technology. Security issues with the IoT are eliminated when this technology is implemented [74]. BC's significance stems from the fact that it is distributed, uses asymmetric encryption, requires less storage space than traditional methods, and is decentralized. BC technology has also improved public sector services [71]. Authentication requires users to provide their own distinct identities. A BC platform has recently been proven capable of managing IoT devices [75]. Thus, the public key and signature of each device are crucial for addressing security issues. The demand for security is increasing in SDN-based IoT, and BC is an effective approach to providing that security in a manner that scales well with the infrastructure [76]. BC's characteristics might be improved by including IoT and SDN. Integrity, authenticity, secrecy, nonreputation, and availability are essential for system security [77]. IoT security can be improved using these BC characteristics.

Decentralized and distributed BC is great for improving IoT. This method eliminates single points of failure and creates a more robust device ecosystem. BC's cryptography would safeguard data. BC can help track billions of linked devices, perform transactions, and coordinate devices [78]. The application of BC in SDN-IoT networks offers several advantages, including enhanced security, privacy, and transparency for IoT devices and data transactions. By integrating BC technology, the SDN-IoT network can ensure automatic control security and confidentiality for smart building applications. Additionally, BC technology allows for the permanent storage of transaction data, thereby improving safety and privacy within the network. Furthermore, the combination of IoT, SDN, and BC technologies can provide reliable data transmission and communication within the network, addressing the complexities and security concerns associated with IoT devices. This integration offers a promising solution for managing and securing IoT devices and data within SDN-based networks. A general architecture of distributed network management for IoT devices using BC and SDN controllers is shown in Figure 11.

4.8. Next-Generation Cellular Technologies. 5G is the fifth generation of mobile network technology, which offers faster data transfer rates, lower latency, and more reliable connectivity compared to 4G. It uses a combination of advanced technologies such as beam-forming, massive MIMO, and millimeter-wave frequencies to achieve higher speeds and better connectivity. 6G is the expected successor to 5G, which is still in the early stages of development. SDN can be employed to offer a general architecture that will allow 5G/6G to operate throughout a control plane. As a result, improved data flows can be provided when data travels across the network. Network slicing, a pivotal element in 5G networks, elevates the notion of virtualization to unprecedented heights. Imagine partitioning a singular physical network into distinct, virtual slices tailored to specific requirements. Here, SDN emerges as an ideal collaborator, utilizing its programming capabilities to dynamically configure and oversee these slices with agility and precision [79]. Additionally, SDN architecture can increase latency and

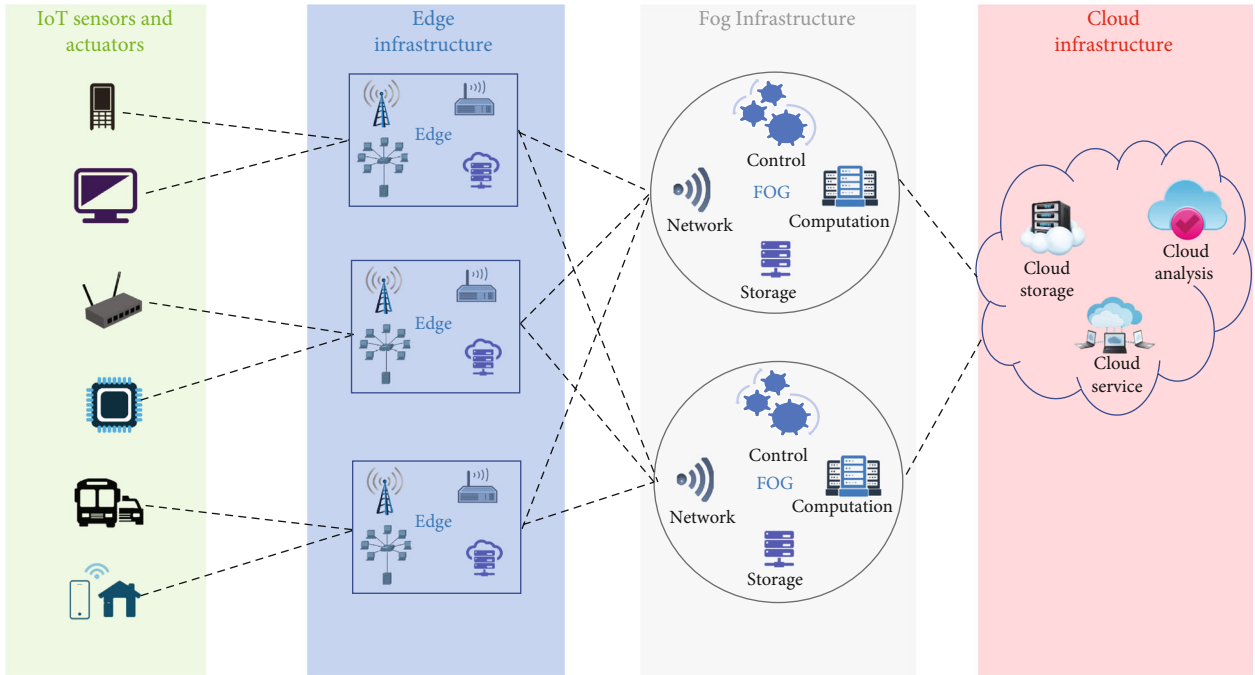

Figure 10: Hierarchy of IoT system with DC.

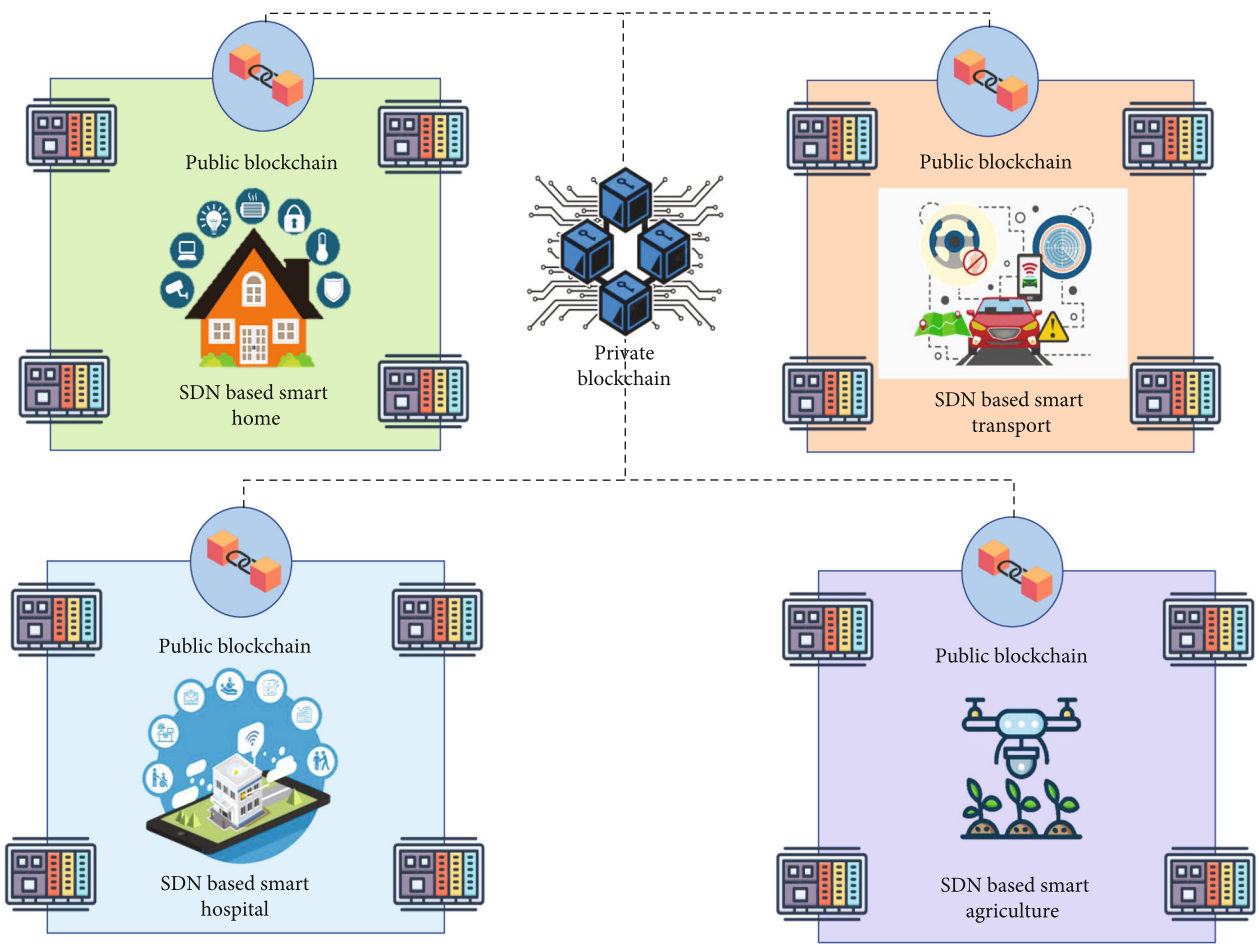

Figure 11: BC enabled SDN controller architecture for IoT network.

decrease network bandwidth. Lastly, because SDN can be used for 5G/6G networks, it offers a method for managing and automating network redundancy from a centralized control plane, avoiding severe failures by figuring out the best data flows in real-time. The 6G communication technology offers a high level of interoperability. Its interoperable nature makes it simple to integrate diverse networks like the IoT. SDNs are used to manage this connection in order to control how well users receive QoS, regardless of the IoT application.

