A survey on the applications of SDN-based IoT Network

Conference Paper · November 2023

DOI: 10.1109/ICI60088.2023.10420869

4 authors, including:

Ngangbam Indrason
VIT-AP University
6 PUBLICATIONS **39** CITATIONS

SEE PROFILE

A survey on the applications of SDN-based IoT Network

Ngangbam Indrason
Dept of Information Technology
North-Eastern Hill University
Shillong, Meghalaya, India
indrasonkangla@gmail.com

Mainkordor Mawblei
Dept of Electronics and Communication Engineering
North-Eastern Hill University
Shillong, Meghalaya, India
mainkordormawblei@gmail.com

Khiakupar Jyndiang
Dept of Electronics and Communication Engineering
North-Eastern Hill University
Shillong, Meghalaya, India
kuparjynd@gmail.com

Amardeep Kumar Thakur
Dept of Electronics and Communication Engineering
North-Eastern Hill University
Shillong, Meghalaya, India
amardeep.kr.thakur@gmail.com

2023 Second International Conference on Informatics (ICI) | 979-8-3503-4383-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICI60088.2023.10420869

***Abstract*— With the rapid advancement of technology, we depend on technology for our comfort and convenience. One such advancing technology is the Internet of Things (IoT), a multi-dimensional technology. IoT can be applied in numerous domains, enhancing our everyday experiences, but it is hindered by energy and resource limitations. Additionally, Software-Defined Networking (SDN) emerges as a complementary technology that can be incorporated into IoT for better network functioning. SDN can make an IoT network more secure, reliable, scalable and ensures optimal performance. In this paper, we have explored the diverse applications of SDN-based IoT networks. SDN enhances the flexibility of IoT networks and provides substantial benefits to mitigate possible network attacks effectively. Furthermore, the performance and security of such networks can further be improved by incorporating other advancing technologies, such as Network Function Virtualization (NFV), Black SDN, and Artificial Intelligence (AI). We can achieve the full potential of SDN-based IoT networks and further expand our technological society by adopting these cutting-edge technologies.**

Keywords*— *Internet of Things (IoT), Software Defined Networks (SDN), Smart devices

I. INTRODUCTION

In this present technological world, we rely on technology to ease our survival. For instance, we use mobile phones to connect with people across long distances, stay updated on global events, and access information swiftly through the internet in a very short time. This advancement significantly enhanced the quality of our life. As a part of this growth, we embrace the numerous advantages of the Internet of Things, such as effortlessly gathering data from remote locations, monitoring and controlling devices wirelessly. Some of the wireless networks include wireless sensor networks (WSN), Wifi, mobile ad-hoc networks (MANET), Bluetooth, ZigBee, and RFID [1]. The advancement of IoT continues to shape the way we interact with various technology, making our lives more interconnected, efficient, and productive. IoT has started implementing in multiple domains, improving the network. With the development of Software Defined Network, IoT network is improved and provides better security.

The main contributions of this paper are as follows:

- To point out the various applications of software-defined networks in the Internet of Things network carried out by various researchers.
- To lay down the future directions for further strengthening the security of the network.

This paper is organized as follows. Section II discussed about the Internet of Things, Software Defined Networks, and the importance of SDN in IoT. Further, the various applications of SDN-based IoT Networks are pointed out in Section III. Section IV discusses the applications and possible future directions, and Section V concludes the paper.

II. BACKGROUND

A. Internet of Things

The Internet of Things which is popularly known as IoT, is the interconnection of various devices through the internet. These devices are generally low-powered, low-resource, and can only perform light operations rather than processing massive computations. In this today's world, the popularity of IoT is so great in such a way that IoT is incorporated into most of the day-to-day tasks, making our life easier. IoT devices include temperature sensors, humidity sensors, light sensors, and many more.

Fig. 1. shows the architecture of the Internet of Things. It consists of three primary layers, namely Perception Layer, Network Layer, and Application Layer. The perception layer consists of sensors and actuators to collect or sense data from the environment and send it to the application layer for processing the data through the network layer. Moreover, it also acts on the environment or the subject according to the sensor's data. The responsibility of the network layer is to route the data from different layers of the architecture. It handles the to-and-fro movement of the data ensuring the data to reach the desired destination. It consists of gateways and the internet for the connection. The application layer is the control centre where all the data received from the sensors are processed and provide commands to the actuators. According to the signal from the application layer, actuators will respond correspondingly.

