[1]Dr. Syed Amjed Hussaini,

[2]Dr. Adil Ahmed khan

Enhancing IoT Security Using Software-Defined Networking

Abstract: To meet the privacy and security needs of the IoT, access control systems are essential. This article presents a method for controlling who may use Internet of Things (IoT) services that rely on the Constrained Application Protocol (CoAP). A single provider's network connecting several IoT endpoints is taken into account by the suggested solution. It enforces policies at the network level based on applications by using the Software-Defined Networking (SDN) paradigm. The IoT endpoints are unaffected by any activities, and the IoT communication protocol does not need any changes. In addition, our solution is practical and simply deployable to an existing network since it is based on standard OpenFlow. By implementing a proof of concept utilizing network emulation, we demonstrate that our strategy is feasible.

***Keywords*:** IoT, SDN, Cloud Computing.

1. INTRODUCTION

Currently, several facets of our lives are governed or facilitated by cyber-physical systems. The Internet of Things (IoT) is being used across several sectors, including agriculture, patient monitoring, home automation, wellness, and smart cities, among others. The Internet of Things primarily consists of gadgets that may lack processing capacity, constant network connection, electricity, or even physical protection. Consequently, it is unsurprising that implementing security solutions in this context is a formidable challenge. This study concentrates on a specific facet of security, namely access control. We examine the scenario of a network operated by a single entity that interconnects many IoT devices. These devices provide resources or actuation services that may be accessed using the Constrained Application Protocol (CoAP).

To justify our approach, we examine the use of a smart city management system. This system comprises IoT sensors (e.g., temperature sensors) and actuators (e.g., switches). Our objective is to empower system administrators to establish context-aware access control rules that regulate access to IoT devices. We want to implement a Mandatory Access Control (MAC) solution in which rules are centrally established by system administrators and are immutable by end users. An illustration of this policy within our reference system is the instance of a switch controlling street lights; in this scenario, the system administrator could establish an access control policy stipulating that "street light switches may be activated after 8 PM and deactivated after 6 AM, with all operations originating from the management center building." This policy delineates the resource (switch), the action (turn on/off), and specifies constraints about the timing of the action and the physical location from which it may originate [1].

The internet of things (IoT) refers to the network of physical objects embedded with sensors, software, and technologies that enable communication, computation, and data exchange with other devices and systems over the internet. Initially introduced by Kevin Ashton 17 years ago, it has subsequently emerged as a fundamental element of the second digital revolution. The services offered by IoT applications include many aspects of human life, including home and building automation, smart industries, smart cities, healthcare, intelligent traffic management, health monitoring, emergency and surveillance services, retail, and supply chain management. Sensors are crucial for facilitating communication between humans and intelligent devices by detecting and collecting information. A Cisco assessment predicts that by 2022, 1 trillion networked sensors will be globally integrated, with projections of up to 45 trillion in 20 years and 500 billion intelligent devices connected on Earth by 2030. IoT systems will include a substantial proportion of these interconnected devices, with many integrated sensors and actuators. IoT technology facilitates electrical communication among ordinary physical things, allowing them to be aware of remote events or respond to occurrences outside their physical perception. Nonetheless, the upkeep and scalability of such a diverse array of interconnected devices pose significant

[1]Sr. Fire Protection Engineer, Reda Hazard Control, amjedhere@gmail.com

[2]System Engineer, Emircom, adilkhan403@gmail.com

challenges. Furthermore, the number of active IoT devices is rapidly rising daily.

Figure 1 delineates the focal points of research works published between 2014 and 2023, represented as extracted terms from the names of articles, conference papers, book chapters, reviews, and conference proceedings. This figure underscores the principal domains and trends within the discipline, placing considerable attention on SDN-IoT concerns and their interaction with other nascent technologies [2].

