Indonesian Journal of Electrical Engineering and Computer Science
Vol. 32, No. 2, November 2023, pp. 915~924
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v32.i2.pp915-924

Software defined internet of things in smart city: a review

Imran Edzereiq Kamarudin, Mohamed Ariff Ameedeen, Mohd Faizal Ab Razak, Azlee Zabidi
Department of Computer Systems and Networking, Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, Malaysia

Article Info

Article history:

Received Apr 10, 2023
Revised Jul 24, 2023
Accepted Jul 28, 2023

Keywords:

Collaboration
Internet of things
SDIoT
Smart city
Software define networking

ABSTRACT

The concept of smart cities has gained traction to enhance citizens' quality of life amidst rapid urbanization. Integration of the internet of things (IoT) is a key component that allows for gathering real-time data to inform decision-making and drive innovation in urban planning and management. However, managing the amount of data generated and the IoT devices rapid growth poses a challenge that leads to network management, interoperability, security, and scalability issues in smart cities. To overcome such problems, integrating software define networking (SDN) in IoT provides a flexible, scalable, and efficient network architecture that can better support the unique demands of IoT devices and applications. Motivated by the extensive research efforts in the software defined internet of things (SDIoT), this paper aims to review SDIoT implementation in smart cities. It first introduces the underlying technology along with various practical applications of SDIoT. The comprehension of SDIoT in smart cities focus on IoT application requirements, including interoperability, scalability, low latency requirement, handling of big data, security, and privacy, energy consumption, quality of service (QoS), and task offloading. The paper concludes by discussing the future research directions that need to be examined in greater depth.

Corresponding Author:

Mohamed Ariff Ameedeen
Department of Computer Systems and Networking, Faculty of Computing
Universiti Malaysia Pahang Al-Sultan Abdullah
26600 Pekan, Pahang, Malaysia
Email: mohamedariff@ump.edu.my

1. INTRODUCTION

In recent years, the internet of things (IoT) has garnered significant interest from both academia and industry, largely driven by the increasing demand for IoT devices. This trend has become a key component of the broader shift towards digital transformation, as IoT enables the integration of the digital and physical realms. Benefiting from this transformation, a wide range of smart devices and ecosystems has been introduced in the market, including homes, vehicles, transportation, health care, and industrial products. It is estimated that by 2030, the economic value IoT could generate is between $5.5 trillion to $2.6 trillion globally, including products and services [1].

With the rapid development of IoT, significant research efforts have been made toward active development and deployment to address its limitation. The major critical success in IoT depends on interoperability and open access between different platforms [2]. Each IoT platform solution offers a distinct infrastructure, devices, application programming interfaces (APIs), and data format. As a result, this creates a challenge for closed ecosystem platforms to work with each other. Furthermore, IoT devices come from heterogeneous network environments [3]. This environment and the vertical fragmented network platform add to the complexity of supporting the large-scale IoT network. Thus, both interoperability and supporting heterogeneous network plays a vital role in the scalability of IoT. With an increase in connected IoT devices, the large amount of data generated presents another challenge for today's networks to handle efficiently [4]. As a result, new ways to filter, classify, and selecting only required data are needed before transmitting to centralized cloud storage. It involves not only data management but also the security and privacy of the data [5].

Software-define internet of things (SDIoT) architecture has been proposed for effective network resource management [6]. With the advancement of IoT, it is crucial to manage the large scale of the network resources. Software define networking (SDN) is a technology that can respond to these IoT requirements by providing centralized control and an overview of the whole network. The centralized control enables network resources to be optimized effectively and adjust dynamically while ensuring interoperability across a heterogenous IoT network. SDN provides a layered framework by separating the data and the control plane to facilitate network resource administration, traffic management, network evolution, and flexible network programmability. The flexibility of SDN to manage the network has been seen as one of the key enablers in solving IoT challenges, especially in managing the complexity of IoT networks [7].

This review performs a detailed study of the literature available on the SDIoT paradigm. It focuses on how SDN and IoT can collaborate by leveraging the advantages of SDN into IoT. Furthermore, this study includes a comprehensive discussion of requirements based on existing works done based on smart cities IoT applications. The key contribution of this review is as:
- Present the foundation of SDIoT by individually reviewing relevant literature on IoT, SDN, and SDIoT.
- Discuss, analyze, and evaluate current implementation efforts of SDIoT to address IoT application requirements in smart cities.
- Present open research challenges and future research directions to provide a roadmap for future research.

2. METHOD

The review process [8] involves three sequential steps: identification, scanning, and eligibility testing to identify and narrow down the search results. The search strategy is based on a combination of keywords; we used the following combination of keywords as the search string: i) "software defined networking" OR "SDN"; ii) "internet of things" OR "IOT"; and iii) "smart cities". The search string is used for articles between 2019 and 2023 in databases such as Web of Science, Elsevier's Scopus, IEEE, MDPI, ACM Digital Library, and Google Scholar. Figure 1 summarizes all steps, including the number of papers identified through database search, removing duplicate and non-conforming papers and lastly, removing papers that are not related in the eligibility testing. After this final step, we selected 29 papers to be included in this review.

