Babylonian Journal of Networking
Vol.2023, **pp**. 15–20
DOI: https://doi.org/10.58496/BJN/2023/003; ISSN: xxxxx
https://mesopotamian.press/journals/index.php/BJN

Research Article

A Survey of Software-Defined Networking (SDN) Controllers for Internet of Things (IoT) Applications

Hiba Sahib Rasheed Alzubaidy [1,*], Hanan Jabber [1]

[1] *Computer lab in accounting department, Technical college of management/ Baghdad, Middle Technical University, Iraq, Baghdad.*

[2] *Cyber security engineering department, Al-shaab University College, Iraq, Baghdad.*

ARTICLE INFO

Article History

Received 02 Jun 2023
Accepted 07 Mar 2023
Published 26 Mar 2023

Keywords

IoT
SDN
IoMT
IoNT
IoBT

ABSTRACT

Many local devices across the globe, including those in homes, oil wells, hospitals, vehicles, and countless more locations, will be linked through the Internet of Things (IoT). The number of connected devices will surpass 50 billion in 2020, as predicted by Gartner. Some examples of this strategy include the (IoMT, IoNT, and IoBT). All of this is situated beneath the network architecture. More design, construction, and mapping flexibility is brought about by the software-defined network, or SDN. To enable SDN to support the functioning of the Internet of Things (IoT), the SDN controller is the "core" of SDN in any network. Given the pervasiveness of IoT devices and the critical role that SDN controllers play in enabling them, we will examine the most effective controller types and determine which ones are most suited to IoT devices. As a result, there are unique requirements for security, speed, and other aspects of IoT applications. This will serve as the foundation for the comparison, which will be carried out utilising the API and the Python programming language.

1. INTRODUCTION

The concept of "Internet of Things" (IoT) pertains to a networked arrangement wherein several interconnected embedded devices collect, exchange, and analyses data to execute diverse functions over an established network [1]. The rapid increase in popularity of the Internet of Things (IoT) can be attributed to the extensive use of consumer gadgets equipped with networking capabilities in several domains [2].

The Internet of Things encompasses several attributes such as intelligence, architecture, complexity, size, weight, and other pertinent properties. The phenomenon of widespread connectivity among devices and the subsequent sharing of data has been referred to by various terms, such as the "Internet of Things," "Internet of Everything," "Internet of Anything," "Machine-to-Machine," and "Industrial Internet of Things" (IIoT) [3].

Given that a significant number of Internet of Things (IoT) technologies have already implemented standardised operating procedures (SOPs), it is imperative for research efforts to focus on enhancing their performance by prioritizing the most critical elements. An illustration of its practicality in daily existence is depicted in Figure (1). show examples of application od IoT, and Figure 2 shows Types of Internets of Things (IoT).

*Corresponding author. Email: queen.of.cipher@gmail.com

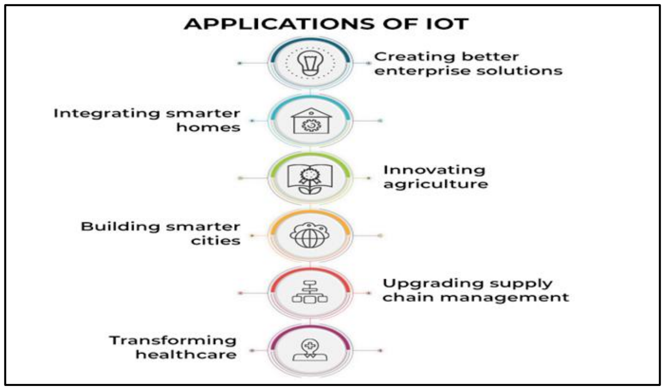

Fig.1. Examples of IoT

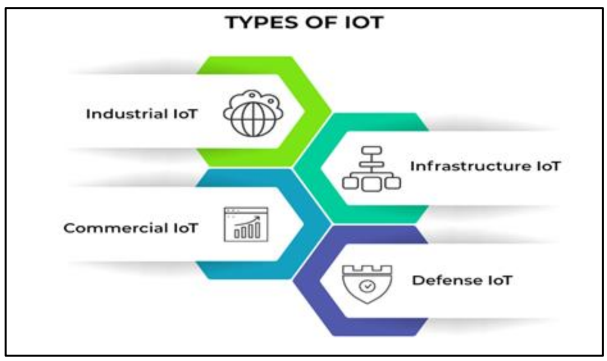

Fig.2. Types of IoT

2. SDN (SOFTWARE DEFINED NETWORK)

A growing number of networking companies are embracing software-defined networking (SDN). The restrictions of conventional networking are something that this new technology is expected to help alleviate [4]. Software-defined networking (SDN) is a new kind of network design that gives administrators more control over their networks. Manageability, dynamism, cost-effectiveness, and malleability are the defining features of SDN [5]. The following are descriptions of some of SDN's most salient features:

a. Networks that can be programmed: disconnecting without worrying about forwarding operations.