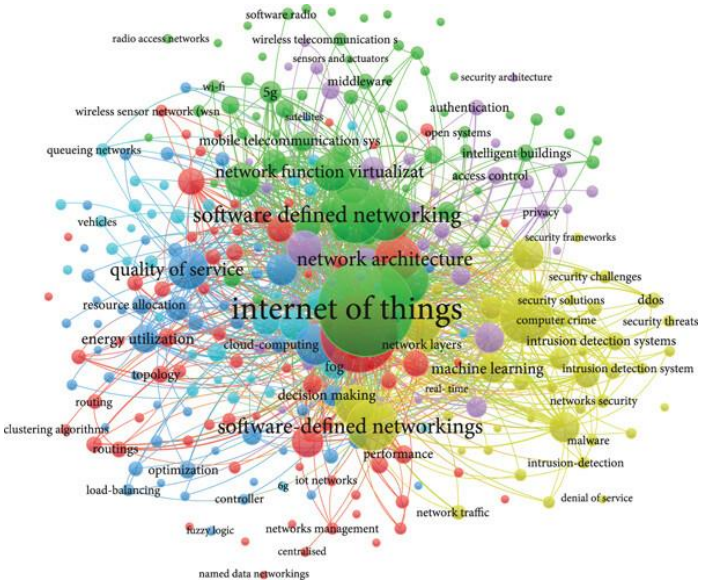

Figure 1: The focus of research studies published from 2014 to 2023, presented as retrieved keywords from the titles of papers (articles, conference papers, book chapters, reviews, and conference reviews) [2].

2. LITERATURE SURVEY

Numerous assessments on different subjects linked to SDN-IoT have been completed in recent years [13]. A thorough analysis of the primary challenges that must be tackled to guarantee the efficient support of IoT systems was provided in . The authors developed an IoT architecture integrated with Software-Defined Networking (SDN) and Data Distribution Service (DDS) middleware, which enhances network flexibility when SDN is used in IoT systems. In the following year, a comprehensive evaluation of diverse SDN solutions beneficial for addressing the particular requirements of IoT across many networking domains, including core, access, edge, and data center networking, was presented in [22]. The writers in [23] similarly offered a thorough examination of the prominent SDN-IoT frameworks. They concentrated on four trends: network function virtualization (NFV), OpenFlow (OF), middleware, and blockchain (BC). There is no correlation between cloud or FC, 4G, or subsequent mobile network technologies in SDN-IoT. The research in [24, 25] offered a comprehensive examination of SDN-based solutions designed to tackle the principal challenges of IoT related to FC. The following year saw an emphasis on the creation of Edge Computing (EC) to tackle the challenges faced by Internet of Things (IoT) systems in processing, filtering, and storing vast quantities of data, as discussed in [26]. The authors stated that Software-Defined Networking (SDN) might mitigate the complexity of EC designs in IoT contexts. Subsequently, the same notion was articulated in [27], whereby the survey advocated for the utilization of SDN and EC to effectively coordinate IoT services and oversee the infrastructure. Certain research delineated the security attributes provided by SDN-IoT.

The security measures established by SDN, including the several strategies for monitoring, managing, and addressing security concerns in the realm of IoT, were examined in [13]. Subsequently, in [28], the authors emphasized the identical function of SDN-IoT network security. The authors further examined several suggested solutions based on NFV, SDN/NFV, and blockchain to secure the IoT network against emerging risks. Blockchain facilitates the safe transmission of data and guarantees the integrity of records, which is crucial for managing sensitive IoT data, a topic that is hardly examined in the existing literature. The article [29] delineated the potential opportunities and substantial challenges associated with the implementation of SDN in hybrid cloud-fog systems to support 5G and future IoT devices and applications; however, the authors neglected to examine the critical role of BC. The authors in [28] examined an additional research that emphasized the significance of combining SDN

with IoT [30]. Recently, similar to the research in [26], the authors in [31] presented a survey of SDN-based designs inside edge-IoT systems. Similar to the majority of research in the literature, the authors failed to address the relevance of fog- and cloud-related systems.