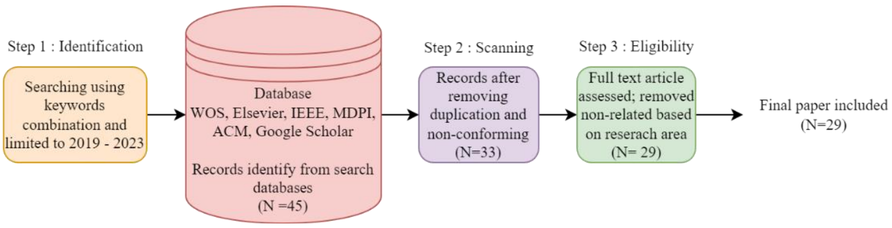

Figure 1. Article selection diagram. N represents the number of papers

3. UNDERLYING TECHNOLOGY

This section discusses the fundamental technologies that serve as the foundation for SDIoT for effective smart cities implementation. It covers the architecture of IoT, SDN, and SDIoT. Understanding these foundational technologies provides valuable insights into how SDIoT empowers smart city initiatives, enabling them to leverage data-driven solutions, optimize resource management, and elevate the overall quality of life for urban residents.

3.1. Internet of things

IoT is an interconnected network of physical objects such as devices, vehicles, buildings, and other items that have been outfitted with sensors, software, and network connectivity, allowing them to collect and share data. This technology has the potential to revolutionize industries and our daily lives by allowing for more informed decisions, increasing efficiency and productivity, and improving the quality of life. International bodies such as the institute of electrical and electronics engineers (IEEE) plays an important role through their research, standards, and education initiatives on IoT [9]. Furthermore, IEEE has a working group, participating in various areas such as generating IoT-related standards for architecture and framework, quality of experience (QoE) and quality of service (QoS) performance, protocol, and test specifications. In addition, when adopted, these standards will guarantee interoperability, security, and reliability in designing and deploying IoT systems [10].

Generally, IoT focuses on various sensors and smart devices that offer a wide range of connectivity and network capabilities. As a result, a significant amount of data will be generated, requiring massive storage and processing power [11]. Figure 2 depicts three main components in IoT architecture: the perception, network, and application layers. First, sensors or actuators in the perception layer gather data from the physical world. Next, the collected data will be filtered, pre-processed, and analyzed in real-time if the gateways are capable. Otherwise, the data will be routed to the next destination, the application layer, which typically consists of higher storage and computation facilities such as cloud computing. Finally, in the application layer, IoT applications frequently use the cloud and the services it provides to store and process data for IoT applications. Examples of IoT applications are smart transportation, smart campus, precision farming, hospitals. and monitoring videos, utilizing these data to provide desirable services for end customers.

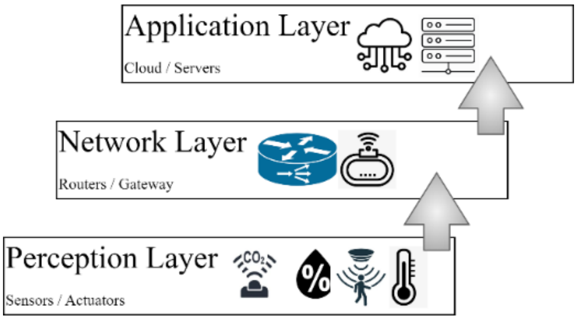

Figure 2. IoT architecture

2.2. Software defined networking

The core concept of SDN is network programmability, which sets it apart from traditional networks. This approach divides the network hardware and software, allowing the network hardware to be generalized and the network control software to be separated from the implementation devices [12]. By isolating the control plane from the network devices, SDN enables the centralization of data control through an external software entity known as the SDN controller. This controller can initiate, regulate, alter, and oversee network behavior through open interfaces in a dynamic manner. SDN's overall architecture comprises four planes: forwarding, management, control, and application planes, as illustrated in Figure 3.

The forwarding plane, also known as the data plane or data path, handles and forwards packets. The forwarding plane provides routing, switching, packet transformation, and filtering functions [13]. Furthermore, it manages packets in the data stream in accordance with the instructions received from the control plane. The data packets can be forwarded, discarded, or modified depending on the action required. The data plane presents a forwarding table that forwards the incoming packets to a network device. Typically, the forwarding plane is where control plane services and applications terminate. Network devices such as switches and routers can be implemented in hardware or software, either physical or virtual.

The management plane [14] is responsible for configuring, monitoring, and maintaining network devices, such as determining the network device’s status. In addition, it provides intelligent provisioning and orchestration systems for entire network management. It ensures the network is running optimally by communicating with the network devices. Typically, the management plane is more concerned with the operational plane of the device than the forwarding plane.