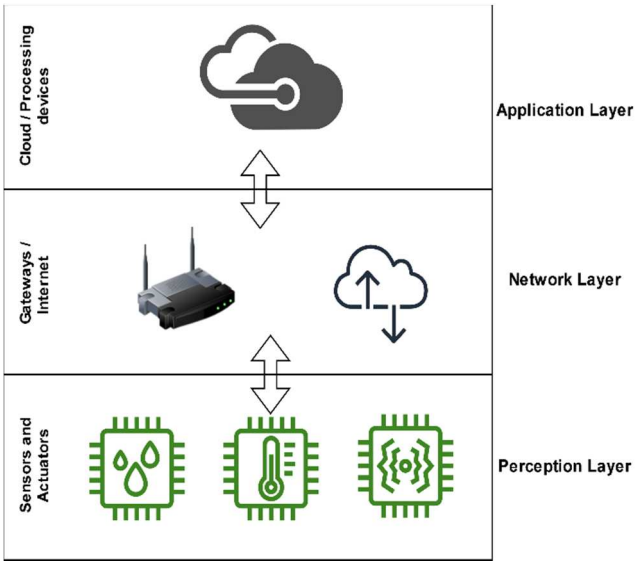

Fig. 1. Architecture of IoT

B. *Software Defined Network*

A Software Defined Network is an advanced form of networking where there is a software-based controller that controls the flow of data from one device to another. It is commonly known as SDN. SDN decouples the data plane and control plane in a networking model, making it simpler to handle or trace any data flow in the network. It has the ability to provide routes of various data generated by multiple devices according to the requirements.

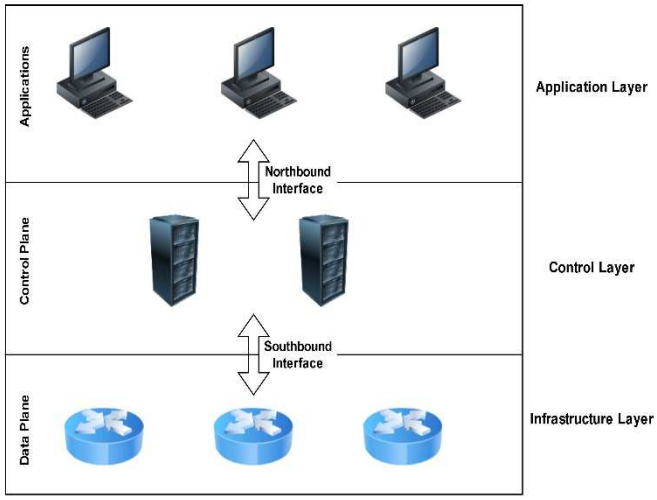

Fig. 2. Architecture of SDN

Fig. 2. represents the architecture of Software Defined Network. It has three layers which are the Infrastructure layer, the Control layer and the Application layer. The infrastructure layer contains switches which are responsible for generating data and sending it to the network. It is also known as the data plane. The transmission of data from the data plane is handled by OpenFlow switches. Next is the control layer, which consists of a controller controlling the data flow. It sets the route of the data generated from the infrastructure layer. According to the assigned path, the data flows and communicate with the application layer. To communicate between the control layer and infrastructure layer, the southbound interface is used, and that of the control layer and application layer is the northbound interface. These planes consist of various protocols such as RESTCONF, NETCONF, OVSDB, SNMP and BGP-LS [2].

C. *Importance of SDN in IoT*

IoT network is prone to attacks for being low-resource devices. It is unable to apply high computational operations to prevent from various attacks. To mitigate such problems, SDN comes into the picture [3]. SDN plays a vital role in shaping the IoT network to provide security, accessibility, scalability, heterogeneity, reliability [4] and more control over the network. It also supports the conventional IoT network by allowing the expansion and updating of the network along with the restructuring of the network for better benefits.