The integration of edge, fog, and cloud in SDN-IoT seeks to address challenges. The edge functions as the local filter and primary responder, whilst the fog augments processing capabilities for pre-processing. Conversely, the cloud provides storage, analytical, and orchestration functionalities. This trio of components provides efficient and prompt data administration, while BC technology safeguards data transfer, so creating a secure and effective conduit for the linked future. Numerous research examined the integrated viewpoint of SDN-IoT and its related application fields. The bulk of these research focused on a particular SDN-IoT context in the literature. Numerous studies concentrated on security concerns, with some including CC , EC , both EC and CC , FC , DC , and mobile networks in the context of IoT; however, they were not linked to SDN. While the authors in [21] addressed all aspects pertaining to SDN, the significant function of BC in the SDN-IoT paradigm was shown. The available studies provide insight into the integration of SDN-IoT with DC. The majority continue to overlook the critical subject of 5G/6G technology and blockchain, which this research examines. This research presents a distinctive model at the intersection of SDN, IoT, DC, BC, and mobile networks; there are no comprehensive survey studies addressing SDN-IoT, DC, BC, and mobile networks from an all-encompassing perspective that includes architecture, administration, security, and other aspects.

3. METHODOLOGY

This section presents the approach for the topical review of SDN-IoT. The techniques for research selection and analysis are delineated. This paper presents a summary of previous investigations on SDN orchestration for IoT integration, emphasizing the significance of CC, EC, FC, or BC as essential enablers. To understand the primary subject of the research, we will first provide background information on pertinent words. Thereafter, we examine several research under the SDN-IoT paradigm. Finally, we examine the concerns, obstacles, and prospective paths within this domain.

Figure 2 illustrates a system for choosing papers via inclusion and exclusion stages, revealing that 59 full-text articles are accessible from the 92 examined, of which 50 articles are chosen for this research. A classification of pertinent SDN-IoT studies across many orchestration domains, including SDN-IoT, cloud computing (CC), fog computing (FC), edge computing (EC), blockchain (BC), and mobile networks. This taxonomy graphically classifies the many facets of SDN-IoT research, highlighting the varied areas of focus and the convergence of SDN-IoT with other nascent technologies. This research includes published publications on SDN-IoT systems, categorized by year, after applying inclusion and exclusion criteria.

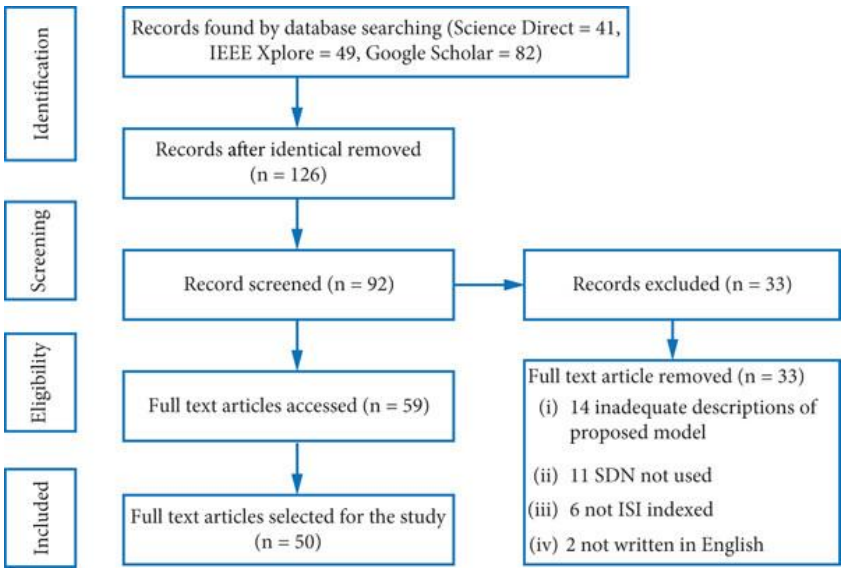

Figure 2: PRISMA diagram of the selection procedure and literature search of the research papers of this study [2]