5. SDN-IoT Architectures, Frameworks, and Solutions

This section explores the constantly evolving topic of SDN-IoT, with a specific focus on the various features of architectures, frameworks, and solutions presented by academics to deal with the emerging difficulties in the area of IoT. An architecture refers to the overall structure of a system, including the components, their relationships, and the communication mechanisms between them. Frameworks and solutions are set of guidelines, protocols, and tools that provide a structured approach to building a system. Table 3 provides a comparison of the existing literature on the SDN-IoT systems based on architectures, models, frameworks, and solutions.

5.1. Security Provisioning Architectures. Security concerns have been raised as an important area since IoT devices are internet-based and contain sensitive and confidential data [97]. Several academics are looking into ways to make the system more secure. Sahoo KS, Sahoo B, and Panda [98] proposed an architecture based on SDN with distributed controller for IoT and ad hoc network to provide secure communications between extended SDN domains. To allow secure, cross-domain connectivity across the enlarged SDN domain, border controllers are developed as specialized controllers. It is a component responsible for interconnecting multiple SDN domains. It acts as a gateway between different SDN domains, allowing for communication between them while maintaining their independence in case of failure. If it fails, any other controller within the domain will assume its responsibilities. All controllers have been outfitted with a security grid to deter infiltration attempts. Another secured network architecture was proposed by Olivier, Carlos, and Florent [99]. They proposed a distributed network access control architecture that uses SDN to tackle the security issues in IoT and ad hoc network, enhancing the security policies between SDN control domains based on the grid of security paradigm. Two new architectures were proposed: one with multiple SDN controllers in equal interaction and another that is scalable with multiple SDN domains. In the latter, each controller is responsible for its own domain and communication between domains is facilitated by them. There are several security attacks on which the author should have worked on.

5.2. WSN and IoT Synergy. One mentionable paradigm is resource management, as maximizing the utilization of resources is a must. El-Mougy, Ibnkahla, and Hegazy [62] proposed an information-centric networking (ICN) architecture based on SDN that addressed end-to-end (E2E) resource management in wireless networks. They also presented WSN management and the role of ICN as a SaaS enabler. Another work for wireless networks was carried out by Bendouda, Rachedi, and Haffaf [100], where they proposed a programmable architecture using SDN to tackle the heterogeneity of wireless networks in IoT for reducing traffic load. In addition to considering the variety of network technologies, the primary objective was to decrease the overhead associated with network control techniques. The proposed semidistributed architecture has three control levels, as opposed to the traditional SDN, consisting of principal (PC), secondary (SC), and local (LC) controllers.

5.3. Industrial IoT (IIoT) Architectures. Significant progress has been made in IIoT-related fields like industrial wireless networks, SDN, and the cloud in recent years. These new tools have the potential to usher in the fourth industrial revolution, often known as Industry 4.0, by facilitating widespread improvements in the manufacturing sector. Large numbers of IIoT network nodes require a large number of decentralized controllers. In practice, coordinating and interacting with these controls is difficult. Huo et al. [84] presented a traffic measurement scheme tailored to these networks, intending to accurately measure the traffic on SDN-based IoT networks with minimal overhead. Through request messages sent to OF-based switches, they could gather both the aggregate flow traffic data and the detailed link traffic statistics. Next, they suggested an objective function to reduce estimation errors and simulated annealing to estimate network traffic based on the coarse-grained flow measurement.

5.4. IoT Management Frameworks. Jararweh et al. [101] proposed a software-defined (SD) IoT framework to make the IoT management process more straightforward and bring an effective solution for the issues in the conventional IoT architecture to transmit, store, and secure the generated data from the IoT gadgets by integrating the SD network, SD storage, and SD security into a single SD control model. Their proposed architecture had three main components: the physical layer, which was classified into several clusters like sensor network cluster, database pool cluster, security appliances cluster, etc., the control layer, and the application layer. For SDN-based IoT networks, several management areas are crucial that we will be discussing next.

5.5. QoS Provisioning Frameworks. Due to the enormous traffic volumes generated by IoT devices, achieving the QoS has become challenging. An SDN-based control and management framework was proposed by Montazerolghaem and Yaghmaee [92] to meet the QoS requirements of different IoT services and make the balance of traffic between IoT servers at the same time. The authors constructed a controller that is predictive and made adjustments depending on data utilizing modules that were based on OF, sFlow, time-series analysis, and fuzzy logic. This controller can also look back in time. Every component of the proposed system,

Table 3: A taxonomy of the previous literature on SDN-IoT.

Research area	Solution/ architecture	Proposed model	Contribution	Future scope
Mobility and gateway access [22]	Architecture	SDN-DDS Architecture distribution of IoT systems and brought pliancy to the network	Improved service	Improving the security and traffic management
Networking infrastructure [80]	✓	Multinetwork information architecture (MINA)	Enabled pliable, feasible, and proficient management on task, flow, network, and resources	Improving the routing protocol
Device and network management [81]	✓	Soft-WSN architecture	Focused on both system control and structure tracking and made thing more adaptable	Analyzing the hardness of putting flow table into place
Security space [82]	✓	Rol-Sec for SDN-IoT	Improved strength of the security space	Trying to mitigate more security issues
Green management [83]	✓	SDN controller dynamic architecture	Optimized network responsiveness	Implementing the network-related machine learning (ML) techniques
Traffic management [84]	✓	SDN-based IoT network traffic measurement scheme	Measured network traffic with low overhead and high accuracy	
IoT resource [85]	Framework	RESTful framework for IoT based on SDN	Transformed IoTs into web resources that can be perceived and managed through a uniform interface	Leading more complex implementations to fortify the robustness
Application layer network protocol [86]	✓	Hybrid communication framework	Made HTTP, CoAP, and MQTT be able to share data in IoT system	Improving security rate and improving the reliability
Reliability and latency [87]	Solution	Atomic-SDN	Provided high reliability and reduced latency in low power WSN	Working on the security of low power WSN
Privacy and information leakage [88]	✓	Privacy-preserving method	Preserved privacy by splitting the data and provided no leakage of information	Working on more metrics for making high-level decision
Virtual manufacturing applications [89]	Framework	Cybersecurity-resilience protection mechanism	Assured the security of SDN applications and assured the reliability	Implementing the methods on the IoT testbed
Access control [90]	Solution	Access control solution for CoAP	Provided the access control security	Changing the link modifier after sometimes
Rule caching cost [91]	Technique	QoS Aware Optimum Path Selection and Rule Caching Policy (QOPS-RCP)	Determined the optimal path that assures the QoS constraints and designed a RC policy	
IoT services and traffic management [92]	Framework	Novel SDN-based control and management framework	Met the QoS requirements of different IoT services and made balance of traffic between IoT servers at the same time	Investigating how SDN's decentralized control plane and multidomain networks affect IoT QoS management
Security (mitigating man-in-the-middle attack) [93]	Solution	A novelty solution of system model using SDN	Protected HTTP-based IoT devices from intrusion	Analyzing the scalability of the system
Controller selection, scalability [94]	Model	Analytical network decision-making process (ANDP) model	Selected the SD-IoT controller based on its features and performance validation	
Data aggregation, security [95]	✓	Distributed and AI-based energy-efficient model	Improved data aggregation and power management and offers security and authentication	Evaluating the ability of the model and made use of cloud services
Security [96]	Framework		Enhanced the security and resilience of IoT	Practical implementation for enhancing the flexibility and reliability

including Open vSwitch, the Floodlight controller, and the Kaa IoT servers, has been implemented in a testbed that simulates the actual world. But there is no investigation of how SDN's decentralized control plane and multidomain networks affect IoT management.

