Bulletin of Electrical Engineering and Informatics
Vol. 13, No. 1, February 2024, pp. 638∼647
ISSN: 2302-9285, DOI: 10.11591/eei.v13i1.6386

Software defined networking for internet of things: review, techniques, challenges, and future directions

Mahmood A. Al-Shareeda[1], Abeer Abdullah Alsadhan[2], Hamzah H. Qasim[1,3], Selvakumar Manickam[4]
[1]Department of Communication Engineering, Iraq University College, Basrah, Iraq
[2]Department of Computer Science, Applied College, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[3]Department of Oil and Gas Engineering, Basrah University Oil and Gas, Basrah, Iraq
[4]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, USM, Penang, Malaysia

Article Info

Article history:

Received Apr 3, 2023
Revised May 25, 2023
Accepted Jun 5, 2023

Keywords:

Internet of things
Software defined networking
Software defined networking-internet of things
Software defined networking review
Techniques

ABSTRACT

Security networks as one of the biggest issue for network managers with the exponential growth of devices connected to the internet. Keeping a big and diverse network running smoothly and securely is no easy feat. With this in mind, emerging technologies like software defined networking (SDN) and internet of things (IoT) hold considerable promise for information service innovation in the cloud and big data era. Therefore, this paper describes the model of SDN and the architecture of IoT. Then this review does not only review the research studies in SDN-IoT but also provides an explanation of the SDN-IoT solution in terms of architecture, main consideration, model, and the implementation of SDN controllers for IoT. Finally, this review discusses the challenges and future directions. This paper can be used as a starting point for thinking about how to improve SDN-IoT security and privacy.

Corresponding Author:

Selvakumar Manickam
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: selva@usm.my

1. INTRODUCTION

In the conventional networking architecture, specialised application-specific integrated circuits are put in networking devices like switches, routers, and intermediary devices to carry out specified functions [1]–[3]. Thus, in order to carry out their designated functions, the devices have been pre-programmed with a variety of complex basics (i.e., protocols) that cannot be altered in actual-time [4]–[6]. Furthermore, the devices' limited resources prevent them from being preprogrammed with many basics to supply optimal system applications. Therefore, conventional system technologies cannot instantly adjust rules sufficiently to fulfil the needs of internet of things (IoT) applications [7]–[9].

A novel concept called software-defined networking (SDN) is proposed to deal with these restrictions in conventional networks. Decoupling network control from the conventional hardware devices is a key feature of SDN [10], [11]. So, the primary goal of SDN is to divide the forwarding devices into a separate data plane from the control plane [12], [13]. It is expected that in the near future, all objects, including sensor devices, embedded networks, and middle nodes, will be able to gather and share data in order to realise the goals of a fully connected world, made possible by the concurrently outstanding system development of IoT [14], [15]. For different actual-time services like intelligent healthcare [16], smart transportation network [17], and intelligent energy technology [18]–[20], an IoT system typically includes various radio frequency identification (RFID) nodes and sensor constituting massive distributed embedded network [21], [22].

It is estimated that there will be 50 billion Internet-connected gadgets (sensors, smart cars, intelligent phones, RFID, apple watch, google glass, intelligent homes, and intelligent cities) in use worldwide by 2020, up from the current total of more than 15 billion. Massive amounts of data are produced by all of the internet-connected objects, making it challenging to keep the IoT network's management, resource allocation, and security in check. In order to solve the problems associated with IoT, we need a centralised monitoring for actual-time flow services and the holistic picture of the network provided by SDN for increased reliability.

The remainder of this paper is organized as follows. Section 2 describes the concept of SDN and the IoT. Section 3 provides an explanation of the SDN-IoT solution. Section 4 reviews the research studies in SDN-IoT. Section 5 discusses the challenges and future directions for this paper. Lastly, section 6 concludes this paper.

2. SOFTWARE DEFINED NETWORKING AND INTERSENSORS THINGS

This section presents SDN and IoT. We describe SDN technology in terms of overview and SDN model. Meanwhile, we describe IoT in terms of overview and architecture of IoT. The description of these technologies are as follows.

2.1. Software defined networking

This subsection presents SDN in details. We describe SDN technology in terms of overview and SDN model. The description of this SDN technology is as follows.

2.1.1. Overview

SDN is a relatively new framework that has been gaining popularity due to its adaptability, reliability, controllability, and high efficiency, making it ideally suited to the high-bandwidth, ever-changing requirements of modern applications. Separating the program's forwarding and control functions like this allows for digital communication to be decoupled from the underlying infrastructure and made directly programmable. To construct SDN solutions, the OpenFlow [23] protocol is essential.

2.1.2. SDN model

As shown in Figure 1, the following are the tiers that make up the SDN architecture. This model of architecture includes application, control layer, and data layers. The layer of network infrastructure, SDN control, and network infrastructure are based on application, control, and data, respectively.