b. This detachment enables quick and adaptable flow modification and attend networking function attendance, which contributes to flexible development.

c. A centralised controller maintains a bird's-eye view of the network and interacts with it by changing flows; this is the basis of software-defined networking (SDN) architecture [6].

d. Facilitates programming automation of devices: software-defined networking (SDN) enables the administrator to set up self-written programmers that streamline the optimisation, configuration, and management of network resources processes.

e. Because it is not dependent on any specific providers, adaptation devices, or protocols, it is able to facilitate the network arrangement and is based on open standards.

f. Researchers and industry practitioners are starting to see the value of software-defined networking (SDN) solutions in Internet of Things (IoT) settings in contexts outside of the smart transportation setting that we covered earlier [7]. Thus, SDN architecture was designed with the goal of meeting the problem needs of IoT environments in mind for a number of reasons:

Resolve issues with the outdated and unproductive traditional network design.

1. With SDN, services on the control plane can have their concerns clearly separated [8].
2. With the help of an explicit SDN controller, SDN methods try to strike a balance between the amount of centralised control and coordination [9].

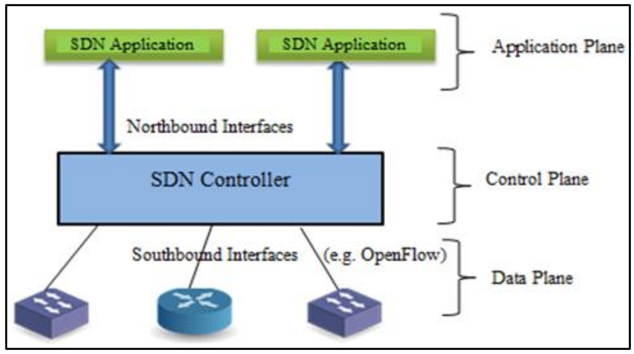

Fig.3. SDN architecture

3. CONTROLLERS

A programme running on a server within the network functions as the controller. An interface is necessary to provide communication between controllers and network devices. There exists a diverse range of controllers, encompassing:

A significant proportion of software-defined networking controllers incorporate the Open Flow protocol as a fundamental component of their interfaces [10]. The Open Flow architecture facilitates the identification of network flows and desired monitoring paths by network managers, while ensuring minimal disruption to existing traffic. Additionally, this study offers methods for identifying regulatory measures that facilitate the enhancement of bandwidth, reduction of latency, minimization of network hops, and optimisation of energy use in order to achieve improved network performance [11]. By leveraging the OpenFlow protocol in an indirect manner, network managers are capable of disentangling network monitoring functionalities from proprietary switches.

UbiFlow [12] is a software-defined Internet of Things (IoT) technology that demonstrates effectiveness in managing mobility and controlling flows inside urban multinetwork.

Designing an IoT Software-Defined Networking (SDN) controller The main aspect of multinetwork that enables the efficient, effective, and flexible administration of tasks, flows, networks, and resources is the implementation of a layered design [13].

Ultimately, the controller is responsible for initiating the necessary communications inside the Internet of Things (IoT) network. Various network vendors provide software-defined networking (SDN) infrastructure for development purposes, which includes a wide range of SDN controllers.

Open Daylight (ODL) is widely regarded as the most prominent SDN controller among its counterparts. Software-defined networking (SDN) installations have the capability to be constructed utilising the infrastructure provided by Open Daylight (ODL), an open-source platform for SDN..

4. APPLICATION PROGRAMMING INTERFACES (APIs)

Application Programming Interfaces (APIs) are frequently utilised to extract data from remote websites. Utilising developer APIs presents a highly effective means of obtaining authenticated data from prominent platforms such as Reddit and Twitter. The act of sending a request to a remote web server and subsequently obtaining the necessary data is commonly referred to as utilising an Application Programming Interface (API). The dynamic nature of data necessitates the utilization of APIs, hence facilitating efficient data management. To ascertain the optimal controller type, we shall utilize this methodology..