5.6. Security Solutions. Al Hayajneh, Bhuiyan, and McAndrew [93] proposed a solution to counteract man-in-the-middle attacks. They offered a system paradigm using SDN and the IoT. They used SDN for securing HTTP-based IoT devices, mitigating and preventing security assaults without modifying the IoT devices themselves. They also used SDN and deep packet inspection to implement ways for separating traffic. Nevertheless, this solution could be used to handle other prominent attacks.

5.7. Mobility Solutions. Another critical challenge of IoT networks is controlling the data traffic from edge devices to the cloud and mobility management. Wu et al. [102] proposed a solution named UbiFlow to provide global flow control, mobility management, and fault tolerance in a SD IoT heterogeneous network. They also offered an algorithm for the controller to find the access point available to devices. They also made a load balancing scheme by experimenting with the difference in flow traffic characteristics. Nevertheless, they could implement IRS technology to reduce data loss.

6. SDN-IoT and DC

As we have discussed earlier, a number of publications have recently proposed several architectures for the integration of SDN and IoT technologies. Among those, we have found a significant number of studies that added the topics of DC. Some of these are detailed in this section. Table 4 compares and assesses several proposed approaches to SDN-IoT network research implemented with DC in terms of their research area, cloud domain (i.e., CC, FC, or EC) contribution, and future scope.

6.1. Cloud Systems. A vast amount of data is injected into CC through the IoT network, which is intended to offer the maximum level of flexibility, scalability, and security to all networked entities. Thus, considering CC in SDN-IoT networks is worth meeting the demands of growing applications and users. A framework on the cloud domain was proposed by Nastic et al. [103] to encapsulate fine-grained IoT materials where IoT functionality is wrapped up well APIs to give a complete overview of how to obtain, configure, and run IoT cloud systems. Using automated provisioning processes and support for managed configuration models, the proposed framework made it easier to set up SD cloud-based systems for the IoT. It also allowed for versatile adjustments to be made to these systems while they were running. However, there is no support for the runtime authority of SDN-IoT systems. Huo et al. [105] proposed an ARIMA model for traffic estimation and an AC algorithm for seeking the fine-grained traffic of flows. The authors collected the statistics of coarse-grained traffic of flows and fine-grained traffic of links, modelled the network traffic as ARIMA, and proposed an objective function to decrease the estimation errors. Other models can be applied for traffic measurement, and different optimization algorithms can be studied for the objective function.

6.2. Edge-Based Systems. For SDN-IoT networks, edge-based architectures are promising to support special needs like scalability problems, handling data stream at the edge, traffic load at the core of the network, E2E delay, and IoT services. Sun and Ansari [108] proposed edge-IoT as a way to bring computing resources closer to IoT devices. The goal was to reduce the amount of traffic in the core network and the delay from computing resources to IoT devices from E2E. They moved computing resources closer to IoT devices to reach these goals. To meet the needs of both individual users and IoT service providers, they created a hierarchical FC architecture with scalable and adaptable computing resource provisioning. Mavromatis et al. [107] proposed a framework named SDIM, an IoT device management framework for multiedge, cloud, and multidomain deployments, allowing for the provisioning of devices, the detection of operational faults, and the control of devices across IoT networks. In addition, SDIM enabled SLAs to better regulate expansive sensor networks by capitalizing on granular details. Uddin et al. [109] proposed Muppet, an SDN-based multiprotocol capable edge-switching architecture on edge for large-scale IoT management. Muppet offered low-latency and energy advantages of the peer-to-peer method, along with ensuring wide-area, cross-protocol automation like the cloud-based solutions. The author can use FC to increase the efficiency of the system. But when the network resources are confined, it becomes harder to perform IoT operations dexterously.

For networks with limited resources, Das et al. [110] presented 6LE-SDN, a SDN architecture based on the network's edge that was managed by multicontrollers. Computing was offloaded to the network's periphery in this 6LE-SDN design. It controlled network operations with open-source SDN controllers. The average round-trip time and packet loss were both reduced with the development of the 6LE-SDN architecture and the optimized routing protocol edge-based 6LoWPAN-SDN Protocol (6LE-SDNP). To make it more amenable to devices with limited resources, the 6LE-SDNP protocol combined elements from 6LoWPAN and OF. In this research, they explored how integrating 6LoWPAN with SDN at the network layer can improve network performance in terms of throughput and latency. Latency could have been an unbearable issue for real-time monitoring systems like video surveillance systems. Video cameras and other high data rate sensors are proliferating in the IoT. It will become increasingly challenging to maintain the practice of shipping all collected data to the cloud for processing as the density of high data rate sensors in the IoT grows [117]. In order to support real-time video surveillance applications, Fathy and Saleh [106] proposed an intelligent adaptive QoS framework that looks into the use of several paradigms. As an investigation of the EC paradigm, it suggested deploying deep learning models locally. The proposed deep learning model used the most recent lightweight version of YOLO for real-time monitoring and weapon identification. Additionally, a SDN paradigm was

Table 4: A taxonomy of the previous literature on SDN-IoT with DC.

Research area	Proposed model	Solution/ architecture	Contribution	Future scope
IoT cloud systems [103]	Software-defined IoT units—a novel approach to IoT CC	Framework	Encapsulated fine-grained IoT materials and IoT functionality are wrapped up well APIs to give a complete overview of how to obtain, configure, and run IoT cloud systems	Proposing techniques and mechanisms to support runtime authority of SDN-IoT systems
Cloud app development [104]	SDG-Pro	✓	Made the IoT cloud app development more efficient and simpler	Adding dynamic infrastructure attributes to the gateway's allocation process
Security and consistency, traffic measurement [105]	ARIMA model for traffic estimation and AC algorithm for seeking the fine-grained traffic of flows	Architecture and solution	Collected the statistics of coarse-grained traffic of flows and fine-grained traffic of links, modeled the network traffic as ARIMA and proposed an objective function to decrease the estimation errors	Other models can be applied for traffic measurement and other optimization algorithms can be studied for the objective function
Video streaming support [106]	Intelligent adaptive QoS framework	Framework	Deployed different paradigms to support real-time video surveillance application	Investigating the differences between real world and theoretical performance of the model
Device management [107]	SDIM	✓	Used SDN principles to set up devices and controlled devices over IoT networks	Device management processes can be virtualized as VNFs the possible advantages of MANO orchestration can be evaluated
Scalability [108]	Edge-IoT	Architecture	Handled data stream in mobile edge, reduced the traffic load in the core network and reduced the E2E delay between IoT devices and computing resources	Developing the system for handling for security threats
Large-scale IoT management [109]	Muppet	✓	Offered low-latency, energy advantages of the peer-to-peer method, along with ensuring wide-area, cross-protocol automation like to the cloud-based solutions	FC can be implemented to increase the efficiency of the system
Large-scale sensing and actuating of IoT [110]	6LE-SDN	Architecture	Improved the network performance over 6LoWPAN, reduced the average round trip time as well as the packet loss, reduced latency and network overhead	RIS can be applied to reduce the data loss of the network
IoT data analysis [111]	Three-tier IoT architecture	✓	Experimented on data anomaly detection and compared between two architectures for ECG diagnosis	Deploying in IoT cloud environment aiming for better diagnosis
Traffic control, resource management, latency [112]	SDN architecture for IoT based on FC	✓	Reduced the amount of resource contention in the IoT ecosystem and boost the overall performance of the IoT	Designing centralized control logic for orchestration of fog services
Security and privacy [113]	SDFC network architecture	✓	Dealt with security and privacy threats for both wireless and optical fog-C network systems	Studying the SDFC in a real environment
Latency [114]	IoT-fog-based system with SDN enabled	Framework	Latency reduction and higher efficiency of resource utilization	Traffic management can be studied under the system
Fog node deployment [115]	SOSW	Solution	Deployed fog nodes in optimal location and reduced the endways delay and energy consumption in SDN-IoT FC	Considering both mobile and fixed IoT devices under this study
IoT-based semipermanent smart infrastructure [116]	SDFog-Mesh	Architecture	Made the support for in-network communications and assisted in selecting the fog nodes	Improving for CoAP and DDS IoT protocols support

introduced to support video surveillance applications, acting as the network's core to regulate the distribution of available bandwidth among various traffic flows, thereby accelerating the prevention of criminal activity following the detection of weapons by means of edge-implemented AI models.