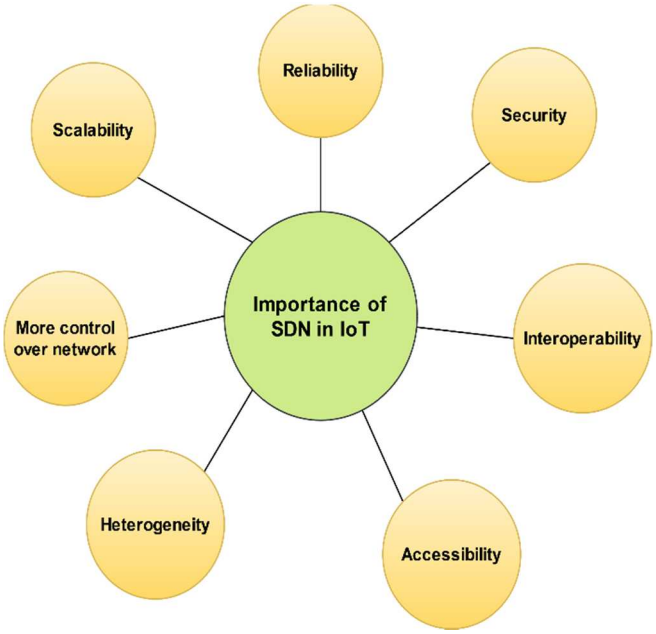

Fig. 3. Importance of SDN in IoT

III. Applications of SDN-based IoT Network

The list of domains where SDN-based IoT Networks are applied is discussed below. Some of the applications that many researchers have applied are healthcare, smart home, smart city, voting system, smart grids, and connected vehicles. It is also shown in Fig. 4.

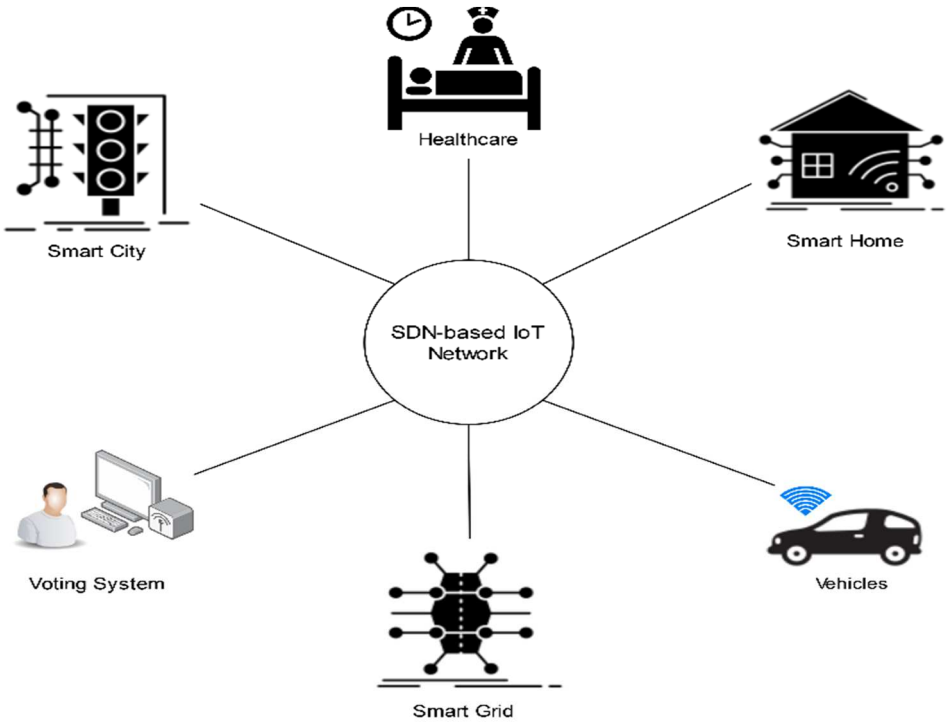

Fig. 4. Various applications of SDN-based IoT Network

A. Healthcare

Healthcare plays a pivotal role in safeguarding the well-being and quality of life of individuals across the globe. Proper healthcare is essential for ensuring not only our physical well-being but also our mental peace and overall quality of life. To take part in networking advancement, IoT can also apply in healthcare. When we apply IoT in healthcare, it is known as the Internet of Healthcare Things (IoHT) [5]. The application of IoT in healthcare provides various advantages, such as monitoring patients remotely using fitness trackers, sensors/actuators, and providing suggestions without waiting for the doctors. Moreover, the doctor will also get notified instantly when any abnormality is observed in the patient. Some of the IoHT devices are glucose monitoring, heart-rate monitoring, Parkinson's disease monitoring, connected inhalers, and ingestible sensors.