The control plane determines how network devices should send packets and pushes those decisions down to network devices for execution [15]. Typically, the control plane is more concerned with the forwarding plane than the operational plane of the device. The control plane may be interested in operational-plane data, such as a particular port’s current status or capabilities. The primary responsibility of the control plane is to fine-tune the forwarding tables residing in the forwarding plane based on the network topology or external service demands. SDN controllers have three interfaces to facilitate communication: northbound toward the application plane, southbound toward the forwarding plane, and eastbound toward other SDN controllers [16].

The application plane hosts applications and services that determine network behavior. This can encompass a range of business applications that manage and optimize various services. To achieve their specific network requirements and behavior, each application communicates directly with the SDN controller through NBIs [17]. Moreover, services within the application plane may offer their services to other applications and services through the service interface. Some example of applications in this layer include network provisioning, path reservation, and network topology discovery.

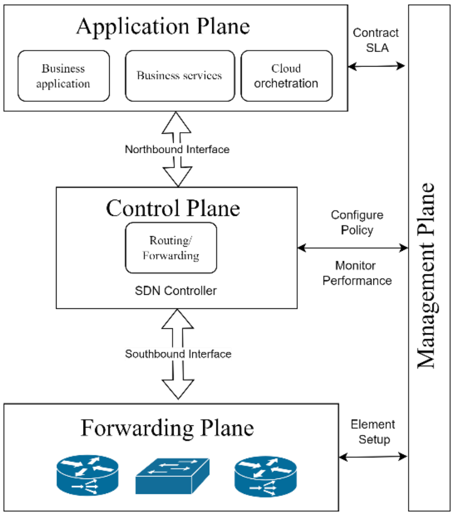

Figure 3. SDN architecture

2.3. Software defined internet of things

SDIoT extends the SDN approach to collect and aggregate data from the IoT perception layer. Compared with the traditional IoT architecture (access, network, and application layer), the SDIoT architecture will have facilities for managing the security and network resources with a centralized control plane. SDIoT is built on the traditional IoT protocol stack, with improvisations of the control plane in the network layer. Its architecture comprises four main components: the forwarding, control, application, and management plane [18].

Figure 4 depicts the SDIoT architecture. It emphasizes the importance of separating services provided in the control plane from those in the forwarding plane [19]. The control plane is responsible for managing network traffic, while the data plane defines the mechanisms for forwarding traffic to the intended destination. This separation ensures that the applications in the management layer interact efficiently with the control plane and collaborate effectively. Additionally, it enables network administrators to define how the control process should be governed by both the SDN controller and human users.

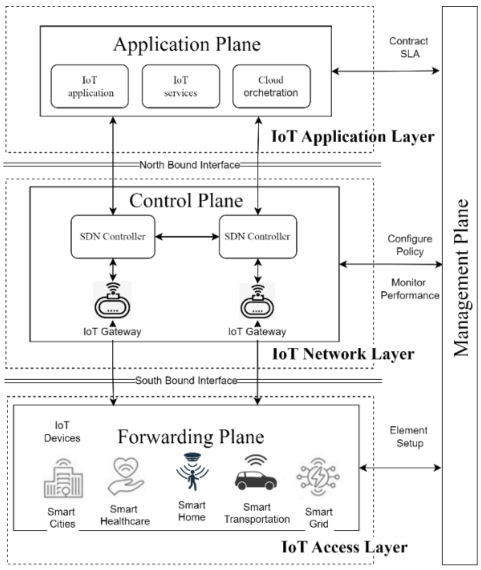

Figure 4. SDIoT architecture

4. SDIOT IN SMART CITIES

This section reviews recent works on smart cities based on SDIoT approaches to address IoT application requirements. The criteria of IoT application requirements include interoperability, scalability, low latency, handling of big data, security and privacy, energy consumption, QoS, and task offloading. Table 1 summarizes the criteria description.

Table 1. Smart cities iot application requirement criteria

Criteria	Description
Interoperability (C1)	The ease of exchanging information among heterogeneous software and hardware.
Scalability (C2)	The IoT ecosystems need to manage the ever-increasing load of work or the possibility of expanding them to deal with that load successfully.
Low latency (C3)	Prioritizing low latency applications with limited resources.
Handling of big data (C4)	Data duplication and redundancy, which will create unnecessary storage loads.
Security and privacy (C5)	Secure IoT infrastructure where multiple users, devices, and service provider participate in a single platform.
Energy consumption (C6)	Manage and optimize energy consumption without compromising IoT services.
QoS (C7)	Classification and prioritizing certain types of IoT network traffic receive priority treatment over others.
Task Offloading (C8)	To meet service level requirements, it is crucial to handle continuous offloading services seamlessly, which involves a smooth transition from task commitment to either the edge or cloud network and reconnecting as needed.

Smart city [20] is a modern urban area that uses different devices, especially IoT, to collect specific data. With real-time data, urban infrastructure can be managed for energy consumption, traffic congestion reduction, sanitation services, lighting, and parking management [21]. Several recent works have been done based on SDIoT architecture to mitigate IoT application requirements in smart cities. Table 2 provides a brief comparison of the articles under review.