6.3. Fog-Based Systems. Khakimov et al. [114] presented a framework which deployed SDN in an IoT-fog-based system. The system deployed an edge layer of fog nodes between the IoT nodes and the cloud. The network was controlled by a centralized hub and consisted of OF switches spread out over the topology, each with restricted computational capabilities. Regarding system management efficiency, the controller might execute quality of support and orchestration in collaboration with fog orchestration. Focusing on latency-sensitive applications and optimizing resource utilization were essential goals of this effort. Tomovic et al. [112] proposed an SDN architecture based on FC for traffic control, resource management, and latency. The proposed architecture supported a high level of scalability, real-time data delivery, and mobility. This also reduced the amount of resource contention in the IoT ecosystem and boosted the overall performance of the IoT. But there was no centralized control logic for the orchestration of fog services.

7. BC in SDN-IoT Systems

BC is a potential solution to meet challenges like secure data transfer, data integrity, and attack detection in the SDN-IoT environment. The studies that were chosen for Table 5 have examined the contributions of integrating BC into the SDN-IoT environment. These works emphasize security, consistency, and IoT services. Moreover, it demonstrates that other attacks and security mechanisms can be studied in future for this scope. Samaniego and Deters [118] proposed a permission-based BC with SDN for provisioning IoT services and security. Their idea was to combine virtualized resources with authorization-based BC on edge hosts. The authorization-based BC was proven to be an effective technique for keeping state information on virtual resources. However, the author did not concentrate on figuring out how the location of BCs and the use of smart contracts will affect things. Pourvahab and Ekbatanifard [120] proposed an efficient forensic SDN-IoT architecture using BC to improve the security of IoT systems. The proposed architecture ensured safety from the beginning of the pocket entry; minimized delay, response time, and processing time; and increased throughput and accuracy. But there was no authentication and load balancing method at gateway entities.

In the analysis of the existing literature on DC associated with BC in SDN-IoT, the authors compiled Table 6 summarizing the various studies that have been conducted on this topic. However, it is realized that the context can be improved by adding a new column to specify the "cloud domain" of the studies. Guha Roy and Srirama [119] proposed a BC-based attack identification system for IoT in mobile edge and FC. The author presented a decentralized architecture which is able to identify and reduce the chances of various security attacks for IoT in mobile edge and FC. They had taken into account widespread assaults like Transmission Control Protocol (TCP) flooding, Internet Control Message Protocol (ICMP) flooding, and denial-of-service (DoS) to evaluate attack identification procedures. But besides attack identification, we need to apply attack prevention techniques which will also improve the system's efficiency. Man-in-the-middle attack and replay attacks can be studied in this framework.

While making the system more secure, we shall not forget about the system's performance. With the help of BC and DC, it is possible to achieve both security and efficiency. Sharma, Chen, and Park [122] proposed a BC-based distributed cloud architecture to give on-demand, low-cost, and secure access to the most competitive computing infrastructures in the IoT network. Moreover, they offered a secure distributed fog node architecture by moving computing resources to the edge of the IoT network using SDN and BC techniques, ensuring that all traffic in the core network is encrypted and streamlined and has a negligible impact on the user experience. The suggested architecture was developed to accommodate several desirable characteristics, such as low latency, high availability, rapid data transfer in real time, scalability, security, and robustness.

8. Advancing Connectivity: SDN-IoT and Next-Gen Mobile Networks

The works conducted in SDN technology for 5G and 6G in the IoT environment are examined in this section. These works offered some SDN-IoT architectures for 5G/6G, each of which serves a particular function. IoT communications, network monitoring, and open networking are some of the most crucial ones. We carefully examined the articles' contributions and mentioned some further research scopes and compiled them in Table 7. Exploring recent literature, we have found that there are very few works that involve 5G/6G mobile networks in this scope. Manogaran et al. [127] proposed AI-assisted service virtualization and flow management framework for resource management in a 6G cloud environment. The proposed framework reduced computation and service time constraints while maximizing service flows in a large-scale IoT platform and utilizing the resources. But the authors neglected the security threats. Tello-Oquendo et al. [125] proposed a 5G SoftAir-based architecture to provide efficient and comprehensive IoT transmission by utilizing a single SD platform. The authors also offered an innovative architecture in which SD gateways function as local IoT controllers, coordinating IoT devices and translating protocols between IoT networks and SD radio access networks. They provided a sum-rate optimization framework for optimal upstream and downstream data rates and effective spectrum use based on the SoftAir architecture. An experimental testbed architecture for SDN orchestration spanning edge, cloud, and IoT domains in 5G service was presented by Fichera et al. [128]. The platform comprised distinct orchestrators for SDN, IoT, and the cloud.

The traditional architecture of the IoT and its associated network protocols were not initially conceived with the explicit purpose of accommodating mobility and scalability.

Table 5: A taxonomy of the previous literature on SDN-IoT with BC.

Year	Research area	Proposed model	Solution/ architecture	Contribution	Future scope
2016	Provisioning IoT services and security [118]	Permission-based BC with SDN	Architecture	IoT facilities can be set up on side hosts by combining virtualized resources with an authorization-based BC	Concentrating on figuring out how the location of BCs and the use of smart contracts will affect things
2021	Cyberattack [119]	BC-based attack identification system	✓	Presented a decentralized architecture that is able to identify and diminish the chances of various security attacks for IoT in EC and FC	Man-in-the-middle and replay attack can be studied
2021	Security and consistency, traffic measurement [105]	ARIMA model for traffic estimation and AC algorithm for seeking the fine-grained traffic of flows	Model and algorithm	Collected the statistics of coarse-grained traffic of flows and fine-grained traffic of links, modeled the network traffic as ARIMA and proposed an objective function to decrease the estimation errors	Other models can be applied for traffic measurement and other optimization algorithms can be studied for the objective function
2019	Security [120]	Efficient forensic architecture in SDN-IoT using BC		Ensured security from the beginning of the pocket entry, minimized delay, response time, processing time and increased throughput, accuracy	Include authentication and load balancing mechanism at gateway entities
2022	Security [121]	Cluster architecture by blockchain-based SDN controllers and N-SMO algorithm	Architecture and algorithm	Secured peer-to-peer communication through effective authentication and enhances the security	Including different environment settings for ensuring the efficacy of the algorithm

Table 6: A taxonomy of the previous literature on SDN-IoT with DC and BC.

Research area	Cloud domain	Proposed model	Solution/ architecture	Contribution	Future scope
Flexibility, scalability [122]	Cloud, fog	Distributed BC cloud architecture	Architecture	Provided secure, low-cost, and on-demand access to the IoT network s most competitive computing infrastructures	Exploring the various energy harvesting technique
Resource utilization, latency, reliability [123]	Fog	IoT-fog system with SDN and BC	Framework	Delivered high performance in the use of resources, great adaptability, and decreased end-to-end latency in IoT networks	Security can be improved by proper use of BC
Cyberattack [119]	Mobile edge, fog	BC-based attack identification system	Mechanism	Presented a decentralized architecture which is able to identify and reduce the chances of various security attacks for IoT in mobile edge and FC	Man-in-the-middle and replay attack can be studied

Furthermore, they were not specifically engineered to effectively manage the substantial volumes of data created by a wide range of interconnected devices. Therefore, there are specific limitations associated with the provision and administration of diverse interconnected devices that generate a substantial amount of data. This research indicates that SDN is widely seen as the most suitable approach to fulfill the objectives of the IoT in terms of flexibility, scalability, heterogeneity, and other notable qualities. Furthermore, the significance of DC in the context of SDN-IoT systems is also brought to light. CC enables the consolidation and centralization of data administration and processing, hence enhancing operational efficiency and cost reduction. Additionally, it has the capability to offer adaptable and expandable resources that may be modified to accommodate evolving requirements. FC has the potential to mitigate latency and enhance network performance through the localization of data processing in proximity to the data source. The significance of this is particularly evident in the context of real-time applications, such as those involving video surveillance or industrial automation.

EC is a comparable notion to FC, although with a heightened level of decentralization. In EC, computing resources and services are predominantly delivered at the periphery

Table 7: A taxonomy of the previous literature on SDN-IoT and mobile networks.