The incorporation of SDN can improve the applicability of IoHT, and this integration can be found in [6] [7] [8]. The use of SDN enables the interconnection of multiple heterogeneous devices to operate efficiently. The authors of [8] proposed health-flow to increase the efficiency of the healthcare network. A precise health-related notification is provided to the user using a machine learning-based SDN controller. [7] uses a cloud-based SDN controller and also ensures trustable reports to the users.

B. Smart Home

A home with connected devices, automation technology, enabling remote control, and monitoring of various aspects within the home is called a smart home. Various IoT devices are involved and controlled centrally or smartphone apps to manage appliances such as security cameras, thermostats, lighting systems, and other connected appliances [9]. It provides easy control of all the appliances, automate tasks, a secure environment, and instant report for any failed devices.

A vertical SDN-based multi-layered architecture is proposed for better controlling of the smart home [10]. It consists of two controllers acting as a parent-child connection. The primary SDN Controller (PSC) acts as the parent controller residing in the cloud to detect security risks and flaws. The local SDN Controller (LSC) lies in the local smart home network maintaining local smart service systems. The authors used API for easier access to the current services. Various topologies are compared such as local topologies and cloud topologies and cloud-local topologies for its performance analysis. The topologies are implemented using Mininet, POX, NOX, and Floodlight controllers for the experimentation. It is found that the cloud-local topologies have lower packet loss than the other topologies. Future work lies in integrating artificial intelligence (AI) tools to impart better error detection capabilities and provide necessary solutions accordingly.

P K Sharma et al. [11] proposed SHSec, an innovative SDN-based security for smart home. It can effectively detect and mitigate a wide range of attacks in smart home including eavesdropping and nefarious activity. It also offers a user-friendly and improved heterogeneous local network. The proposed architecture focuses on preserving user privacy, prevents communication delays and security breaches in home voice assistants. Through comprehensive testing, SHSec achieves 89% accuracy and 91% sensitivity rates ensuring the security and privacy aspects of smart home environments.

C. Smart City

The use of technologies such as IoT in a city to collect data for analysis to make our life better, more efficient and more advanced is smart city. The main objective for this domain is to improve governance, better connectivity among the citizens and social well-being. IoT in smart city provides real-time data about the happenings in the city such as traffic flow and surveillance cameras [12]. These data help in better decision-

making processes to bring forth resource optimization, public safety, and citizen engagement. IoT devices used in the smart city includes smart sensors to monitor the environmental conditions, smart streetlight to maintain the light intensity according to the situation, and video surveillance cameras for public safety.

We have seen some researchers who worked in the integration of SDN and IoT in smart city. [13] proposed an SDN-IoT-based Smart City framework to handle the increasing number of devices for proper communication and mitigate any errors. In addition to this, a distributed addressing scheme is also proposed to assign dynamically unique IPv6 addresses to each device in the network. This scheme provides higher uniqueness, low addressing latency and addressing overhead, scalability, and lower complexity.

The authors [14] proposed distributed Black SDN-IoT architecture incorporated with NFV (Network Function Virtualization) for smart city. It improves availability, privacy, authentication, integrity, confidentiality, energy saving and load balancing.

B K Mukherjee et al. [15] utilize the advantages of NFV in the SDN-IoT network of smart city to improve the throughput and delay. Multiple distributed controllers are also used in a distributed manner to enhance load balancing, scalability, and security. The proposed model is simulated using Mininet-Wifi and Wireshark.

A new routing protocol is proposed using a supervised machine learning algorithm called the Naive Bayes algorithm. This algorithm is based on SDN to improve delay in the network. [16]. For designing and developing the protocol, the authors used the RYU SDN controller.

D. Voting System

One of the most undeniable tasks of a democratic citizen is voting. Every citizen has a right to cast a vote to elect a competent candidate for the betterment of the society. To carry out this operation, various methods are used such as paper ballot, postal ballot, e-voting system, EVM based booth-voting system [17]. This voting process should be transparent, accurate, and proper security measures should be taken place.