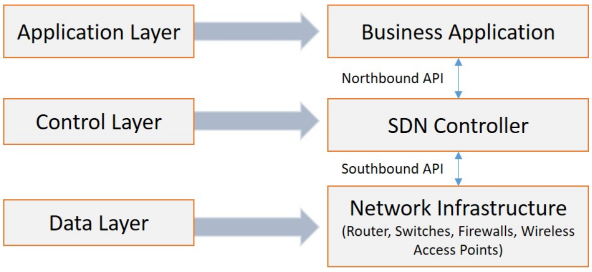

Figure 1. Model of SDN

- Application layer: applications can use what is called a ”management plan” to take use of northbound APIs to define a network's management policy; the controller will then take those commands and execute them locally on devices connected using southbound APIs.
- Control plan: it's the part of the network that has been separated from the components that make up the network itself, known as the SDN controller. This controller is responsible for translating the conduct basics determined by uses on the incoming flow into rules and injecting them into the program's routing equipment via the southbound APIs.
- Data plan: messages can be transferred between devices via either wireless signals or hardwired cords, based on the connection module included in each piece of technology.

- The APIs: each of the 4 kinds of APIs—northbound, southbound, eastbound, and oustbound—is responsible for facilitating interaction between specific parts of the SDN architecture.
  - *a*. The northbound API (RESTfull): offer a layer of system abstraction and expose it as a system to applications, and permit interfacing between the control layer and the application layer so that the ideal quality of service (QoS) for the application can be stated to the controllers.
  - *b*. The southbound API (Openflow): provides a bridge between the data plane and the control plane, letting you programmatically add rules to devices like routers, switches, and wireless access points; additionally, these devices can interact with the control plane.
  - *c*. TheEastbound and westbound APIs: in the context of using an orchestrator, both are put to use when connecting controllers so that they can work together to make decisions.
- Orchestrator: there is a requirement for complete software development. Users can connect via WiFi, WAN, LAN, and firewalls/other system nodes if the service can be applied in a datacenter. It is a fallacy to believe that a single controller can script the complete pipeline.

2.2. Internet of things

This section presents IoT in details. We describe IoT in terms of overview and architecture of IoT. The description of this IoT technology is as follows.

2.2.1. Overview

When there are more connected devices than individuals using the internet, we talk about the IoT. IoT aims to improve human existence by creating a smart environment through the use of ”smart things”. Which can collect data about their surroundings without human intervention.

2.2.2. Architecture of IoT

As shown in Figure 2, each of these components plays an important role in the IoT’s overall structure. The architecture of IoT includes perception, network, application, middleware layers. The component plays in the application layer is cloud and servers. The component plays in the network layer is router and gateways. The component plays in the perception layer is sensors and actuators.

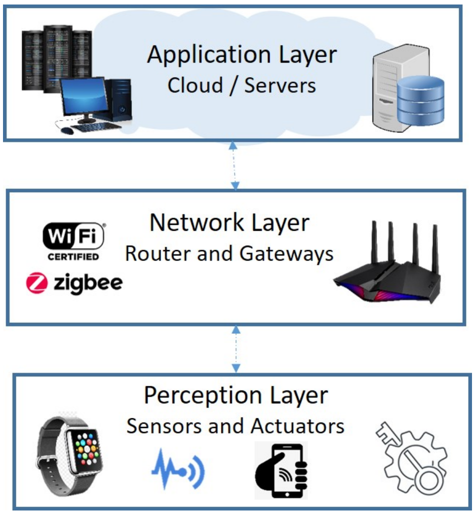

Figure 2. Architecture of IoT

- Layer of perception: it is made up of physical items that can sense and convert physical quantities (such as temperature, pressure, vibrations, and rays) into magnitudes of digital, then procedure, save, and wirelessly communicate this data to a sink or system gateway. The IoT includes things like wireless sensors [24], [25] radio frequency identification [26], handsets [27], wearables, connected automobiles [28], and intelligent houses [29].
- Network layer: it sends the analogue representation of the digital data gathered from the physical world to a sink or the network gateway. Many other technologies, such as Zigbee [30], low energy Bluetooth

[31], [32] Lorawan [33], [34], Wi-Fi [35], and many more, are found in this setting and are in a constant state of development [36].

- Application layer: it provides a means by which users can access data collected at the perception layer, modify those data to meet the needs of a given domain, and then feed those modified data into a processing network.
- Layer of middleware: when various IoT nodes in the same field need to connect with a single suitable device, this layer enables to parse the data being transmitted by the various pieces of hardware and convert it into addressable, service-specific data.

3. SOFTWARE DEFINED NETWORKING FOR INTERNET OF THINGS

3.1. Architecture of SDN-IoT

As shown in Figure 3, there are three tiers to the SDN-IoT as follows. The model of SDN-IoT includes infrastructure, control, and application layers. The description of each layer are provided as follows.