BACKGROUND

The fast proliferation of IoT devices has resulted in the development of novel technologies and paradigms to manage and handle the extensive data created by these devices. Software-Defined Networking (SDN) is a networking architecture that facilitates efficient and flexible administration and control, while Cloud Computing (CC) offers a scalable and cost-effective platform for data storage and processing. Nevertheless, the conventional cloud-based architecture may fail to provide the low latency and real-time processing essential for several IoT applications. To tackle this difficulty, Fog computer (FC) and Edge Computing (EC) have been suggested as alternative paradigms that position computer resources nearer to IoT devices and applications. Moreover, the advent of blockchain technology has facilitated a safe and transparent method for managing IoT devices and data. The next 5G/6G networks are anticipated to provide enhanced speed and reliability in communication, enabling novel use cases and applications for IoT. This part will delineate and examine the essential specifications of SDN, IoT, SDN-IoT, CC, FC, EC, BC, and 5G/6G, along with their various functions in facilitating IoT applications in distinct subsections.

SDN

The word "SDN" was first used to delineate the ideas and research related to OF at Stanford University in Stanford, California, United States [44]. The Open Networking Foundation (ONF) is dedicated to the development, standardization, and commercialization of Software-Defined Networking (SDN) for transport and IP network layers. The SDN architecture consists of three levels [46–50], which interact via northbound and southbound application programming interfaces (APIs). The separation of the control plane and data plane is fundamental to Software-Defined Networking (SDN). An application plane exists that communicates its needs to the control plane. The OF or network configuration (NETCONF) protocols standardize the southbound interface used by the controller to configure the data plane. Nonetheless, OF cannot be the only SDN protocol, since alternative protocols such as BGP , ForCES , LISP , NETCONF , OVSDB , and OpenState also exist. However, these are less conventional methods. No standard presently exists for the northbound interface. A representational state transfer (REST) API may be created to enable applications to convey their requirements to the network.

IoT

The Internet of Things (IoT) connects various devices, such as automobiles and refrigerators, to the internet in innovative manners that surpass human capabilities. Identifiable and linked entities might manifest as either physical or digital forms . The data is gathered, administered, conveyed, saved, and analyzed by IoT devices and objects. The implementation of IoT spans all sectors and contexts, offering innovative solutions to improve efficiency, connection, and decision-making. The integration of IoT is essential for the advancement of smart cities, enhancing efficiency, connection, and data-informed decision-making across many urban sectors. The implementation of IoT facilitates the optimization of transportation systems, intelligent energy management, and the enhancement of urban infrastructure, hence fostering the development of flexible, sustainable urban settings that efficiently adapt to changing demands. The Internet of Things (IoT) is complicated not only by the inherent challenges of coordinating diverse sensing devices but also by the vast number of objects capable of connecting to the network and exchanging data through various protocols and network models.

SDN-IoT

SDN-IoT denotes the integration of Software-Defined Networking and Internet of Things technologies. This architecture employs SDN principles to oversee and regulate IoT devices, enabling network managers to centrally manage and automate the deployment, setup, and maintenance of IoT networks. The Internet of Things (IoT) presents challenges such as erratic network conditions, diverse communication protocols, application-specific quality-of-service (QoS) requirements, and substantial data flow, which may be addressed by Software-Defined Networking (SDN) as a viable approach for consolidating network management via rule-based governance. The abstractions of SDN provide comprehensive network governance via high-level rules, eliminating the need to address low-level configuration issues. Consequently, it is beneficial to address the heterogeneity and application-specific requirements of IoT. The amalgamation of IoT with SDN improves IoT efficiency and security by allowing comprehensive remote management of NETCONF without requiring physical proximity to IoT devices. The SDN controller inside the IoT with SDN architecture enables the segmentation of the network into several

subnets. The SDN controller employs the northbound API to interface with the IoT application. This evaluates network traffic and responds in line with the prescribed regulations. The controller engages with network switches using a southbound API in accordance with established protocols. Figure 3 depicts the overarching architecture of SDN-IoT, which facilitates IoT applications.