Table 2. Recent work addressing IoT application requirement with SDIoT

Author	Criteria							
	C1	C2	C3	C4	C5	C6	C7	C8
Alassery [22]				✓		✓		
Fawwaz *et al*. [20]		✓				✓		
Sellami *et al*. [23]			✓			✓		
Lin *et al*. [24]			✓			✓		
Chen and Chen [25]	✓		✓	✓	✓			
Kumar *et al*. [26]								✓
Babbar *et al*. [27]		✓	✓					
Keshari *et al*. [28]		✓	✓					
Babbar *et al*. [29]		✓				✓		
Khazael *et al*. [30]			✓			✓		
Eghbali and Lighvan [31]			✓	✓		✓		
Lv *et al*. [32]		✓		✓			✓	
Ke *et al*. [33]			✓			✓		
Peyman *et al*. [34]		✓		✓				
Yang [17]			✓			✓		
Cao *et al.* [35]	✓						✓	
Li *et al*. [36]	✓						✓	
Silva *et al*. [37]					✓			
El-Garoui *et al*. [38]	✓					✓		
Xu *et al*. [39]					✓	✓		✓
Zhang [40]		✓		✓				
Gheisari *et al*. [41]		✓			✓			
Alsmadi *et al*. [42]					✓	✓		
Lin *et al*. [43]		✓						✓
Lin *et al*. [44]		✓	✓					
Guo *et al*. [45]		✓						✓
Liu *et al*. [46]			✓			✓		
Rego *et al*. [47]	✓					✓		
Chaudhary *et al*. [48]					✓	✓	✓	

To manage the massive amount of data, smart cities require efficient, fast, and intelligent data analysis [22], [48]. This process requires compute-intensive devices near the end user to make fast decision, especially for latency-aware applications such as traffic control and public safety. Furthermore, fast decisions can be archived without human interaction by integrating machine learning algorithms [45], [49], [50] into the smart cities platform. Another significant aspect of smart cities is managing the overall network resources. With the massive scale of an urban area, a centralized control that can oversee the whole network is desirable [27]. For example, traffic lights and other traffic control systems can be connected to a central network, which manages and optimize traffic flow and reduce congestion.

Several notable works are worth highlighting based on SDIoT architecture to mitigate IoT application requirements in smart cities. To address the interoperability, El-Garoui *et al*. [38] proposed an SDN-based routing protocol that combines SDN's flexibility with Naive Bayes prediction to improve delay by predicting destination node location and periodically gathering network node statistics. The simulation results show that the routing scheme outperforms comparative protocols. Meanwhile, Kumar *et al*. [26] proposed software-defined control-enabled deep reinforcement learning (SDDRL), a traffic-light scheduling framework that uses machine learning algorithm to balance traffic flow and prevent congestion in dense regions. The simulation shows the effectiveness of SDDRL compared to other algorithms. However, both solutions require high CPU and storage usage.

In order to address the scalability, Babbar *et al*. [29] proposed a multiple distributed controller load balancing algorithm (MDCLB) to solve load unbalancing on an immense-scale SDN-IoT for smart cities. Simulation results showed lower CPU utilization compared to other load-balancing algorithms. Meanwhile, Eghbali and Lighvan [31] proposed a hierarchical SDN-based approach for load balancing and data management between IoT devices in a single domain and different network clusters. The simulation shows improved processing performance, task distribution, and network resource usage. However, energy consumption was not considered in both works.

Keshari *et al.* [28] proposed an intelligent differential evolution and whale optimization (DEWO) algorithm to optimize SDN controller placement in smart cities networks for minimum latency by minimizing link failure and evaluating end-to-end delay. The simulation results show minimum delays for both average and worst-case scenarios. Meanwhile, Babbar *et al*. [29] proposed a dynamic QoS-aware load balancing switch migration algorithm (LBSMT) to efficiently improve throughput, response time, CPU, and memory utilization in ITS communication. The simulation shows promising results compared to existing schemes, but the proposed approach may be complex in a dense network. Both works aimed to address the low latency requirement. However, the possibility of applying both approaches in real environments is still an open issue.

Alassery [22], proposed a priority packets deadline first (PPDF) scheme to address the handling of big data, focusing on emergency applications in smart cities. The scheme goal is to reduce waiting time, end-to-end delay, packet loss and energy consumption. PPDF prioritises packets between controllers and destination nodes by starting with the earliest deadline. The proposed scheme effectively manages network resources by facilitating the transfer of priority information between source and destination nodes, while also ensuring access to nodes through the time-division multiple access medium access control (TDMA MAC) protocol.

Alsmadi *et al*. [42], proposed an SDIoT framework with the counter-based DDoS attack detection (C-DAD) application, which efficiently detects DDoS attacks with less CPU and memory resources consumption through SDN. On the other hand, Chaudhary *et al*. [48], introduced a blockchain-based secure energy trading (BEST) scheme for electric vehicles (EVs), using SDN to transfer requests to a global controller while validating them through miner nodes in a distributed manner. BEST increases security, imposes minimal overheads, and ensures resilience against the single point of failure, although it is complex to implement in dense networks. Both works aimed to address the security and privacy requirement.