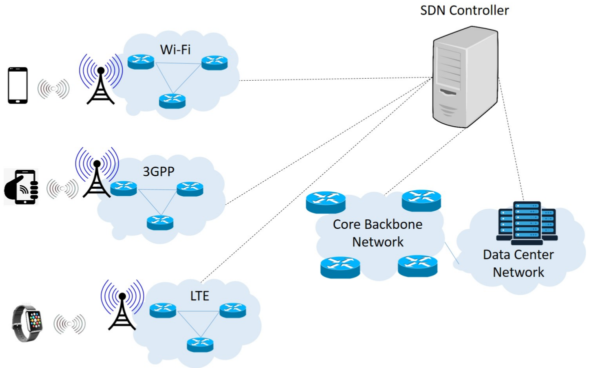

Figure 3. Architecture of SDN-IoT

- The infrastructure layer: linked to layer of access via base stations, wireless access points, and network gateways, this layer houses a wide variety of devices such as RFID readers RFID [26], wireless sensors [24], intelligent phones [27] with detecting capability, and intelligent automobiles [28].
- The control layer: it's the layer in between the service and the infrastructure, and it offers APIs that developers may use to build their own IoT apps. These APIs can also be used to manage data access and lower-level network devices.
- The application layer: allows IoT application tuning without requiring knowledge of lower network transport and data connection layers thanks to northbound APIs' ability to provide a full abstraction of the underlying network infrastructure.

3.2. Main considerations

The potential of SDN solutions to achieve the concept of software-defined IoT is discussed, along with some of the main considerations of IoT applications, as shown in Figure 4. The main considerations for SDN-IoT are network management, network function virtualization, accessing information from anywhere, resource utilization, energy management, security, and privacy. These considerations are described as follows.

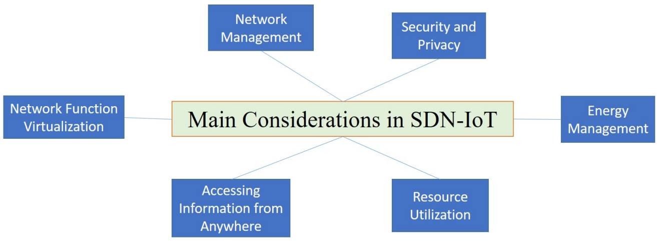
Network Management
Security and Privacy
Network Function Virtualization
Main Considerations in SDN-IoT
Energy Management
Accessing Information from Anywhere
Resource Utilization

Figure 4. Main considerations for SDN-IoT

– Network management: in the next decade or so, thanks to IoT technology, billions of objects will be in use all over the world [37]–[39]. As a result, it's clear that the devices will produce a flood of data that must be processed quickly and effectively. IoT network administration can benefit from SDN-based solutions including load balancing, traffic forwarding at a granular level, and better usage of available capacity [40], [41].
– Network function virtualization: recent advances in the field of network function virtualization (NFV) have made it possible for devices to switch between multiple roles and adapt their capabilities in real time to meet the needs of individual applications. Therefore, SDN-based approaches are crucial to bringing NFV to life in a massive-scale IoT network [42], [43].
– Accessing information from anywhere: the devices' user will be able to log in to their devices from any location at any time to manage and customise their devices' features as needed [44], [45]. SDN-based technology, such system components can be managed without invading anyone else's privacy [46], [47].
– Resource utilization: both under- and over-utilization can reduce a network's capacity, reducing the value of the system as a whole. So, better resource use is needed to increase the network's utility, and this in turn necessitates effective mapping of customer request [48]. Depending on the flow-rules set upon by the SDN controller, requests from numerous users can be routed along the appropriate path [49], [50].
– Energy management: it will take a massive infrastructure of data centres to process the massive amounts of information generated by the billions of IoT devices [51], [52]. This allows for dynamic ON/OFF switching of data centre devices as needed [53], which in turn creates a more efficient data centre networking environment. From the standpoint of an IoT network, this capability is quite useful [54].
– Security and privacy: it is crucial to ensure the safety of the devices and network in order to accommodate a wide variety of devices, vendors, and users on a single platform [55], [56]. Researchers need to take this into account so that users' privacy is protected as they use a unified platform across various devices. Security and privacy of network traffic are improved by SDN's fine-grained control of flows [57].

3.3. Model of SDN-IoT

Various architectures of SDN-IoT and their benefits, drawbacks, and applications are discussed here. The architectures of SDN-IoT are plugin IoTDM, cluster head, edge computer server, and distributed network control. These architectures for SDN-IoT are provided as follows.

– Plugin IoTDM architecture [58]: the primary function is to manage and store M2M-compliant data from IoT devices. This is because of common protocols for a wide variety of end-user programs and the potential for further plugins to be developed to link various technologies in industrial settings. However, an important IoTDM plugin relies on the OpenDaylight controller.
– Cluster head architecture [59]: most commonly, it is used to set up specialized subsystems within larger ones by connecting the many communication hubs within a cluster. This is because policies in the underlying network have been adopted based on how traffic is actually being used. However, the needs of the subsystem as a whole may have an impact on the flow of things.
– Edge computer server architecture [59]: efficient use of available computing resources. This is due to improve the response time of time-sensitive services by decreasing the amount of traffic on the network connecting them to the cloud. However, does not replace cloud-based servers, making the solution harder to implement and potentially costlier.
– Distributed network control architecture [60], [61]: management and command of isolated parts of a system. The ability to more quickly and precisely regulate the various parts of the network. Lack of a single point of failure throughout an industrial network. However, the solution becomes more complicated because of the need to coordinate multiple autonomous subsystem controllers.