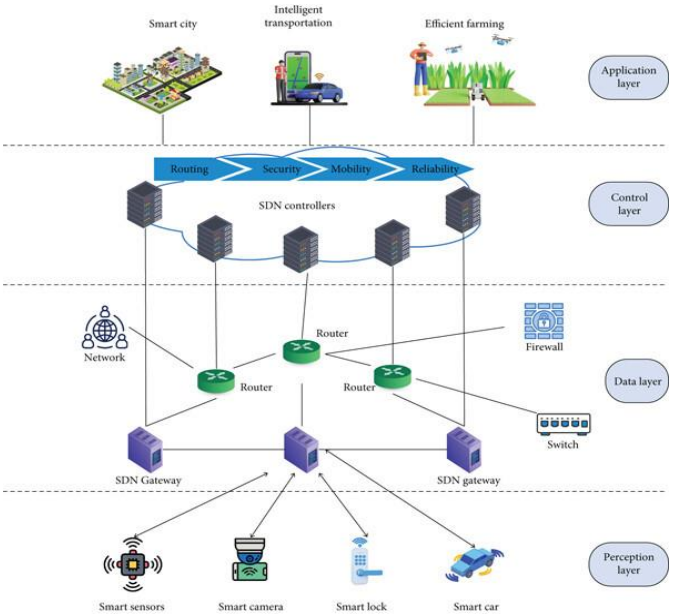

Figure 3: SDN-IoT architecture [2].

4. SDN-IOT ARCHITECTURES, FRAMEWORKS, AND SOLUTIONS

This section examines the dynamic subject of SDN-IoT, concentrating on the many characteristics of architectures, frameworks, and solutions proposed by scholars to address the rising challenges in the IoT domain. Architecture denotes the whole framework of a system, including its components, their interrelations, and the communication protocols among them. Frameworks and solutions include a collection of principles, protocols, and tools that provide a systematic methodology for constructing a system.

SDN-IoT and DC

As was said previously, a number of publications have lately suggested numerous designs for the integration of SDN and Internet of Things technologies. Here are some of the architectures that have been offered. We discovered a sizeable number of research that included DC as a subject among those that were examined. Several of them are discussed in further depth in this section.

BC in SDN-IoT Systems

When it comes to addressing difficulties in the SDN-IoT context, such as secure data transmission, data integrity, and attack detection, BC is a viable solution that might be used. The research that were selected for this synthesis have investigated the contributions that may be made by incorporating BC into the SDN-IoT ecosystem. In these works, security, consistency, and Internet of Things services are emphasized. In addition to this, it illustrates that other security procedures and assaults might be investigated in the future for this scope. The delivery of Internet of Things services and security was suggested by Samaniego and Deters using a permission-based BC in conjunction with SDN. On edge hosts, they proposed combining virtualized resources with authorization-based BC. This was their proposition. The authorization-based BC has been shown to be an efficient method for maintaining state information on virtual resources because of its effectiveness. On the other hand, the author did not put much effort into determining how the geographic placement of blockchains and the implementation of smart contracts would influence the situation. An effective forensic SDN-IoT architecture that makes use of BC was presented by Pourvahab and Ekbatanifard in order to enhance the safety of Internet of Things (IoT) systems. The design that was presented maximized throughput and accuracy while simultaneously reducing latency,

reaction time, and processing time. It also guaranteed that safety was maintained from the very beginning of the pocket input process. However, there was no mechanism of authentication or load balancing at the gateway entity.

Challenges and Future Direction

SDN has emerged as a viable option for controlling the intricate and dynamic networks of the IoT. The adoption of SDN in IoT systems has certain issues that must be addressed to properly use its advantages. This section addresses the principal issues and challenges associated with SDN-IoT systems, along with the prospective research opportunities in this domain.