In order to address energy consumption, Khazael *et al*. [30] proposed an architecture that integrates a publish-subscribe pattern with SDN for urban monitoring applications to address IoT energy consumption. The architecture supports Tesla complicated event definition language, QoS requirements, and improves distributed processing and complex event detection. Simulation results show improvements in data traffic and energy consumption compared to baseline methods. Meanwhile, Yang [17] introduced the wavelet neural network (WNN) model for network traffic estimation in smart transportation based on SDN. WNN integrates wavelet decomposition and artificial neural network (ANN) model to break down network traffic into components for training, with an optimization function to decrease estimation error. The proposed scheme has low estimation error but requires high CPU and storage usage.

Cao *et al*. [35] proposed a fog computing and SDN-based 5G internet of vehicles (IoV) architecture that guarantees QoS via an improved optimization algorithm. This modal considers service delay, task execution stability, energy consumption, and load balancing in the IoV environment. The experiment shows that the algorithm outperforms similar approaches, but its practical application is an open issue. On the other hand, Li *et al*. [36] introduced a three-layer hierarchy control framework for SDN-IoV based on mobile-edge computing (MEC) to minimize the delay between switches and controllers. A Louvain algorithm-based controller placement policy was proposed to optimize controller location, achieving better delay and load balance index than two baseline methods, but without considering energy consumption. Both mentioned works aimed to address QoS.

To address the task offloading, Lin *et al*. [43] proposed a grid-based model integrated with SDN to identify the traffic-congestion probability in a transportation network. The proposed model employs an algorithm that can be solved in polynomial time and utilises time-expanded network technology. This enables the model to identify the grids that impact the probability of traffic congestion and determine an optimal path that takes congestion into account. The simulation shows that the proposed model efficiently detects and predicts possible traffic congestion and can accurately determining an optimal routing path.

5. FUTURE RESEARCH DIRECTION

While the integration of SDIoT in smart cities has yielded numerous benefits, there are still several challenges and issues that need to be addressed to fully integrate SDN into IoT applications. This section focuses on identifying major challenges and discussing new ideas and guidelines that should be explored by the research community. By addressing these issues, we can pave the way for a more robust and efficient integration of SDN and IoT, further enhancing the capabilities of smart cities.

5.1. Interoperability

For any network architecture that involves managing the exchange of information between diverse IoT devices, platforms, and systems, interoperability is essential. Recently, the number of IoT solutions providers increased rapidly, each platform having its own preferred operating systems, architecture, programming language, and data structure. This dissimilarity is a challenge to create cross-platform and cross-domain IoT applications. For this reason, the SDIoT should provide interoperability at the platform level by providing some cross-platform functions. This cross-platform function will act as a bridge to integrate all IoT platforms available in the network.

5.2. Scalability

In any network architecture designed to support IoT ecosystems, scalability is a crucial factor. The system must be able to handle an increasing number of workloads from software, hardware, and networks while maintaining the QoS for each service. It is known that the number of connected things is increasing, which may interrupt existing services and causes network bottleneck due to the massive quantity of data generated. For this reason, SDIoT should guarantee scalability by applying some mechanisms such as load balancing and prioritizing types of service.

5.3. Low latency

Each IoT service has its requirement for low latency and high reliability. In an IoT ecosystem, limited network resources must be managed efficiently and assigned accordingly to multiple IoT services. The system must guarantee all IoT services are given the required network resources to function without interruption. For this reason, it is necessary to develop algorithms that optimize the usage of network resources and prioritize IoT services. These measures ensure that each IoT service can operate without interruption.

5.4. Handling of big data

In an IoT environment, the amount of data collected from real-time sensors is huge. This massive amount of data has to be managed efficiently in terms of processing and data storage. Obtaining sufficient and high-quality data are crucial to ensure the accuracy of the later stage of data processing and analytic operations. For this reason, future works must address resolving unnecessary data, such as duplication and redundancy to optimize the storage usage in SDIoT.

5.5. Security and privacy

Security is a crucial concern in SDIoT due to the complexity of its architecture. The involvement of multiple users, IoT devices, and data in the network creates potential security vulnerabilities that must be addressed. To ensure communication security, various mechanisms such as cryptography, hash functions, and blockchain can be deployed using a hierarchical structure. These measures help to mitigate the risks of potential security breaches.

5.6. Energy consumption

The complexity of SDIoT, with its multiple layers and distributed systems, comes with a significant energy consumption and increased costs. To overcome this challenge, future work should focus on developing new protocols or optimizing existing ones that prioritize energy efficiency without sacrificing the performance of IoT services. By addressing this issue, we can minimize the environmental impact of SDIoT deployments and make them more economically viable in the long run.

5.7. Quality of service

QoS is an important network aspect that guarantees its capability to run high-priority IoT applications. By prioritizing the transmission of data types, QoS regulates network resources to meet the needs of numerous data transmissions. To ensure an acceptable level of QoS for high-priority IoT applications, QoS approaches such as traffic classification and traffic shaping must exist at every layer of the SDIoT architecture.