3.4. The implementation of SDN controllers for IoT

This subsection explains the implementation of SDN controllers for IoT. This subsection only focuses on centralized, distributed, and hybrid. The description of these implementations is provided as follows.

– Centralized: complete network oversight and management. Keeping things easy for app developers by only having to worry about one set of system requirements. In large networks, bandwidth and control latency difficulties can be handled by a single controller. There are constraints on the system's ability to scale and resist failure.

- Distributed: improved capacity, scalability, and responsiveness to link failures, flow requests, intrusions, and other network events. Signifies an excessive amount of control traffic in the network and hence a need for a dynamic load balance. There are a number of obstacles, such as interoperability, consistency, and controller placement.
- Hybrid: permits enterprises and operators to ease into SDN networks. Having fewer demands placed on the SDN controller improves its responsiveness and scalability. Numerous restrictions arise from the wide variety of network gadgets that converge here. The configuration, topology, and management of a system are all intricately intertwined.

4. RESEARCH STUDIES IN SDN-IOT

This section reviews the achievement of an overall SDN-IoT solution in various research studies. There is a proposal for improving SDN's applicability in the IoT as a whole in [62]. A control layer comprising i) monitoring, ii) administration and optimization, and iii) acquisition, broadcasting, and processing based on the established area is also proposed by Wan *et al.* [63] to provide a comprehensive software definition of the IoT.

There are times when the scope of an SDN installation is severely limited. For instance, the almost predictable behaviour of wireless networks in IoT given in [64], [65] is achieved by having a centralised element (an SDN controller) take all decisions. Thus, the controller of SDN is responsible for generating routes and assigning time/frequency slots, among other factors. This implementation's drawback is that it can only be used with predictable flows, as those seen in IWSNs. The difficulty lies in extending this concept to scenarios that use the same network architecture but feature heterogeneous flow and dynamic behaviour [62], [66].

While OpenFlow isn't the only SDN-friendly specification, its guiding principles have been widely adopted, making it one of the most widely implemented criteria, as suggested in [67]. So, OpenFlow-based SDN has been used in real-world applications like corporate intranets and data centres. OpenFlow has a great deal of backing from the published works as well. In addition, certain authors, such as Hu [68], deal with all the needs for the efficient and practical deployment of OpenFlow/SDN systems. OpenFlow is also the gold standard in the framework for industrial automation described in [69]. Real-time reservations are a huge step forward for latency-sensitive applications, and they are presented in detail in [70].

Some of the issues with deploying SDN in IoT communication processes are described in [63], including the fact that: due to the huge amount of entire networks in IoT, distributed controllers are needed, and the configuration of a forwarding plane mentioned by software is a challenge as OpenFlow has improved and the commuter's flow chart has developed into a various structure table with more areas. The greater the significance of SDN's application. Specifically, Abdellatif *et al.* [71] is concerned with a larger-scale industrial network, rather than, say, the network of a single factory. The primary goal in this case is to supply network services dependent on the requirements of the applications being used.

Radanliev *et al.* [72] offer a summary of international projects focusing on various areas of industry 4.0. None of these concerns are tailored to industrial communication networks, nor do they address the technical challenges of today and the question of whether or not they will grow worse in the future. One possible replacement for traditional server hardware when implementing SDN in IoT is the utilization of Raspberry Pi (RPi) boards, as discussed in the aforementioned literature. Ahmed *et al.* [73] use a Raspberry Pi as a software-defined controller in place of more conventional proprietary programmable logic controllers (PLCs) in an experiment verifying their suggested design (PLC). The literature review also revealed that RPi plates are used as SDN switches.

Utilizing optimization mechanisms that guarantee the necessary QoS allows SDN to be used in industrial settings. The primary purpose of optimization algorithms is to identify the paths through a network that, given a set of goals, are the most effective at bringing about those goals. Optimization techniques like the L 1 norm used to minimise wait times are one example [73].

Industrial networks have a hard time providing the QoS required by some mission-critical applications like fault-tolerance, advanced control, remote monitoring, and predictive maintenance Bi *et al.* [74]. As suggested in [73], network technologies including WirelessHART, WebSocket, and constrained application protocol (CoAP) can be employed in SDN system area in IoT to create a SDN that meets the minimal needs of all IoT applications. The PROFINET standard was chosen for the control and data plane separation that materialised the suggested SDN standard in the study described in [69], thus the results are intriguing.

The challenges and worldwide objectives that may arise in IoT systems were addressed by Qin *et al.* [75], who began an enticing endeavour to simplify various operation features in IoT scenarios by shifting them to the link layer. Maximum acceptable delay, minimum data rate, and package loss for each autonomous flow are instances of packet processing [75]. Li *et al.* [59] conducted a classification that split traffic into regular and unexpected flows, although this is only one possible way to classify traffic. Effective security is the topic of the research by Babiceanu and Seker [76]. Additionally, Radanliev *et al.* [72] demonstrate how automation and AI can lessen IoT hazards.