Ensuring Security

The domain of SDN-IoT security has arisen as a somewhat novel area of research. SDN demonstrates security concerns due to its centralized control and the intrinsic constraints of switch table capacities. If these outstanding issues continue, they pose significant security threats to SDN and have a substantial effect on an IoT network with many devices. Therefore, guaranteeing security is of utmost significance in the interconnected and heterogeneous ecosystem 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 giving access. Advanced identification and authorization techniques, including biometric authentication, multifactor authentication, and identity and access management systems, may significantly improve security protocols. A significant difficulty in data security is the need to protect sensitive information from unauthorized access and disclosure. To address this problem, the system may use advanced encryption techniques such as homomorphic encryption, differential privacy, and secure multiparty computation. Furthermore, it is essential to implement proper segmentation of SDN-IoT networks to reduce the danger of unauthorized access to critical data or resources. In the future, the use of advanced network segmentation techniques like SD perimeter may improve security in the realm of SDN-IoT. SDN-IoT devices are susceptible to DoS attacks, which may disrupt network operations and hinder the processing of legitimate data. Within the IoT ecosystem, DDoS assaults, ICMP flooding, and TCP flooding have been recognized and efficiently mitigated using SDN-related strategies [30]. The integration of advanced intrusion detection and prevention systems, firewalls, and cyberattack mitigation strategies holds considerable promise for future systems. Machine learning and artificial intelligence has the capacity to promptly identify and mitigate security threats, hence reducing the probability of security breaches. Blockchain technology is a feasible solution for augmenting the security of data and transactions inside SDN-IoT systems. Its use may efficiently preserve the integrity and validity of data. Integrating more metrics into the SDN controller helps improve the overall level of data security. In recent years, several architectural concepts have been proposed. These architectural designs may be implemented and evaluated on a practical testbed.

Handling Traffic

The substantial volume of traffic generated by many IoT devices presents a considerable challenge for traffic control in maintaining network accessibility. Therefore, it is crucial to consider possible bottlenecks resulting from the significant surge of traffic in the SDN-IoT ecosystem while developing innovative security methods used by many IoT devices. Furthermore, it is essential to evaluate the communication traffic between the controller and the gateway. Machine learning approaches may be used to predict traffic patterns and proactively manage traffic. This may aid in alleviating network congestion and improving QoS in SDN-IoT systems. Furthermore, these systems must endeavor to optimize traffic for several purposes, including improving network speed, guaranteeing Quality of Service (QoS), reducing energy usage, and bolstering security. Future research may examine the effectiveness of multiobjective optimization methods in effectively reconciling various aims. Network slicing facilitates the creation of virtual networks that can handle traffic from diverse IoT devices and applications. Investigation of dynamic network slicing solutions that can adapt to variable traffic patterns and maximize network resources is also important. Research on traffic management with BC and traffic processing employing EC are promising fields of study.

5. CONCLUSIONS

The principal impetus for doing this study stems from the recognition that IoT devices are increasingly becoming ubiquitous in our daily lives. Therefore, it is essential to understand the repercussions and implications related to this rising phenomena. Numerous impartial assessments have been performed in recent years on several issues

pertaining to SDN-IoT. These evaluations cover several subjects, including DC, BC, and mobile network technologies for IoT. Despite the close link among these technologies, no thorough research has been undertaken to examine them together. This study aims to provide significant insights to assist policymakers, corporate leaders, and people in making educated choices about the use of IoT devices and their effects on everyday life. This research thoroughly investigates the evolution of SDN-IoT, using pertinent academic literature to condense the findings into a singular publication. A systematic technique is used to choose 50 research articles for this investigation. These papers are then evaluated based on their model proposals, contributions, and prospective applications. A thorough study is thereafter performed on the selected papers. This review assessment includes an extensive analysis of the fundamental SDN-IoT situation. Additionally, it examines the present implementation of SDN-IoT alongside DC, BC, and 5G/6G technologies, analyzing, assessing, and deliberating their ramifications. This article also offers a comprehensive elucidation of the fundamental specifications of the various underlying technologies to enhance understanding of the SDN-IoT concept.