5. LITERATURE REVIEW

The proliferation of communication technologies and computing devices has experienced exponential expansion due to the concurrent reduction in size and cost of hardware and software components. Organizations and suppliers are currently venturing into unfamiliar domains as they endeavour to uncover computer and communication solutions that are more flexible and adaptive. The convergence of the Internet of Things (IoT) and software-defined networks (SDNs) is now being researched in order to develop intelligent systems that can provide advantages to human beings. While Virtual Private Networks (VPNs), which are considered traditional networks, may not possess the capability to adequately serve the Internet of Things (IoT), software-defined networking (SDN) presents a viable option by enabling the adaptation of current networks to accommodate emerging service requirements [14]. Furthermore, the conventional network exhibits numerous limitations, including sluggishness, susceptibility to errors, a high rate of conversion, restricted automation capabilities, and a tendency to stifle innovation.

The ascent of Martin Casado's invention in 2007, known as Software Defined Networks (SDN), serves as an emblematic representation of this period of growth. One crucial aspect of software-defined networking (SDN) involves the division between the control plane and data plane, the consolidation of network intelligence and state, and the abstraction of the underlying network infrastructure from applications. Software-Defined Networking (SDN) places emphasis on the prioritization of open interfaces between controllers and data plane devices, the implementation of a centralised controller and network perspective, and the ability to programme the network through external applications [15]. Several software-defined networking controllers include Open Daylight, Open Source SDN Platform (OPSDP), OpFlex, NETCONF, SNMP, and OpenFlow.

There are several benefits associated with the utilization of an SDN controller, such as cost efficiency, centralization, optimisation, enhanced functionality, redirection, load balancing, and fault tolerance.

The topic of software-defined networking (SDN), its architecture, and its distinctions from traditional networking were examined by [16]. The course also included coverage of simulation tools for architecture, OpenFlow, and Software-Defined Networking (SDN). Based on their research findings, it has been determined that Software-Defined Networking (SDN) has the potential to enhance network management through the elimination of intermediary units and the facilitation of more adaptable configuration updates.

Li et al. (2016) proposed a software-defined network (SDN) framework designed specifically for horizontal Internet of Things (IoT) services. By imbuing nodes with environmental awareness, this architecture facilitated horizontal interworking across multiple study domains.

Furthermore, there exists a range of levels of endorsement for the concept of interoperability and the provision of Internet data. The implementation elucidated the manner in which the proposed framework enables the reutilization of preexisting apps and data, hence enabling the expeditious construction of Internet applications.

In 2016, survey research was conducted by [17] with the objective of identifying a suitable approach for integrating SDN control planes into IoT networks. Prior to discussing the notable problems associated with this merger, this study provides a summary of the architectural characteristics and its development to examine the current status of IoT management, focusing on the SDN centralised control plane in different IoT stakeholders. In the context of Internet of Things (IoT) applications, it is imperative to focus our attention on the controller that is widely regarded as the most ideal.

In a study conducted in [18] conducted a comparative analysis of different controllers based on multiple parameters. Additionally, performance testing using Cbench was conducted. Based on their research findings, Open Daylight emerges as a highly commendable choice for a controller that offers a wide array of features. The aforementioned technology exhibits potential to emerge as the predominant controller due to its extensive range of applications and well-developed ecosystem. In its latest iteration, the system emerged as the primary candidate for the forthcoming "Internet of the future" controller election. This achievement was accomplished through the incorporation of an IoT data broker and the introduction of novel southbound interfaces specifically designed for IoT applications.

The integration of SDN, network virtualization, and the Internet of Things was examined in a survey conducted by [19]. This paper presents an overview of the proposed protocols, architectural models, algorithms, and applications pertaining to the Internet of Things (IoT). Before entering into the research of Wireless Sensor Networks (WSNs), the authors presented an overview of Software-Defined Networking (SDN) and Network Virtualization (NV) enabled architectures for the Internet of Things (IoT), along with real-world deployments and use cases.