5. CHALLENGES AND FUTURE DIRECTIONS

Despite these benefits and available technologies, additional research is required before complete integration of edge and fog computing on top of IoT applications can occur. The research community has significant issues, which we explore along with some new concepts and guidelines.

- Scalability: network architectures must be scalable if they are to effectively meet the needs of an increasing number of clients, such as mobile devices operating on the network's periphery.
- Service availability: for real-time applications like video streaming, which necessitate a short time for processing and response, availability is crucial in network architectures. However, in vehicular edge computing, in which many variables can impact the service availability, such as vehicles' mobility and obstacles, availability is especially crucial.
- High mobility support: most IoT devices, including smartphones, cars, and drones, are always in motion, which causes connectivity issues between them and servers.
- Energy management: with so many moving parts, the fog computing architecture is bound to have a high energy footprint and corresponding cost.
- Security and privacy: one of the most pressing concerns regarding edge and fog computing networks is the matter of security. Various tools, including cryptography, and hash functions, can accomplish this. To ensure the safety of data exchanges in an IoT network utilising fog computing, it must be implemented.

6. CONCLUSION

In light of the exploding number of Internet-connected devices, ensuring a safe and secure infrastructure has become a major headache for IT administrators. Keeping a network of this size and diversity up and running securely is no easy feat. SDNs have emerged in the past few years, giving network operators more leeway in terms of how they can manage and programme their network. Such a network overcomes the constraints of older ones. Therefore, this paper describes the concept of SDN and the IoT and provides an explanation of the SDN-IoT solution. Then, this paper also reviews the research studies in SDN-IoT and discusses the challenges and future directions for this paper.

REFERENCES

[1] R. K. Das, N. Ahmed, A. K. Maji and G. Saha, "Nx-IoT: Improvement of Conventional IoT Framework by Incorporating SDN Infrastructure," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2473-2482, 1 Feb.1, 2023, doi: 10.1109/JIOT.2022.3215650.

[2] A. Bhardwaj, K. Kaushik, M. Alshehri, A. A.-B. Mohamed, and I. Keshta, "Isf: Security analysis and assessment of smart home iot-based firmware," *ACM Transactions on Sensor Networks*, 2023, doi: 10.1145/3578363.

[3] S. Bhardwaj and S. N. Panda, "Performance evaluation using ryu sdn controller in software-defined networking environment," *Wireless Personal Communications*, vol. 122, no. 1, pp. 701–723, 2022, doi: 10.1007/s11277-021-08920-3.

[4] M. A. Al-Shareeda and S. Manickam, "A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework," *IEEE Access*, vol. 11, pp. 46218-46228, 2023, doi: 10.1109/ACCESS.2023.3274774.

[5] P. R. Desai, S. Mini, and D. K. Tosh, "Edge-based optimal routing in sdn-enabled industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18898-18907, Oct. 2022, doi: 10.1109/JIOT.2022.3163228.

[6] D. Das, S. Banerjee, K. Dasgupta, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain enabled sdn framework for security management in 5g applications," *24th International Conference on Distributed Computing and Networking*, Jan. 2023, pp. 414–419, doi: 10.1145/3571306.3571445.

[7] A. N. Mian, S. W. H. Shah, S. Manzoor, A. Said, K. Heimerl, and J. Crowcroft, "A value-added iot service for cellular networks using federated learning," *Computer Networks*, vol. 213, Aug. 2022, doi: 10.1016/j.comnet.2022.109094.

[8] Z. G. Al-Mekhlaf *et al.*, "Efficient authentication scheme for 5g-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, pp. 1–18, 2023, doi: 10.3390/s23073543.

[9] A. Liatifis, P. Sarigiannidis, V. Argyriou, and T. Lagkas, "Advancing sdn from openflow to p4: A survey," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–37, 2023, doi: 10.1145/3556973.

[10] S. Siddiqui *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, doi: 10.1109/ACCESS.2022.3188311.

[11] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, "Software-defined networking in vehicular networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 10, p. e4265, 2022, doi: 10.1002/ett.4265.

[12] S. Z. Marshoodulla and G. Saha, "An approach towards removal of data heterogeneity in sdn-based iot framework," *Internet of Things*, 2023, doi: 10.1016/j.iot.2023.100763.

[13] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "Anaa-fog: A novel anonymous authentication scheme for 5g-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, pp. 1–19, 2023, doi: 10.3390/math11061446.

[14] J. A. Shilvya *et al.*, "Home based monitoring for smart health-care systems: A survey," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/1829876.

[15] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for sdn-enabled intrusion detection system in iot networks," *Information*, vol. 14, no. 1, pp. 1–21, 2023, doi: 10.3390/info14010041.