REFERENCE

[1] Bander Alzahrani, Nikos Fotiou, Enhancing Internet of Things Security using Software-Defined Networking, Journal of Systems Architecture, Volume 110, 2020, 101779, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2020.101779.

[2] Shafiq, Shakila, Rahman, Md. Sazzadur, Shaon, Shamim Ahmed, Mahmud, Imtiaz, Hosen, A. S. M. Sanwar, 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, International Journal of Distributed Sensor Networks, 2024, 9006405, 26, pages, 2024. https://doi.org/10.1155/2024/9006405

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

[4] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Inter-net of things: evolution and technologies from a security per-spective," Sustainable Cities and Society, vol. 54, p. 101728,2020.

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

[6] "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.

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

[8] A. Darabseh and N. M. Freris, "A software-defined architec-ture for control of IoT cyberphysical systems," Cluster Com-puting, vol. 22, no. 4, pp. 1107–1122, 2019.

[9] Y. Jararweh, M. Al-Ayyoub, and E. Benkhelifa, "An experi-mental framework for future smart cities using data fusionand software defined systems: the case of environmentalmonitoring for smart healthcare," Future Generation Com-puter Systems, vol. 107, pp. 883–897, 2020.

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

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

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

[13] "Software-definednetworking-wikipedia," https://en.wikipedia.org/wiki/Software-defined_networking.

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

[15] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey onemerging SDN and NFV security mechanisms for IoT sys-tems," IEEE Communications Surveys & Tutorials, vol. 21,no. 1, pp. 812–837, 2019.

[16] 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 Communica-tions Surveys & Tutorials, vol. 19, no. 1, pp. 303–324, 2017.

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

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

[19] S. Patel and R. Patel, "Fog computing: a comprehensive anal-ysis of simulation tools, applications and research challengeswith use cases," Journal of Engineering Science & TechnologyReview, vol. 15, no. 3, pp. 63–83, 2022.

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

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

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

[23] S. S. Jazaeri, S. Jabbehdari, P. Asghari, and H. Haj SeyyedJavadi, "Edge computing in SDN-IoT networks: a systematicreview of issues, challenges and solutions," Cluster Comput-ing, vol. 24, no. 4, pp. 3187–3228, 2021.

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

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

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

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

[28] R. S. Alonso, I. Sittón-Candanedo, S. Rodríguez-González,Ó. García, and J. Prieto, "A survey on software-defined net-works and edge computing over IoT," in In Highlights of Practical Applications of Survivable Agents and Multi-AgentSystems. The PAAMS Collection: International Workshops ofPAAMS 2019, Ávila, Spain, June 26–28, 2019, Proceedings17, pp. 289–301, Springer, 2019.

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

[30] M. Babiker Mohamed, O. Matthew Alofe, M. Ajmal Azad,H. Singh Lallie, K. Fatema, and T. Sharif, "A comprehensivesurvey on secure software-defined network for the internetof things," Transactions on Emerging TelecommunicationsTechnologies, vol. 33, no. 1, article e4391, 2022.

[31] E. Ahvar, S. Ahvar, S. M. Raza, J. Manuel Sanchez Vilchez,and G. M. Lee, "Next generation of SDN in cloud-fog for5G and beyond-enabled applications: opportunities and chal-lenges," Network, vol. 1, no. 1, pp. 28–49, 2021.

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

[33] 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 con-ference on future networks and distributed systems, Cam-bridge, United Kingdom, 2017.

[34] T. Kunz and K. Muthukumar, “Comparing OpenFlow andNETCONF when interconnecting data centers,” in 2017 IEEE25th International Conference on Network Protocols (ICNP),Toronto, ON, Canada, 2017.

[35] 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.

[36] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, “A surveyon the contributions of software-defined networking to trafficengineering,” IEEE Communications Surveys & Tutorials,vol. 19, no. 2, pp. 918–953, 2017.

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