Research area	Network generation	Proposed model	Solution/ architecture	Contribution	Future scope
Network monitoring [124]	5G	Architecture of software-defined 5G network with IoT monitoring framework	Architecture	Implemented a monitoring system for mobile network operators and a common IoT framework for telemetry transfer inside the framework	Developing more practical architecture for 6G network
IoT communications [125]	5G	SoftAir architecture	✓	Provided efficient and encyclopedic IoT transmission by utilizing a single software-defined platform	Increasing the security of the IoT communication
Open networking [126]	5G	AI-enabled SDN-based 5G/IoT network	✓	Provided motility and elasticity of resource allocation and utilization	Implementing more efficient AI methods
Resource management [127]	6G	AI-assisted service virtualization and flow management framework	Framework	Reduced computation and service time constraints while maximizing service flows in a large-scale IoT platform and utilized the resources	Implementing IRS for reducing the data loss

of the network, frequently on discrete devices like sensors or smartphones. SDN-IoT systems can derive significant use from this technology as it facilitates instantaneous decision-making and mitigates the volume of data that necessitates transmission to the cloud or data center. This has the potential to enhance the overall performance of the system and mitigate the requirement for costly network bandwidth. Additionally, this report highlights the increasing demand for BC technology in the context of SDN-IoT systems. This is attributed to the safe and decentralized nature of BC, which offers a robust platform for efficient data management and sharing across diverse devices and networks. The significance of incorporating 5G and potential 6G networks into SDN-IoT systems is growing due to its ability to offer enhanced connection in terms of speed, reliability, and efficiency for a diverse array of devices and applications.

9. Challenges and Future Direction

SDN has emerged as a promising solution for managing the complex and dynamic networks of the IoT. However, the implementation of SDN in IoT systems poses certain challenges that necessitate resolution to fully use its capabilities. This section focuses on the primary concerns and difficulties related to SDN-IoT systems, as well as the future research potentials of this area.

9.1. Ensuring Security. The field of SDN-IoT security has emerged as a relatively new topic of study. SDN exhibits security vulnerabilities as a result of its central control and the inherent limitations of switch table sizes. If these unresolved concerns persist, they provide considerable security risks for SDN and exert a notable impact on an IoT network comprising a vast number of devices. Hence, ensuring security has paramount importance within the integrated and heterogeneous environment of SDN-IoT. SDN-IoT systems must prioritize the establishment of network access only for authorized devices and the authentication of all devices prior to granting access. Sophisticated methods of identification and authorization, such as biometric authentication, multifactor authentication, and identity and access management systems, have the potential to enhance security measures. One of the challenges that arises in the realm of data security is the need to safeguard sensitive information against unauthorized access and disclosure. In order to tackle this issue, the system can use sophisticated encryption methods like as homomorphic encryption, differential privacy, and secure multiparty computing. In addition, it is imperative to ensure appropriate segmentation of SDN-IoT networks in order to mitigate the risk of unwanted intrusion into sensitive data or resources. In forthcoming times, the use of sophisticated network segmentation methods such as SD perimeter holds the potential to enhance security within the context of SDN-IoT. SDN-IoT devices is vulnerable to DoS attacks, which have the potential to interrupt network operations and impede the processing of valid data.

In the context of the IoT environment, the occurrence of DDoS attacks, ICMP flooding, and TCP flooding has been identified and effectively addressed through the utilization of SDN-associated approaches [119, 129]. In the realm of future systems, the incorporation of sophisticated intrusion detection and prevention systems, firewalls, and cyberattack mitigation approaches has significant potential. ML and AI have the potential to effectively detect and address security risks in real time, hence minimizing the likelihood of security breaches. BC technology is a viable option for enhancing the security of data and transactions inside SDN-IoT systems. Its use may effectively safeguard the integrity and authenticity of data. Incorporating supplementary measurements into the SDN controller can enhance the overall degree of data security. In recent years, several architectural designs have been put forth. These architectural designs have the potential to be constructed and tested in a real testbed.

9.2. Preserving Privacy. So far, a limited number of studies have employed SDN as a means to augment privacy in the context of the IoT. While SDN possesses attractive attributes

such as dynamism, flexibility, and agility, the integration of SDN with IoT introduces significant vulnerabilities. The issue of privacy poses significant challenges in the context of multitier systems, such as IoT networks, which encompass several interconnected devices. In order to protect privacy, it is imperative to establish explicit norms and procedures pertaining to security. It is imperative for the system to possess configurability, allowing users to exercise control over the extent of private data collection, the entities responsible for such collection, and the specific actions performed on the data. One additional privacy concern in the context of SDN-IoT is to the unauthorized gathering and utilization of personal data without obtaining proper consent. In order to tackle this difficulty, it is possible to apply data reduction approaches, which involve limiting the acquisition of superfluous data and employing methods such as pseudonymization and anonymization for protecting personal data. SDN controllers provide the capability to make informed judgments by taking into consideration the sensitivity level of data present in IoT devices [88]. Hence, it is possible to incorporate additional measures into the SDN controller in order to generate decisions that effectively preserve privacy at a heightened degree.

9.3. Managing Mobility and Flow Control. There are a lot of IoT devices available that are mobile and not fixed. The utilization of mobility management techniques results in a notable volume of signalling traffic for the purpose of locating and monitoring the positions and locations of devices, hence leading to a decrease in network performance. The high degree of mobility shown by IoT devices poses significant challenges for SDN controllers in effectively managing spatial-temporal demands for IoT objects, facilitating seamless handover through integration with other controllers, and implementing dynamic flow management inside IoT networks. The difficulty of maintaining uninterrupted connectivity and flawless data transfer while transitioning devices across several network domains is of considerable importance. The resolution of this issue may be achieved by the use of seamless handover methods, which provide uninterrupted switching of devices between network domains. These methodologies have the capability to predict the movement of mobile devices, hence reducing handover latency and optimizing the utilization of network resources. The precision of location tracking for IoT devices may be enhanced by using advanced technologies such as global positioning systems, indoor positioning systems, and RFID.

SDN has the potential to leverage these technologies in order to improve location management, provide context-aware services, and optimize resource allocation. Another difficulty in the context of SDN-IoT mobility pertains to the identification and selection of the most optimal network domain for a given device. The authors have the option to employ sophisticated network discovery and selection mechanisms in order to choose the most optimal network domain for a given device. This selection process takes into consideration several aspects such signal strength, availability of bandwidth, and level of security. To enhance scalability, distributed SDN architectures and EC can alleviate a portion of the mobility-related workload from the central controller. The achievement of distributing mobility management operations and enhancing overall scalability may be realized by employing hierarchical SDN control architectures, wherein LC rule specific network domains. Novel SD IoT systems, such as Ubiflow [102], have the potential to be deployed and evaluated in order to assess their effectiveness in managing flow control and mobility.

9.4. Handling Traffic. The significant quantity of traffic produced by the multitude of IoT devices poses a noteworthy obstacle for traffic management in ensuring network accessibility. Hence, it is important to take into account potential bottlenecks arising from the substantial influx of traffic in the SDN-IoT ecosystem while devising novel security mechanisms deployed by many IoT devices. In addition, it is necessary to consider the matter of communication traffic between the controller and the gateway. ML methodologies can be employed to forecast traffic trends and proactively administer traffic. This might potentially contribute to the mitigation of network congestion and enhancement of QoS in SDN-IoT systems. In addition, these systems must also strive to optimize traffic for several reasons, including enhancing network performance, ensuring QoS, minimizing energy consumption, and enhancing security. Future study might investigate the efficacy of multiobjective optimization techniques in efficiently balancing these objectives. The utilization of network slicing enables the establishment of virtual networks capable of managing traffic originating from various IoT devices and applications. Exploration of dynamic network slicing strategies that possess the ability to adapt to fluctuating traffic patterns and optimize network resources is also worth considering. The studies of traffic management based on BC and traffic processing based on EC are viable areas of research.

9.5. Resource Management. The challenges of resource management arises from its interconnections with other factors, such as the diversity of resources, imbalanced communication, unequal distribution of tasks, and dependence on resources [130]. The optimization of resource utilization and the effective administration of the control layer provide significant challenges within a heterogeneous ecosystem of SDN-IoT. The primary effects of this phenomenon are observed in the QoS and energy consumption of the IoT network. Researchers have found that effectively scheduling traffic flows on the E2E channel and enhancing resource utilization is a challenging task. In order to address these challenges, it is imperative for resource management programs to effectively resolve fundamental difficulties, such as task allocations. Improving network performance necessitates an understanding of the resources management algorithm and the consideration of bandwidth, since it has a significant impact on overall performance.

9.6. Resiliency. The concept of network resilience refers to the capacity of a system to maintain adequate service levels even in the face of abnormal operating situations [131]. There is an anticipation that SDN has the potential to

provide comparable or enhanced levels of availability when compared to conventional IP networks. Nevertheless, in the absence of human interaction, it is imperative to implement appropriate preventive measures to ensure the security of the network and the provision of essential services. The topic of discussion frequently revolves on the resilience of SDNs in the face of various failures, including link failure, node failure, malfunctioning SDN components, improperly configured hardware, and unavailability of SDN controllers [132]. Extensive scholarly research has been conducted on SDNs; nevertheless, further investigation is required on their practical implementations in order to achieve a truly resilient and reliable SDN infrastructure.