5.8. Task offloading

Task offloading plays a crucial role in enhancing system performance and conserving local resources by transferring computational tasks from IoT devices to SDIoT infrastructure. To ensure successful offloading, it is imperative to carefully evaluate and consider factors like network connectivity, resource availability, and time constraints associated with each task. By taking these aspects into account, efficient task offloading strategies can be developed, enabling optimal utilization of resources and maximizing the overall performance of SDIoT systems.

6. CONCLUSION

As the number of data generated and IoT devices in smart cities continues to grow, both pose significant challenges for network resource management, data processing, storage, and analysis, which can affect the overall efficiency and effectiveness of the smart city ecosystem. However, SDN presents a promising solution to mitigate these problems. By enabling centralized network management, SDN can help to optimize network resources, enhance network scalability and flexibility, and improve data security and privacy in smart cities. With SDIoT, smart cities can overcome the challenges of growing data size and IoT devices to build more efficient and sustainable urban environments.

This paper presents a review of SDIoT for IoT applications in smart cities. The study focuses on the SDIoT implementation to address challenges in IoT applications related to interoperability, scalability, latency, big data handling, security and privacy, energy consumption, QoS, and task offloading. In addition, this paper finally highlights open research challenges and future research directions for SDIoT in smart city.

ACKNOWLEDGEMENTS

This work was supported by Universiti Malaysia Pahang Al-Sultan Abdullah, under the Postgraduate Research Grant Scheme (PGRS 230396).

REFERENCES

[1] M. Chui, M. Collins, and M. Patel, *The internet of things: catching up to an accelerating opportunity*, McKinsey & Company, Nov. 2021.
[2] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jun. 2019, doi: 10.1007/s11036-018-1089-9.
[3] A. Cimmino, M. Poveda-Villalón, and R. García-Castro, "EWOT: a semantic interoperability approach for heterogeneous IoT ecosystems based on the web of things," *Sensors (Switzerland)*, vol. 20, no. 3, p. 822, Feb. 2020, doi: 10.3390/s20030822.
[4] L. Tu, S. Liu, Y. Wang, C. Zhang, and P. Li, "An optimized cluster storage method for real-time big data in internet of things," *Journal of Supercomputing*, vol. 76, no. 7, pp. 5175–5191, Jul. 2020, doi: 10.1007/s11227-019-02773-1.
[5] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: challenges and findings," *Future Internet*, vol. 12, no. 3, p. 55, Mar. 2020, doi: 10.3390/fi12030055.
[6] V. Balasubramanian, M. Aloqaily, M. Reisslein, and A. Scaglione, "Intelligent resource management at the edge for ubiquitous IoT: An SDN-based federated learning approach," *IEEE Network*, vol. 35, no. 5, pp. 114–121, Sep. 2021, doi: 10.1109/MNET.011.2100121.
[7] B. Preveze, A. Alkhayyat, F. Abedi, A. M. Jawad, and A. S. Abosinnee, "SDN-driven internet of health things: a novel adaptive switching technique for hospital healthcare monitoring system," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–11, Jun. 2022, doi: 10.1155/2022/3150756.
[8] S. Shukla, M. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan, and M. K. Khan, "Improving latency in internet-of-things and cloud computing for real-time data transmission: a systematic literature review (SLR)," *Cluster Computing*, Apr. 2021, doi: 10.1007/s10586-021-03279-3.
[9] "ITU-T Y.2060 - overview of the internet of things," *Series Y: Global information infrastructure, internet protocol aspects and next-generation networks - Frameworks and functional architecture models*, International Telecommunication Union, 2012.
[10] E. Lee, Y. D. Seo, S. R. Oh, and Y. G. Kim, "A survey on standards for interoperability and security in the internet of things," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 2, pp. 1020–1047, 2021, doi: 10.1109/COMST.2021.3067354.
[11] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," *Internet of Things (Netherlands)*, vol. 20, p. 100626, Nov. 2022, doi: 10.1016/j.iot.2022.100626.