[16] S. Venkatasubramanian, "Ambulatory monitoring of maternal and fetal using deep convolution generative adversarial network for smart health care iot system," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, 2022, doi: 10.14569/IJACSA.2022.0130126.

[17] R. Jabbar *et al.*, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, vol. 10, pp. 20995-21031, 2022, doi: 10.1109/ACCESS.2022.3149958.

[18] H. Zhu *et al.*, "Key technologies for smart energy systems: Recent developments, challenges, and research opportunities in the context of carbon neutrality," *Journal of Cleaner Production*, vol. 331, 2022, doi: 10.1016/j.jclepro.2021.129809.

[19] S. Javanmardi, M. Shojafar, R. Mohammadi, V. Persico, and A. Pescape, "S-fos: A secure workflow scheduling approach for performance optimization in sdn-based iot-fog networks," *Journal of Information Security and Applications*, vol. 72, 2023, doi: 10.1016/j.jisa.2022.103404.

[20] A. Razmjoo, S. Mirjalili, M. Aliehyaei, P. A. Østergaard, A. Ahmadi, and M. M. Nezhad, "Development of smart energy systems for communities: Technologies, policies and applications," *Energy*, vol. 248, 2022, doi: 10.1016/j.energy.2022.123540.

[21] D. Sahana and S. Brahmananda, "Secure authentication framework for sdn-iot network using keccak-256 and bliss-b algorithms," *International Journal of Information Technology*, vol. 15, no. 1, pp. 335–344, 2023, doi: 10.1007/s41870-022-01074-w.

[22] B. A. Mohammed *et al.*, "Fc-pa: Fog computing-based pseudonym authentication scheme in 5g-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571-18581, 2023, doi: 10.1109/ACCESS.2023.3247222.

[23] T. Kunz and K. Muthukumar, "Comparing openflow and netconf when interconnecting data centers," *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, Toronto, ON, Canada, 2017, pp. 1-6, doi: 10.1109/ICNP.2017.8117598.

[24] J. Frolik, J. E. Lens, M. M. Dewoolkar, and T. M. Weller, "Effects of soil characteristics on passive wireless sensor interrogation," *IEEE Sensors Journal*, vol. 18, no. 8, pp. 3454-3460, Apr. 2018, doi: 10.1109/JSEN.2018.2810132.

[25] A. Alotaibi and A. Barnawi, "Securing massive iot in 6g: Recent solutions, architectures, future directions," *Internet of Things*, 2023, doi: 10.1016/j.iot.2023.100715.

[26] J. F. Zhang and C. J. Wen, "The university library management system based on radio frequency identification," *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Shanghai, China, 2017, pp. 1-6, doi: 10.1109/CISP-BMEI.2017.8302176.

[27] K. B. Jadhav and U. M. Chaskar, "Design and development of smart phone based ecg monitoring system," *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2017, pp. 1568-1572, doi: 10.1109/RTEICT.2017.8256862.

[28] P. Satam, J. Pacheco, S. Hariri, and M. Horani, "Autoinfotainment security development framework (ASDF) for smart cars," *2017 International Conference on Cloud and Autonomic Computing (ICCAC)*, Tucson, AZ, USA, 2017, pp. 153-159, doi: 10.1109/ICCAC.2017.22.

[29] D. Pal, S. Funilkul, N. Charoenkitkarn, and P. Kanthamanon, "Internet-of-things and smart homes for elderly healthcare: An end user perspective," *IEEE Access*, vol. 6, pp. 10483-10496, 2018, doi: 10.1109/ACCESS.2018.2808472.

[30] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2017, pp. 195-212, doi: 10.1109/SP.2017.14.

[31] H. Zemrane, Y. Baddi, and A. Hasbi, "Sdn-based solutions to improve iot: survey," *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, Marrakech, Morocco, 2018, pp. 588-593, doi: 10.1109/CIST.2018.8596577.

[32] D. Antonioli, N. O. Tippenhauer, K. Rasmussen, and M. Payer, "Blurtooth: Exploiting cross-transport key derivation in bluetooth classic and bluetooth low energy," *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 196–207, doi: 10.1145/3488932.3523258.

[33] R. Fujdiak, K. Mikhaylov, J. Pospisil, A. Povalac, and J. Misurec, "Insights into the issue of deploying a private lorawan," *Sensors*, Tvol. 22, no. 5, pp. 1–25, 2022, doi: 10.3390/s22052042.

[34] Z. G. Al-Mekhlaf *et al.*, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5g-enabled vehicular networks," *Electronics*, vol. 12, no. 4, pp. 1–12, 2023, doi: 10.3390/electronics12040872.

[35] S. Nishikori, K. Kinoshita, Y. Tanigawa, H. Tode, and T. Watanabe, "A cooperative channel control method of zigbee and wifi for iot services," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCNC.2017.7983071.

[36] P. Chauhan and M. Atulkar, "A framework for ddos attack detection in sdn-based iot using hybrid classifier," *Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021*, 2023, pp. 889–900, doi: 10.1007/978-981-19-5868-7_67.