9.7. Switch Design. A diverse array of switches is now accessible, each possessing distinct specifications, features, performance capabilities, power consumption levels, security measures, scaling potentials, and architectural designs. TCAMs, encompassing SRAM, DRAM, RLDRAM, FPGA, GPU, CPUs, NPs, and other specialized network processors, provide effective performance when integrated with diverse SDN switch designs [46, 133]. One challenge is in the development of switches that possess the capability to effectively store rules inside a multitude of flow tables. The primary objective of forthcoming research endeavors should revolve around the advancement of a controller architecture that possesses the dual characteristics of modularity and flexibility, while simultaneously integrating all essential components.

9.8. Placement of the Controller. The controller serves as a pivotal function inside the SDN architecture, prompting engineers to exert significant efforts in enhancing its availability, speed, scalability, and ease of use. According to reference [134], it is argued that a solitary controller would face limitations in managing the substantial volume of traffic generated by diverse IoT devices as the network expands. Hybrid controller placement strategies can be employed to integrate centralized and distributed controller placement methodologies in order to address challenges related to scalability. There exist a number of inquiries that require responses, including the determination of the requisite quantity of controllers, the optimal placement of these controllers, and the identification of the individual or entity accountable for the allocation of forwarding devices. Dynamic controller placement techniques can be employed to optimize the positioning of controllers in accordance with fluctuating network conditions, including variations in traffic load, alterations in network topology, and occurrences of failures. Future study can investigate dynamic controller placement strategies that have the ability to adapt to fluctuating network conditions and enhance network performance and efficiency.

Despite the numerous challenges that SDN-IoT systems face, their future scope appears to be very promising. The proliferation of CC, FC, and EC designs in IoT systems has led to a heightened demand for specific solutions in network orchestration and administration. SDN-based solutions have the potential to effectively meet these needs through the provision of adaptable and dynamic NETCONFs. Furthermore, the incorporation of ML and AI techniques into SDN-based solutions has the potential to augment the efficiency and security of IoT networks.

10. Conclusions

The primary motivation for doing this research is from the acknowledgement that IoT devices are progressively gaining widespread adoption in our everyday routines. Consequently, it is imperative to comprehend the consequences and ramifications associated with this emerging phenomenon. Several evaluations have been conducted independently over the past few years on various themes related to SDN-IoT. These assessments encompass a range of topics, such as DC, BC, and mobile network technologies for IoT. Although these technologies share a tight relationship, there has been no comprehensive study conducted to investigate them collectively. This research endeavors to provide valuable insights that can aid policymakers, business executives, and individuals in making well-informed decisions regarding the utilization of IoT devices and their impact on daily life. To achieve this objective, the study comprehensively examines the development of SDN-IoT, drawing upon relevant scholarly papers to consolidate the information in a single publication. To facilitate the execution of this study, a systematic approach is employed to choose 50 research papers. These publications are subsequently assessed based on their model suggestions, contributions, and potential future applications. A comprehensive analysis is then conducted on the chosen publications. This review evaluation encompasses a comprehensive study of the basic SDN-IoT scenario. Furthermore, it focuses on the current deployment of SDN-IoT in conjunction with DC, BC, and 5G/6G technologies, scrutinizing, evaluating, and discussing their implications. Moreover, to facilitate comprehension of the SDN-IoT idea, this paper also provides a detailed explanation of the essential specifications of the many underlying technologies.

The presentation concludes by offering a road map for future research in the field of SDN-IoT. This road map is established via the identification of distinctive open research inquiries, barriers, problems, and prospective research objectives. In summary, SDN-IoT networks not only provide significant opportunities for innovation but also present substantial challenges that require the collective efforts of scholars and professionals to address. This study highlights the necessity for further research in the field of SDN-IoT to address challenges pertaining to security, scalability, resource management, traffic management, quality of service, and integration with other developing technologies. Researchers must prioritize the development of novel techniques, methodologies, and benchmarks in order to effectively integrate SDN with IoT, therefore laying the foundation for the advancement of contemporary network infrastructures.

Data Availability Statement

The authors declare that the data supporting the findings of this study are openly available in public repositories and databases and can be accessed as per the terms of use of those repositories. As such, there are no additional data files to share.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This research was supported by Jahangirnagar University Research Fund, Savar, Dhaka, Bangladesh, and the Woosong University Academic Research Fund, 2024, South Korea.

References

[1] "What is the internet of things (IoT)?," https://www.oracle.com/internet-of-things/what-is-iot/.

[2] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[3] V. Afshar, "Cisco: enterprises are leading the internet of things innovation," https://www.huffpost.com/entry/cisco-enterprises-are-leading-the_internet_of-things_b_59a41fcee4b0a62d0987b0c6, 2017.

[4] "Cisco and SAS edge-to-enterprise IoT analytics platform," https://www.cisco.com/c/dam/global/fr_fr/solutions/data-center-virtualization/big-data/solution-cisco-sas-edge-to-entreprise_iot.pdf.

[5] L. S. Vailshery, "Global IoT and non-IoT connections 2010-2025," https://www.statista.com/statistics/1101442/iot-number-of-connected-devices_worldwide/, 2022.

[6] A. Darabseh and N. M. Freris, "A software-defined architecture for control of IoT cyberphysical systems," *Cluster Computing*, vol. 22, no. 4, pp. 1107–1122, 2019.

[7] Y. Jararweh, M. Al-Ayyoub, and E. Benkhelifa, "An experimental framework for future smart cities using data fusion and software defined systems: the case of environmental monitoring for smart healthcare," *Future Generation Computer Systems*, vol. 107, pp. 883–897, 2020.

[8] I. Haque, M. Nurujjaman, J. Harms, and N. Abu-Ghazaleh, "SDSense: an agile and flexible SDN-based framework for wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1866–1876, 2019.

[9] I. Alam, K. Sharif, F. Li et al., "IoT virtualization: a survey of software definition & function virtualization techniques for internet of things," 2019, https://arxiv.org/abs/190210910.

[10] "Scopus preview," https://www.scopus.com/.

[11] "Software-defined networking - wikipedia," https://en.wikipedia.org/wiki/Software-defined_networking.

[12] J. Hendler and J. Golbeck, "Metcalfe's law, web 2.0, and the semantic web," *Journal of Web Semantics*, vol. 6, no. 1, pp. 14–20, 2008.

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

[14] S. Khan, A. Gani, A. W. A. Wahab, M. Guizani, and M. K. Khan, "Topology discovery in software defined networks: threats, taxonomy, and state-of-the-art," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 303–324, 2017.

[15] K. Poularakis, Q. Qin, E. M. Nahum, M. Rio, and L. Tassiulas, "Flexible SDN control in tactical ad hoc networks," *Ad Hoc Networks*, vol. 85, pp. 71–80, 2019.

[16] A. Montazerolghaem, M. H. Yaghmaee, and A. Leon-Garcia, "Green cloud multimedia networking: NFV/SDN based energy-efficient resource allocation," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 3, pp. 873–889, 2020.

[17] S. Patel and R. Patel, "Fog computing: a comprehensive analysis of simulation tools, applications and research challenges with use cases," *Journal of Engineering Science & Technology Review*, vol. 15, no. 3, pp. 63–83, 2022.

[18] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: a survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[19] S. Misra and N. Saha, "Detour: dynamic task offloading in software-defined fog for IoT applications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 5, pp. 1159–1166, 2019.

[20] A. J. Kadhim and S. A. H. Seno, "Maximizing the utilization of fog computing in internet of vehicle using SDN," *IEEE Communications Letters*, vol. 23, no. 1, pp. 140–143, 2019.

[21] S. S. Jazaeri, S. Jabbehdari, P. Asghari, and H. Haj Seyyed Javadi, "Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions," *Cluster Computing*, vol. 24, no. 4, pp. 3187–3228, 2021.

[22] A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, 2015.

[23] S. Siddiqui, S. Hameed, S. A. Shah et al., "Toward software-defined networking-based IoT frameworks: a systematic literature review, taxonomy, open challenges and prospects," *IEEE Access*, vol. 10, pp. 70850–70901, 2022.

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

[25] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: an SDN and fog computing perspective," *Computer Networks*, vol. 143, pp. 221–246, 2018.

[26] R. S. Alonso, I. Sittón-Candanedo, S. Rodríguez-González, Ó. García, and J. Prieto, "A survey on software-defined networks and edge computing over IoT," in *In Highlights of Practical Applications of Survivable Agents and Multi-Agent Systems. The PAAMS Collection: International Workshops of PAAMS 2019, Ávila, Spain, June 26–28, 2019, Proceedings 17*, pp. 289–301, Springer, 2019.