[12] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: a comprehensive survey," *Journal of Network and Computer Applications*, vol. 159, p. 102595, Jun. 2020, doi: 10.1016/j.jnca.2020.102595.
[13] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *Journal of Network and Computer Applications*, vol. 156, p. 102563, Apr. 2020, doi: 10.1016/j.jnca.2020.102563.
[14] K. Nisar *et al.*, "A survey on the architecture, application, and security of software defined networking: challenges and open issues," *Internet of Things*, vol. 12, p. 100289, Dec. 2020, doi: 10.1016/j.iot.2020.100289.
[15] G. Lakhani and A. Kothari, "Fault administration by load balancing in distributed SDN controller: a review," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3507–3539, 2020, doi: 10.1007/s11277-020-07545-2.
[16] B. Almadani, A. Beg, and A. Mahmoud, "DSF: a distributed SDN control plane framework for the east/west interface," *IEEE Access*, vol. 9, pp. 26735–26754, 2021, doi: 10.1109/ACCESS.2021.3057690.
[17] Y. Yang, "A SDN-based traffic estimation approach in the internet of vehicles," *Wireless Networks*, Jul. 2021, doi: 10.1007/s11276-021-02668-1.
[18] P. P. Ray and N. Kumar, "SDN/NFV architectures for edge-cloud oriented IoT: a systematic review," *Computer Communications*, vol. 169, pp. 129–153, Mar. 2021, doi: 10.1016/j.comcom.2021.01.018.
[19] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, "A fog computing model for VANET to reduce latency and delay using 5G network in smart city transportation," *Applied Sciences (Switzerland)*, vol. 12, no. 4, 2022, doi: 10.3390/app12042083.
[20] D. Z. Fawwaz, S. H. Chung, C. W. Ahn, and W. S. Kim, "Optimal distributed MQTT broker and services placement for SDN-edge based smart city architecture," *Sensors*, vol. 22, no. 9, p. 3431, Apr. 2022, doi: 10.3390/s22093431.
[21] A. Montazerolghaem, "Software-defined load-balanced data center: design, implementation and performance analysis," *Cluster Computing*, vol. 24, no. 2, pp. 591–610, Jun. 2021, doi: 10.1007/s10586-020-03134-x.
[22] F. Alassery, "High performance priority packets scheduling mechanism for big data in smart cities," *Computers, Materials and Continua*, vol. 72, no. 1, pp. 535–559, 2022, doi: 10.32604/cmc.2022.023558.
[23] B. Sellami, A. Hakiri, S. B. Yahia, and P. Berthou, "Energy-aware task scheduling and offloading using deep reinforcement learning in SDN-enabled IoT network," *Computer Networks*, vol. 210, p. 108957, Jun. 2022, doi: 10.1016/j.comnet.2022.108957.
[24] C. Lin *et al.*, "Mobile-edge computing-based delay minimization controller placement in SDN-IoV," *Computer Networks*, vol. 27, no. 4, pp. 3832–3840, 2021, doi: 10.1109/TGCN.2022.3162237.
[25] N. Chen and Y. Chen, "Anomalous vehicle recognition in smart urban traffic monitoring as an edge service†," *Future Internet*, vol. 14, no. 2, 2022, doi: 10.3390/fi14020054.
[26] N. Kumar, S. Mittal, V. Garg, and N. Kumar, "Deep reinforcement learning-based traffic light scheduling framework for SDN-enabled smart transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2411–2421, 2022, doi: 10.1109/TITS.2021.3095161.
[27] H. Babbar, S. Rani, A. K. Bashir, and R. Nawaz, "LBSMT: load balancing switch migration algorithm for cooperative communication intelligent transportation systems," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1386–1395, 2022, doi: 10.1109/TGCN.2022.3162237.
[28] S. K. Keshari, V. Kansal, and S. Kumar, "A systematic review of quality of services (QoS) in software defined networking (SDN)," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2593–2614, 2021, doi: 10.1007/s11277-020-07812-2.
[29] H. Babbar, S. Rani, D. Gupta, H. M. Aljahdali, A. Singh, and F. Al-Turjman, "Load balancing algorithm on the immense scale of internet of things in sdn for smart cities," *Sustainability (Switzerland)*, vol. 13, no. 17, 2021, doi: 10.3390/su13179587.
[30] B. Khazael, H. T. Malazi, and S. Clarke, "Complex event processing in smart city monitoring applications," *IEEE Access*, vol. 9, pp. 143150–143165, 2021, doi: 10.1109/ACCESS.2021.3119975.
[31] Z. Eghbali and M. Z. Lighvan, "A hierarchical approach for accelerating IoT data management process based on SDN principles," *MENDEL*, vol. 25, no. 1, pp. 121–130, Jun. 2019, doi: 10.13164/mendel.2019.1.121.
[32] Z. Lv, D. Chen, R. Lou, and Q. Wang, "Intelligent edge computing based on machine learning for smart city," *Future Generation Computer Systems*, vol. 115, pp. 90–99, Feb. 2021, doi: 10.1016/j.future.2020.08.037.
[33] R. Ke, Y. Zhuang, Z. Pu, and Y. Wang, "A smart, efficient, and reliable parking surveillance system with edge artificial intelligence on IoT devices," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 4962–4974, Aug. 2021, doi: 10.1109/TITS.2020.2984197.
[34] M. Peyman, P. J. Copado, R. D. Tordecilla, L. D. C. Martins, F. Xhafa, and A. A. Juan, "Edge computing and iot analytics for agile optimization in intelligent transportation systems," *Energies*, vol. 14, no. 19, 2021, doi: 10.3390/en14196309.
[35] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3832–3840, Jun. 2021, doi: 10.1109/TITS.2020.3048844.
[36] B. Li, X. Deng, and Y. Deng, "Mobile-edge computing-based delay minimization controller placement in SDN-IoV," *Computer Networks*, vol. 193, p. 108049, Jul. 2021, doi: 10.1016/j.comnet.2021.108049.
[37] F. S. D. Silva, E. Silva, E. P. Neto, M. Lemos, A. J. V. Neto, and F. Esposito, "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," *Sensors (Switzerland)*, vol. 20, no. 11, p. 3078, May 2020, doi: 10.3390/s20113078.
[38] L. El-Garoui, S. Pierre, and S. Chamberland, "A new sdn-based routing protocol for improving delay in smart city environments," *Smart Cities*, vol. 3, no. 3, pp. 1004–1021, Sep. 2020, doi: 10.3390/smartcities3030050.
[39] X. Xu, Q. Huang, X. Yin, M. Abbasi, M. R. Khosravi, and L. Qi, "Intelligent offloading for collaborative smart city services in edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7919–7927, Sep. 2020, doi: 10.1109/JIOT.2020.3000871.
[40] C. Zhang, "Design and application of fog computing and internet of things service platform for smart city," *Future Generation Computer Systems*, vol. 112, pp. 630–640, Nov. 2020, doi: 10.1016/j.future.2020.06.016.
[41] M. Gheisari, G. Wang, and S. Chen, "An edge computing-enhanced internet of things framework for privacy-preserving in smart city," *Computers and Electrical Engineering*, vol. 81, p. 106504, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106504.
[42] A. M. Alsmadi *et al.*, "An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT)," *Future Generation Computer Systems*, vol. 33, no. 2, pp. 243–253, 2020, doi: 10.1016/j.future.2018.05.054.
[43] C. Lin, G. Han, J. Du, T. Xu, L. Shu, and Z. Lv, "Spatiotemporal congestion-aware path planning toward intelligent transportation systems in software-defined smart city IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8012–8024, Sep. 2020, doi: 10.1109/JIOT.2020.2994963.
[44] C. Lin, G. Han, X. Qi, M. Guizani, and L. Shu, "A distributed mobile fog computing scheme for mobile delay-sensitive applications in SDN-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5481–5493, May 2020, doi: 10.1109/TVT.2020.2980934.
[45] H. Guo, J. Liu, J. Ren, and Y. Zhang, "Intelligent task offloading in vehicular edge computing networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 126–132, Aug. 2020, doi: 10.1109/MWC.001.1900489.