[37] O. Vermesan *et al.*, "Internet of things cognitive transformation technology research trends and applications," *Cognitive Hyperconnected Digital Transformation*, pp. 17–95, 2022.

[38] C. Gundogan, P. Kietzmann, T. C. Schmidt, and M. Wahlisch, "Information-centric networking for the industrial internet of things," *Wireless Networks and Industrial IoT*, 2021, pp. 171–189, doi: 10.1007/978-3-030-51473-0_9.

[39] A. Alamer, "Security and privacy-awareness in a software-defined fog computing network for the internet of things," *Optical Switch-*

ing and Networking, vol. 41, Sep. 2021, doi: 10.1016/j.osn.2021.100616.

[40] L. F. Eliyan and R. Di Pietro, "Dos and ddos attacks in software defined networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, 2021, doi: 10.1016/j.future.2021.03.011.

[41] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114-119, Feb. 2013, doi: 10.1109/MCOM.2013.6461195.

[42] M. Priyadarsini and P. Bera, "Software defined networking architecture, traffic management, security, and placement: A survey," *Computer Networks*, vol. 192, 2021, doi: 10.1016/j.comnet.2021.108047.

[43] P. Kujur and S. Patel, "Network Functions Virtualization and SDN," *Software Defined Networks: Architec- ture and Applications*, pp. 191–229, 2022, doi: 10.1002/9781119857921.ch7.

[44] D. Giusto, A. Iera, G. Morabito, and L. Atzori, *The internet of things: 20th Tyrrhenian workshop on digital communications*, Springer Science & Business Media, 2010.

[45] N. Atta, "Internet of things, big data and information platforms for advanced information management within fm processes," *Internet of Things for Facility Management*, 2021, pp. 41–49, doi: 10.1007/978-3-030-62594-8_4.

[46] K. Kawila, J. Kim, and K. Rojviboonchai, "An sdn-coordinated steering framework for multipath big data transfer application," *IEEE Access*, vol. 10, pp. 95859-95875, 2022, doi: 10.1109/ACCESS.2022.3205118.

[47] H. Yoon, S. Kim, T. Nam, and J. Kim, "Dynamic flow steering for iot monitoring data in sdn-coordinated iot-cloud services," *2017 International conference on information networking (ICOIN)*,Da Nang, Vietnam, 2017, pp. 625-627, doi: 10.1109/ICOIN.2017.7899572.

[48] S. Sharma and V. K. Verma, "An integrated exploration on internet of things and wireless sensor networks," *Wireless Personal Communications*, vol. 124, no. 3, pp. 2735–2770, 2022, doi: 110.1007/s11277-022-09487-3.

[49] G. Han, A. M. Abu-Mahfouz, J. J. Rodrigues, and X. Wang, "Guest editorial: Ai-enabled software-defined industrial networks: Architectures, algorithms, and applications," in *IEEE Transactions on Industrial Informatics,*, vol. 18, no. 6, pp. 4210-4214, June 2022, doi: 10.1109/TII.2022.3142146.

[50] N. Samarji and M. Salamah, "ESRA: Energy soaring-based routing algorithm for IoT applications in software-defined wireless sensor networks," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 215–224, 2022, doi: 10.1016/j.eij.2021.12.004.

[51] F. Emmert-Streib and O. Yli-Harja, "What is a digital twin? experimental design for a data-centric machine learning perspective in health," *International Journal of Molecular Sciences*, vol. 23, no. 21, pp. 1–12, 2022, doi: 10.3390/ijms232113149.

[52] J. H. Kim, "6g and internet of things: a survey," *Journal of Management Analytics*, vol. 8, no. 2, pp. 316–332, 2021, doi: 10.1080/23270012.2021.1882350.

[53] E. Masanet, A. Shehabi, N. Lei, S. Smith, and J. Koomey, "Recalibrating global data center energy-use estimates," *Science*, vol. 367, no. 6481, pp. 984–986, 2020, doi: 10.1126/science.aba3758.

[54] F. F. Jurado-Lasso, K. Clarke, and A. Nirmalathas, "A software-defined management system for IP-enabled WSNs," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2335-2346, June 2020, doi: 10.1109/JSYST.2019.2946781.

[55] R. Faqihi, J. Ramakrishnan, and D. Mavaluru, "An evolutionary study on the threats, trust, security, and challenges in siot (social internet of things)," *Materials today: proceedings*, 2020, doi: 10.1016/j.matpr.2020.09.618.

[56] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy internet of things: A survey on trust management applications and schemes," *Computer Communications*, vol. 160, pp. 475–493, 2020, doi: 10.1016/j.comcom.2020.06.030.

[57] 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, doi: 10.3390/computers9010008.

[58] J. L. Romero-Gazquez and M. Bueno-Delgado, "Software architecture solution based on sdn for an industrial iot scenario," *Wireless Communications and Mobile Computing*, vol. 2018, 2018, doi: 10.1155/2018/2946575.