In [20] proposed a novel design that leverages Software Defined Networks (SDN) to enable Low power wireless personal area network (6LowPAN) devices to efficiently access network resources as needed. The suggested architectural paradigm will increase both the control and monitoring applications of the Internet of Things (IoT). Furthermore, this discussion will elucidate the manner in which developers of Smart City Internet of Things (IoT) applications can effectively employ Software Defined Network (SDN) Architecture to tackle the challenges associated with high bandwidth requirements and potential disconnections within the IoT network.

The study conducted by Sajad and Ali (2017) titled "An Experimental Investigation of SDN Controller Live Migration in Virtual Data Centres" revealed that the efficiency of SDN controllers during live migration is negatively impacted while working on bigger virtual machines, especially under high network traffic loads. The discussion surrounding the enhancement of the live migration process has also included an examination of the potential impacts of a high-throughput transport layer protocol on the live migration of the SDN controller. Furthermore, we have conducted an analysis on the impact of virtual machine size on software-defined networking live migration.

In the year 2018, the directorship of Farzad Kiani was assumed. Based on a scientific classification of management frameworks and open issues in the sector, it has been observed that a viable administration solution for the architecture of the Internet of Things (IoT) has not yet been produced. This encompasses programmable administrative structures based on APIs and engineering that utilizes software-defined networking (SDN).

Many existing frameworks for managing IoT setups tend to overlook the intricate operational aspects of practical components. This study investigates the aspects of security provisioning, adaptation to non-critical failure, energy management, and load balancing in relation to the specific requirements of the executive's system for the Internet of Things (IoT).

In the realm of the Internet of Things (IoT), it is noteworthy that a significant proportion of current literature advocating for an administration system based on Software-Defined Networking (SDN) falls short in addressing the problem at hand.

Therefore, it is imperative to prioritise selecting the appropriate controller for the specific Internet of Things technology.

A study conducted in [21] aimed to evaluate the security of various key Internet of Things (IoT) frameworks. A total of eight frameworks were included in the analysis. I have examined the suggested architectural framework, the essential components required for the development of third-party intelligent applications, the hardware compatibility considerations, and the security aspects associated with each framework.

Different methodologies were employed to incorporate diverse security measures. However, while comparing security architectures, it was observed that similar standards were employed to ensure the security of communications. The significance of security measures in each framework is underscored, since the validation of several security elements and the ability to withstand attacks are prominent contemporary concerns associated with the Internet of Things.

in [22] introduced the innovative SDN controller architecture for IoT multi-networks. The use of layered architecture in the controller introduces a novel feature that enables efficient and adaptable administration of task networks and resources. A model of network Calculus was developed to estimate the end-to-end flow performance in IoT multi-networks. The implementation of a layered controller design is of utmost importance in effectively managing diverse Internet of Things (IoT) multi-networks. These systems can be conceptualized as modules and can be adjusted or substituted in various IoT scenarios utilising the Genetic Algorithm (GA) technique.

6. CONCLUSION

The convergence of the Internet of Things (IoT) and Software-Defined Networking (SDN) offers a potentially fruitful pathway for the advancement of intelligent systems. Conventional networks, specifically Virtual Private Networks (VPNs), encounter constraints when it comes to accommodating evolving service demands. Powered by its focus on programmability, centralization, and open interfaces, SDN emerges as a feasible remedy to surmount these constraints. In SDN, the partitioning of the control and data planes facilitates effective network administration, financial savings, optimisation, and improved functionality. Anthology investigates a multitude of facets within this domain, encompassing security implications, the integration of SDN, network virtualization, and IoT, as well as the evaluation of security controller selection. SDN architecture advancements for IoT services, the efficacy of controllers such as Open Daylight, and the implementation of SDN to address challenges in Smart City IoT applications are all noteworthy discoveries. Notwithstanding the advantages that SDN offers for the Internet of Things, concerns regarding the effectiveness of live migration, security protocols, and appropriate administrative structures continue to be areas of continuous investigation. Qin et al. introduced the layered architecture of SDN controllers for IoT multi-networks, which is notable for its adaptability and efficiency in administering a variety of IoT scenarios.