[46] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent edge computing for IoT-based energy management in smart cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, 2019, doi: 10.1109/MNET.2019.1800254.

[47] A. Rego, L. Garcia, S. Sendra, and J. Lloret, "Software defined network-based control system for an efficient traffic management for emergency situations in smart cities," *Future Generation Computer Systems*, vol. 88, pp. 243–253, Nov. 2018, doi: 10.1016/j.future.2018.05.054.

[48] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "BEST: blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Computers & Security*, vol. 85, pp. 288–299, Aug. 2019, doi: 10.1016/j.cose.2019.05.006.

[49] C. Campolo, G. Genovese, G. Singh, and A. Molinaro, "Scalable and interoperable edge-based federated learning in IoT contexts," *Computer Networks*, vol. 223, p. 109576, Mar. 2023, doi: 10.1016/j.comnet.2023.109576.

[50] R. Saha, N. Ahmed, and S. Misra, "SDN-controller triggered dynamic decision control mechanism for healthcare IoT," in *2021 IEEE Global Communications Conference, GLOBECOM 2021 - Proceedings*, Dec. 2021, pp. 1–6, doi: 10.1109/GLOBECOM46510.2021.9685911.

BIOGRAPHIES OF AUTHORS

Imran Edzereiq Kamarudin received his B.Sc. degree in Data Communications and Networking and Master of Computer Science (Computer Network) from the Universiti Teknologi Mara, Malaysia. He is currently pursuing his Ph.D. from the Universiti Malaysia Pahang, Malaysia. His area of research includes the internet of things (IoT) and software defined networking (SDN). He can be contacted at email: edzereiq@ump.edu.my.

Mohamed Ariff Ameedeen obtained his Ph.D. in Computer Science from the University of Birmingham, United Kingdom, in 2014. He is currently serving as the Chief Information Officer (CIO) of Universiti Malaysia Pahang, a public university in Malaysia, and an Associate Professor in the Faculty of Computing. His research interests include cloud computing, artificial intelligence, blockchain, and model-driven development. He can be contacted at email: mohamedariff@ump.edu.my.

Mohd Faizal Ab Razak obtained his Ph.D. in Information Security from Universiti Malaya in 2018 and Master of Computer Science from the University of Malaysia Pahang, Malaysia, in 2013. He has published several conference and journal papers locally and internationally. His research interests include information security (intrusion detection and prevention systems), risk assessment, artificial intelligence, and library information systems. He can be contacted at email: faizalrazak@ump.edu.my.

Azlee Zabidi obtained his Ph.D. in Electrical Engineering from the Universiti Teknologi MARA (UiTM) in 2018. He is a senior lecturer at the Universiti Malaysia Pahang (UMP). His research interests include digital signal processing, optimization algorithm, and IoT with analytic and artificial intelligence. He can be contacted at email: azlee@ump.edu.my.