[27] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.

[28] M. Babiker Mohamed, O. Matthew Alofe, M. Ajmal Azad, H. Singh Lallie, K. Fatema, and T. Sharif, "A comprehensive survey on secure software-defined network for the internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 1, article e4391, 2022.

[29] E. Ahvar, S. Ahvar, S. M. Raza, J. Manuel Sanchez Vilchez, and G. M. Lee, "Next generation of SDN in cloud-fog for 5G and beyond-enabled applications: opportunities and challenges," *Network*, vol. 1, no. 1, pp. 28–49, 2021.

[30] A. H. Mohammed, R. M. Khaleefah, and I. A. Abdulateef, "A review software defined networking for internet of things," in *2020 International Congress on Human-Computer Interaction,*

Optimization and Robotic Applications (HORA), Ankara, Turkey, 2020.

[31] N. Lo and I. Niang, "SDN-based QoS architectures in edge-IoT systems: a comprehensive analysis," in *2023 IEEE World AI IoT Congress (AIIoT)*, pp. 605–611, Seattle, WA, USA, 2023.

[32] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[33] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[34] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[35] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[36] W. Yu, F. Liang, X. He et al., "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[37] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: fundamental, network applications, and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1826–1857, 2018.

[38] H. Elazhary, "Internet of things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: disambiguation and research directions," *Journal of Network and Computer Applications*, vol. 128, pp. 105–140, 2019.

[39] F. Javed, M. K. Afzal, M. Sharif, and B. S. Kim, "Internet of things (IoT) operating systems support, networking technologies, applications, and challenges: a comparative review," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018.

[40] J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, 2018.

[41] I. Alam, K. Sharif, F. Li et al., "A survey of network virtualization techniques for internet of things using SDN and NFV," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–40, 2021.

[42] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: a systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[43] X. Wang, X. Zha, W. Ni et al., "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[44] K. Greene, "Breakthrough technologies: software-defined networking mit technol," *Review*, vol. 10, 2009.

[45] "Open networking foundation," https://opennetworking.org/.

[46] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[47] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using http traffic characteristics," *Computers & Electrical Engineering*, vol. 66, pp. 353–368, 2018.

[48] S. K. Tayyaba, M. A. Shah, N. S. A. Khan, Y. Asim, W. Naeem, and M. Kamran, "Software-defined networks (SDNs) and internet of things (IoTs): a qualitative prediction for 2020," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 11, 2016.

[49] M. S. Bonfim, K. L. Dias, and S. F. Fernandes, "Integrated NFV/SDN architectures: a systematic literature review," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–39, 2019.

[50] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network (SDN) based internet of things (IoT) a road ahead," in *Proceedings of the international conference on future networks and distributed systems*, Cambridge, United Kingdom, 2017.

[51] T. Kunz and K. Muthukumar, "Comparing OpenFlow and NETCONF when interconnecting data centers," in *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, Toronto, ON, Canada, 2017.

[52] P. Lin, J. Bi, and H. Hu, "Internetworking with SDN using existing BGP," in *In Proceedings of the Ninth International Conference on Future Internet Technologies*, Tokyo, Japan, 2014.

[53] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, "A survey on the contributions of software-defined networking to traffic engineering," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 918–953, 2017.

[54] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, *The Locator/Id Separation Protocol (Lisp)*, Technical report (No. rfc6830), 2013.

[55] S. Popic, M. Vuleta, P. Cvjetkovic, and B. M. Todorović, "Secure topology detection in software-defined networking with network configuration protocol and link layer discovery protocol," in *2020 International Symposium on Industrial Electronics and Applications (INDEL)*, Banja Luka, Bosnia and Herzegovina, 2020.

[56] B. Pfaff and B. Davie, *The open vSwitch database management protocol*, Technical report (No. rfc7047), 2013.

[57] A. Capone, C. Cascone, A. Q. Nguyen, and B. Sanso, "Detour planning for fast and reliable failure recovery in SDN with OpenState," in *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 25–32, Kansas City, MO, USA, 2015.

[58] J. Rischke and H. Salah, "Software-defined networks," in *In Computing in Communication Networks*, pp. 107–118, Elsevier, 2020.

[59] P. He, N. Almasifar, A. Mehbodniya, D. Javaheri, and J. L. Webber, "Towards green smart cities using internet of things and optimization algorithms: a systematic and bibliometric review," *Sustainable Computing: Informatics and Systems*, vol. 36, article 100822, 2022.

[60] A. Carie, M. Li, S. Anamalamudi et al., "An internet of software defined cognitive radio ad-hoc networks based on directional antenna for smart environments," *Sustainable Cities and Society*, vol. 39, pp. 527–536, 2018.

[61] J. Li, E. Altman, and C. Touati, "A general SDN-based IoT framework with NVF implementation," *ZTE communications*, vol. 13, no. 3, pp. 42–45, 2015.

[62] A. El-Mougy, M. Ibnkahla, and L. Hegazy, "Software-defined wireless network architectures for the internet-of-things," in

2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), pp. 804–811, Clearwater Beach, FL, USA, 2015.

[63] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc, 2014.

[64] M. Satyanarayanan, R. Schuster, M. Ebling et al., "An open ecosystem for mobile-cloud convergence," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 63–70, 2015.

[65] Z. Ghanbari, N. Jafari Navimipour, M. Hosseinzadeh, and A. Darwesh, "Resource allocation mechanisms and approaches on the internet of things," *Cluster Computing*, vol. 22, no. 4, pp. 1253–1282, 2019.

[66] A. Mayoral, R. Vilalta, R. Muñoz, R. Casellas, and R. Martínez, "SDN orchestration architectures and their integration with cloud computing applications," *Optical Switching and Networking*, vol. 26, pp. 2–13, 2017.

[67] G. I. Klas, "Fog computing and mobile edge cloud gain momentum open fog consortium, ETSI MEC and cloudlets," *Google Scholar*, vol. 1, no. 1, pp. 1–13, 2015.

[68] G. Maier and M. Reisslein, "Transport SDN at the Dawn of the 5G Era," *Optical Switching and Networking*, vol. 33, pp. 34–40, 2019.

[69] K. Ahmadi, M. Esmaili, and S. Khorsandi, "A P2P file sharing market based on blockchain and IPFS with dispute resolution mechanism," in *2023 IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings)*, Mount Pleasant, MI, USA, 2023.

[70] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[71] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2019.

[72] A. Banafa, *Secure and smart internet of things (IoT): Using blockchain and artificial intelligence (AI)*, Stylus Publishing, LLC, 2019.

[73] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[74] Q. Xu, Z. He, Z. Li, M. Xiao, R. S. M. Goh, and Y. Li, "An effective blockchain-based, decentralized application for smart building system management," in *In real-time data analytics for large scale sensor data*, pp. 157–181, Elsevier, 2020.

[75] S. R. Basnet and S. Shakya, "BSS: blockchain security over software defined network," in *In 2017 International conference on computing, communication and automation (ICCCA)*, pp. 720–725, Greater Noida, India, 2017.

[76] N. O. Nawari and S. Ravindran, "Blockchain and building information modeling (BIM): review and applications in post-disaster recovery," *Buildings*, vol. 9, no. 6, p. 149, 2019.

[77] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, pp. 261–266, Baltimore, MD, USA, 2017.

[78] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, 2017.

[79] R. Singh, A. Mehbodniya, J. L. Webber et al., "Analysis of network slicing for management of 5G networks using machine learning techniques," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9169568, 10 pages, 2022.

[80] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the internet-of-things," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, Krakow, Poland, 2014.

[81] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-WSN: software-defined WSN management system for IoT applications," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2074–2081, 2018.

[82] K. Kalkan and S. Zeadally, "Securing internet of things with software defined networking," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 186–192, 2018.

[83] M. Bonanni, F. Chiti, R. Fantacci, and L. Pierucci, "Dynamic control architecture based on software defined networking for the internet of things," *Future Internet*, vol. 13, no. 5, p. 113, 2021.

[84] L. Huo, D. Jiang, Z. Lv, and S. Singh, "An intelligent optimization-based traffic information acquirement approach to software-defined networking," *Computational Intelligence*, vol. 36, no. 1, pp. 151–171, 2020.

[85] Z. Wen, X. Liu, Y. Xu, and J. Zou, "A restful framework for internet of things based on software defined network in modern manufacturing," *The International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1-4, pp. 361–369, 2016.

[86] C. H. Lee, Y. W. Chang, C. C. Chuang, and Y. H. Lai, "Interoperability enhancement for internet of things protocols based on software-defined network," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Kyoto, Japan, 2016.