[59] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in sdn-based industrial internet of things with edge computing," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1351-1360, Jun. 2018, doi: 10.1109/JIOT.2018.2797187.

[60] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for iot networks with blockchain-based security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-638, 1 Jul.-Aug. 2020, doi: 10.1109/TSC.2020.2966970.

[61] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[62] N. Bizanis and F. A. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey," in *IEEE Access*, vol. 4, pp. 5591-5606, 2016, doi: 10.1109/ACCESS.2016.2607786.

[63] J. Wan *et al.*, "Software-defined industrial internet of things in the context of industry 4.0," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7373-7380, Oct.15, 2016, doi: 10.1109/JSEN.2016.2565621.

[64] P. Thubert, M. R. Palattella, and T. Engel, "6TiSCH centralized scheduling: When SDN meet IoT," in *2015 IEEE conference on standards for communications and networking (CSCN)*, Tokyo, Japan, 2015, pp. 42-47, doi: 10.1109/CSCN.2015.7390418.

[65] M. Mahamat, G. Jaber, and A. Bouabdallah, "Achieving efficient energy-aware security in iot networks: a survey of recent solutions and research challenges," *Wireless Networks*, vol. 29, no. 2, pp. 787–808, 2023, doi: 10.1007/s11276-022-03170-y.

[66] M. K. Pulligilla and C. Vanmathi, "An authentication approach in sdn-vanet architecture with rider-sea lion optimized neural network for intrusion detection," *Internet of Things*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100723.

[67] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart factory of industry 4.0: Key technologies, application case, and challenges," in *IEEE Access*, vol. 6, pp. 6505-6519, 2018, doi: 10.1109/ACCESS.2017.2783682.

[68] F. Hu, *Network Innovation through Openflow and SDN*. Crc Press, 2014.

[69] K. Ahmed, J. O. Blech, M. A. Gregory, and H. Schmidt, "Software defined networking for communication and control of cyber-physical systems," in *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, Melbourne, VIC, Australia, 2015, pp. 803-808, doi: 10.1109/ICPADS.2015.107.

[70] L. Silva, P. Goncalves, R. Marau, and P. Pedreiras, "Extending openflow with industrial grade communication services," *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, Trondheim, Norway, 2017, pp. 1-4, doi: 10.1109/WFCS.2017.7991965.

[71] S. Abdellatif, P. Berthou, T. Villemur, and F. Simo, "Management of industrial communications slices: Towards the application

driven networking concept," *Computer Communications*, vol. 155, pp. 104–116, 2020, doi: 10.1016/j.comcom.2020.02.057.

[72] P. Radanliev, D. De Roure, R. Nicolescu, and M. Huth, "A reference architecture for integrating the industrial internet of things in the industry 4.0," *University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre*, vol. 2, 2019.

[73] K. Ahmed, J. O. Blech, M. A. Gregory, and H. W. Schmidt, "Software defined networks in industrial automation," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 33, 2018, doi: 10.3390/jsan7030033.

[74] Y. Bi, G. Han, C. Lin, Y. Peng, H. Pu, and Y. Jia, "Intelligent quality of service aware traffic forwarding for software-defined networking/open shortest path first hybrid industrial internet," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1395-1405, Feb. 2020, doi: 10.1109/TII.2019.2946045.

[75] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the internet-of-things," *2014 IEEE network operations and management symposium (NOMS)*, Krakow, Poland, 2014, pp. 1-9, doi: 10.1109/NOMS.2014.6838365.

[76] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial internet of things: A software-defined networking approach," in *Computers in industry*, vol. 104, pp. 47–58, 2019, doi: 10.1016/j.compind.2018.10.004.

BIOGRAPHIES OF AUTHORS

Mahmood A. Al-Shareeda obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a lecturer at communication engineering, Iraq College University, Basra, Iraq. His current research interests include network monitoring, internet of things (IoT), vehicular ad hoc betwork (VANET) security and IPv6 security. He can be contacted at email: alshareeda022@gmail.com.

Abeer Abdullah Alsadhan is currently working as Assistant Professor in Information Security and Artificial Intelligence at Imam Abdulrahman Bin Faisal University Dammam Saudi Arabia. Her research interests include machine learning, deep learning, cyber security, and internet of things. She has published a number of publications in reputed journals. She can be contacted at email: Aalsadhan@iau.edu.sa.

Hamzah H. Qasim received the B.S. degrees in Communication Engineering. In 2018, he received the M.Sc. degree in Electrical Engineering from University Tun Hussein Onn Malaysia (UTHM), Malaysian. He is currently PhD student in Universiti Teknologi MARA (UiTM), Malaysian. In addition, he is currently a lecturer In Basrah University for Oil and Gas, Department of Oil and Gas Engineering. His current research interests include IoT, WSN, V2X; SUMO, OMNET++ and mobility management for resource allocation in cellular communication. He can be contacted at email: Enghamza.iq@gmail.com and Hamza.hadi@buog.edu.iq.

Selvakumar Manickam is currently working as an Associate Professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 Ph.Ds. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.