Conflicts Of Interest

None

Funding

None

Acknowledgment

None

References

[1] Z. Qin et al., "A Software Defined Networking architecture for the Internet-of-Things," in *Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS)*, Krakow, Poland, 5–9 May 2014, pp. 1–9. [CrossRef]

[2] O. Salman et al., "A review on machine learning–based approaches for Internet traffic classification," *Ann. Telecommun.*, vol. 75, pp. 673–710, 2020. [CrossRef]

[3] L. Song et al., "QoS-Aware Energy-Efficient Cooperative Scheme for Cluster-Based IoT Systems," *IEEE Syst. J.*, vol. 11, pp. 1447–1455, 2017. [CrossRef]

[4] J. Chen et al., "When Software Defined Networks Meet Fault Tolerance: A Survey," in *Algorithms Archit. Parallel Process.*, 2015, pp. 351–368. [CrossRef]

[5] Z. Wen et al., "A RESTful framework for Internet of things based on software defined network in modern manufacturing," *Int. J. Adv. Manuf. Technol.*, vol. 84, pp. 361–369, 2016. [CrossRef]

[6] H. Babbar and S. Rani, "Software-Defined Networking Framework Securing Internet of Things," in *Integration of WSN and IoT for Smart Cities*, S. Rani et al., Eds. Springer International Publishing, 2020, pp. 1–14.

[7] H. Kang, C. Yoon, and S. Shin, "Astraea: Towards an effective and usable application permission system for SDN," *Comput. Netw.*, vol. 155, pp. 1–14, 2019. [CrossRef]

[8] A. L. Aliyu et al., "A Trust Management Framework for Software Defined Network (SDN) Controller and Network Applications," *Comput. Netw.*, 2020, 107421. [CrossRef]

[9] T. P. Anithaashri et al., "Security enhancement for software defined network using game theoretical approach," *Comput. Netw.*, vol. 157, pp. 112–121, 2019. [CrossRef]

[10] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," *Comput. Ind.*, vol. 104, pp. 47–58, 2019. [CrossRef]

[11] Y. Bi et al., "Intelligent Quality of Service Aware Traffic Forwarding for Software-Defined Networking/Open Shortest Path First Hybrid Industrial Internet," *IEEE Trans. Ind. Inform.*, vol. 16, pp. 1395–1405, 2020. [CrossRef]

[12] "Mininet: An Instant Virtual Network on Your Laptop (or Other PC)—Mininet." Available online: http://mininet.org/ (accessed on 13 September 2021).

[13] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet Things J.*, vol. 7, pp. 3559–3570, 2020. [CrossRef]

[14] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Decentralized Cloud-SDN Architecture in Smart Grid: A Dynamic Pricing Model," *IEEE Trans. Ind. Inform.*, vol. 14, pp. 1220–1231, 2018. [CrossRef]

[15] A. Yazdinejad et al., "An Energy-Efficient SDN Controller Architecture for IoT Networks with Blockchain-Based Security," *IEEE Trans. Serv. Comput.*, vol. 13, pp. 625–638, 2020. [CrossRef]

[16] R. K. Das et al., "6LE-SDN: An Edge-Based Software-Defined Network for Internet of Things," *IEEE Internet Things J.*, vol. 7, pp. 7725–7733, 2020. [CrossRef]

[17] T. Sato et al., "Remote Control Experiments of an Industrial Robot Using Two Distributed Robot Controllers." Available online: http://biblio.yamanaka.ics.keio.ac.jp/file/MPLS2016_extended_summaries_draft_final.pdf (accessed on 30 July 2021).

[18] S. Ahmad and A. H. Mir, "Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers," *J. Netw. Syst. Manag.*, vol. 29, p. 1, 2020. [CrossRef]

[19] R. Khondoker et al., "Feature-Based Comparison and Selection of Software Defined Networking (SDN) Controllers," in *Proceedings of the 2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Hammamet, Tunisia, 17–19 January 2014, pp. 1–7. [CrossRef]

[20] M. A. R. AlShehri and S. Mishra, "Feature Based Comparison and Selection of SDN Controller," *Int. J. Innov. Technol. Manag.*, vol. 16, p. 1950029, 2019. [CrossRef]

[21] V. A. Reddy, K. Venkatesh, and L. N. B. Srinivas, "Software Defined Networking Based Delay Sensitive Traffic Engineering of Critical Data in Internet of Things." Available online: https://www.ingentaconnect.com/content/asp/jctn/2020/00000017/00000001/art00010 (accessed on 5 July 2021).

[22] P. Thubert et al., "6TiSCH centralized scheduling: When SDN meet IoT," in *Proceedings of the 2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28–30 October 2015, pp. 42–47. [CrossRef]