[87] M. Baddeley, U. Raza, A. Stanoev et al., "Atomic-SDN: is synchronous flooding the solution to software-defined networking in IoT?," *IEEE Access*, vol. 7, pp. 96019–96034, 2019.

[88] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernandez-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Computers & Security*, vol. 87, article 101470, 2019.

[89] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: a software-defined networking approach," *Computers in Industry*, vol. 104, pp. 47–58, 2019.

[90] B. Alzahrani and N. Fotiou, "Enhancing internet of things security using software-defined networking," *Journal of Systems Architecture*, vol. 110, article 101779, 2020.

[91] H. Mahantesh, M. Nageswara Guptha, and M. Hema, "Optimized path and reduced rule caching cost for software defined network (SDN) based internet of things (IoT)," *Wireless Personal Communications*, vol. 120, no. 3, pp. 2349–2365, 2021.

[92] A. Montazerolghaem and M. H. Yaghmaee, "Load-balanced and QoS-aware software-defined internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3323–3337, 2020.

[93] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving internet of things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, p. 8, 2020.

[94] J. Ali and B. Roh, "A novel scheme for controller selection in software-defined internet-of-things (SD-IoT)," *Sensors*, vol. 22, no. 9, p. 3591, 2022.

[95] K. Haseeb, N. Islam, I. Ahmed, M. M. Hassan, and G. Jeon, "Artificial intelligence-enabled distributed energy conservative model for mobile internet of things using software-defined network," *International Journal of Communication Systems*, no. article e5295, 2022.

[96] A. Dawoud, S. Shahristani, and C. Raun, "Deep learning and software-defined networks: towards secure IoT architecture," *Internet of Things*, vol. 3-4, pp. 82–89, 2018.

[97] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: a top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[98] K. S. Sahoo, B. Sahoo, and A. Panda, "A secured SDN framework for IoT," in *2015 International Conference on Man and Machine Interfacing (MAMI)*, Bhubaneswar, India, 2015.

[99] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Procedia Computer Science*, vol. 52, pp. 1028–1033, 2015.

[100] D. Bendouda, A. Rachedi, and H. Haffaf, "Programmable architecture based on software defined network for internet of things: connected dominated sets approach," *Future Generation Computer Systems*, vol. 80, pp. 188–197, 2018.

[101] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, "SDIoT: a software defined based internet of things framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 4, pp. 453–461, 2015.

[102] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin, and J. A. McCann, "Ubiflow: mobility management in urban-scale software defined IoT," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 208–216, Hong Kong, China, 2015.

[103] S. Nastic, S. Sehic, D. H. Le, H. L. Truong, and S. Dustdar, "Provisioning software-defined IoT cloud systems," in *2014 International Conference on Future Internet of Things and Cloud*, pp. 288–295, Barcelona, 2014.

[104] S. Nastic, H. L. Truong, and S. Dustdar, "SDG-Pro: a programming framework for software-defined IoT cloud gateways," *Journal of Internet Services and Applications*, vol. 6, no. 1, pp. 1–17, 2015.

[105] L. Huo, D. Jiang, S. Qi, and L. Miao, "A blockchain-based security traffic measurement approach to software defined networking," *Mobile Networks and Applications*, vol. 26, no. 2, pp. 586–596, 2021.

[106] C. Fathy and S. N. Saleh, "Integrating deep learning-based IoT and fog computing with software-defined networking for detecting weapons in video surveillance systems," *Sensors*, vol. 22, no. 14, p. 5075, 2022.

[107] A. Mavromatis, C. Colman-Meixner, A. P. Silva, X. Vasilakos, R. Nejabati, and D. Simeonidou, "A software-defined IoT device management framework for edge and cloud computing," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1718–1735, 2020.

[108] X. Sun and N. Ansari, "EdgeIoT: mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.

[109] M. Uddin, S. Mukherjee, H. Chang, and T. Lakshman, "SDN-based multi-protocol edge switching for IoT service automation," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2775–2786, 2018.

[110] R. K. Das, N. Ahmed, F. H. Pohrmen, A. K. Maji, and G. Saha, "6LE-SDN: an edge-based software-defined network for internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7725–7733, 2020.

[111] D. Wu, X. Xie, X. Ni et al., "Software-defined edge computing: a new architecture paradigm to support IoT data analysis," 2021, https://arxiv.org/abs/210411645.

[112] S. Tomovic, K. Yoshigoe, I. Maljevic, and I. Radusinovic, "Software-defined fog network architecture for iot," *Wireless Personal Communications*, vol. 92, no. 1, pp. 181–196, 2017.

[113] A. Alamer, "Security and privacy-awareness in a software-defined fog computing network for the internet of things," *Optical Switching and Networking*, vol. 41, article 100616, 2021.

[114] A. Khakimov, A. A. Ateya, A. Muthanna, I. Gudkova, E. Markova, and A. Koucheryavy, "IoT-fog based system structure with SDN enabled," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, Amman, Jordan, 2018.

[115] M. Ibrar, L. Wang, G. M. Muntean, N. Shah, A. Akbar, and K. I. Qureshi, "SOSW: scalable and optimal nearsighted location selection for fog node deployment and routing in SDN-based wireless networks for IoT systems," *Annals of Telecommunications*, vol. 76, no. 5-6, pp. 331–341, 2021.

[116] S. Ali, M. Pandey, and N. Tyagi, "SDFog-Mesh: a software-defined fog computing architecture over wireless mesh networks for semi-permanent smart environments," *Computer Networks*, vol. 211, article 108985, 2022.

[117] M. Satyanarayanan, P. Simoens, Y. Xiao et al., "Edge analytics in the internet of things," *IEEE Pervasive Computing*, vol. 14, no. 2, pp. 24–31, 2015.

[118] M. Samaniego and R. Deters, "Using blockchain to push software-defined IoT components onto edge hosts," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, Blagoevgrad, Bulgaria, 2016.

[119] D. Guha Roy and S. N. Srirama, "A blockchain-based cyber attack detection scheme for decentralized internet of things using software-defined network," *Software: Practice and Experience*, vol. 51, no. 7, pp. 1540–1556, 2021.

[120] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573–99588, 2019.

[121] P. S. Manocha and R. Kumar, "Improved spider monkey optimization-based multi-objective software-defined networking routing with block chain technology for internet of things security," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 11, article e6861, 2022.

[122] P. K. Sharma, M. Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[123] A. Muthanna, A. Ateya, A. Khakimov et al., "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 15, 2019.

[124] T. Maksymyuk, S. Dumych, M. Brych, D. Satria, and M. Jo, "An IoT based monitoring framework for software defined 5G mobile networks," in *Proceedings of the 11th international conference on ubiquitous information management and communication*, Beppu, Japan, 2017.

[125] L. Tello-Oquendo, S. C. Lin, I. F. Akyildiz, and V. Pla, "Software-defined architecture for QoS-aware IoT deployments in 5G systems," *Ad Hoc Networks*, vol. 93, article 101911, 2019.

[126] B. S. P. Lin, "Toward an AI-enabled SDN-based 5G & IoT network," *Network and Communication Technologies*, vol. 5, no. 2, pp. 1–7, 2021.

[127] G. Manogaran, T. Baabdullah, D. B. Rawat, and P. M. Shakeel, "AI-assisted service virtualization and flow management framework for 6G-enabled cloud-software-defined network-based IoT," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14644–14654, 2022.

[128] S. Fichera, M. Gharbaoui, P. Castoldi, B. Martini, and A. Manzalini, "On experimenting 5G: testbed set-up for SDN orchestration across network cloud and IoT domains," in *2017 IEEE Conference on Network Softwarization (NetSoft)*, Bologna, Italy, 2017.

[129] M. Özçelik, N. Chalabianloo, and G. Gür, "Software-defined edge defense against IoT-based DDoS," in *2017 IEEE international conference on computer and information technology (CIT)*, pp. 308–313, Helsinki, Finland, 2017.

[130] A. S. Da Silva, P. Smith, A. Mauthe, and A. Schaeffer-Filho, "Resilience support in software-defined networking: a survey," *Computer Networks*, vol. 92, pp. 189–207, 2015.

[131] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya et al., "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[132] R. Masoudi and A. Ghaffari, "Software defined networks: a survey," *Journal of Network and Computer Applications*, vol. 67, pp. 1–25, 2016.

[133] M. Karakus and A. Durresi, "A survey: control plane scalability issues and approaches in software-defined networking (SDN)," *Computer Networks*, vol. 112, pp. 279–293, 2017.

[134] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 473–478, 2012.