An SDN and IoT voting system is proposed to prevent proxy voting, vote manipulation, multiple votes, and forced votes [18]. In this proposed architecture, voting booths are considered as IoT devices where votes are collected. These devices are controlled by the SDN controller to prevent misuse of the voting booth. Besides, any foreign devices trying to connect to the voting network are detected by the SDN controller and discard the request from the foreign/unknown devices. The SDN controller can also detect any affected voting devices by analyzing the activities of the voting devices. In this way, SDN can prevent potential attacks in the IoT-based voting system.

E. Smart Grid

A smart grid is an advanced form of the traditional electric grid which involves the incorporation of digital technologies, communication systems, and intelligent devices. It is a part of the advancement of the Industrial Internet of Things (IIoT) [19]. This involvement enhances the efficiency, reliability, and sustainability of electricity generation, transmission, distribution, and consumption. IoT-based smart grid comprises of smart meters, sensors, and actuators to collect voltage and current information, data management system, grid management, and control systems.

A real-time monitoring technique is proposed using SDN based on IIoT to recover failures in smart grid [20]. It has the ability to monitor natural disasters, electric outages and fault events. During any failure, it can send grid control commands through a dynamic route.

P R Grammatikis et al. [21] presented the SDN-microSENSE architecture to increase the resiliency of smart grid along with the improvement in risk assessment, intrusion detection and correlation, and self-healing. SDN can even prevent potential cyberattacks and anomalies.

F. Vehicles

The interconnection of vehicles, communication systems to exchange information to improve transportation systems and safety is called the Internet of Vehicles (IoV) [22]. In other words, IoV is the combination of the vehicular ad-hoc network (VANET) and IoT. IoV connects vehicles with one another through a variety of technologies, including IoT, wireless communication, and intelligent transportation systems. This incorporation of technologies enhances the overall driving experience. IoV consists of various types of communications such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C), Vehicle-to-Network (V2N) and Vehicle-to-Everything (V2X) Communications [23][24]. This network provides a list of benefits: efficient traffic management, enhanced driver experience, intelligent fleet management, and making the transport system safer, more efficient and connected.

The integration of NFV and SDN in IoV improves performance, provides better Quality-of-Service (QoS) and customization [25]. A few applications of IoV are vehicle collision warning, autonomous driving, virtual reality and augmented reality. This integration improves latency, reliability, and ubiquitous and efficient connections.

L Alouache et al. [26] proposed a routing protocol for the V2V communication using SDN to maintain connectivity during the mobility of the vehicles. It provides reliability, availability, connectivity, cost-effectiveness and reduces end-to-end delay.

IV. Discussion

The application of the Internet of Things is very vast. It can be applied across numerous domains, offering significant advantages. Since IoT devices are typically low-resource so they can seamlessly integrate into diverse networks and get updated with real-time data. Traditional IoT networks often face challenges such as susceptibility to attacks and limited scalability, so SDN plays a significant role in handling the mentioned issues. SDN enhances scalability, reliability, control, and security within the network infrastructure, ensuring efficient and secure communication. SDN-based IoT networks have far-reaching implications across various domains, including healthcare, smart homes, smart cities, voting systems, smart grids, and connected vehicles.

The summary of various applications of SDN-based IoT network is shown in Table 1.

TABLE 1

Summary of various applications of SDN-based IoT Network

Paper	Application	Contribution
[7]	Healthcare	Uses a cloud-based SDN controller to ensure trustable reports to the users.
[8]	Healthcare	Proposed health-flow to increase the efficiency of the healthcare network.
[10]	Smart Home	Proposed a vertical SDN-based multi-layered architecture to control the smart home efficiently.
[11]	Smart Home	Proposed SHSec to mitigate attacks like eavesdropping and nefarious activity effectively.
[13]	Smart City	Proposed a framework to handle the devices to communicate and mitigate any errors.
[14]	Smart City	Proposed a distributed Black SDN-IoT architecture to improve the functioning of smart city.
[15]	Smart City	Uses NFV in SDN-IoT Network to improve throughput and delay.
[16]	Smart City	Proposed a new routing protocol using a supervised machine learning algorithm to improve delay in the network
[18]	Voting System	Prevents proxy voting, vote manipulation, multiple votes, and forced votes.
[20]	Smart Grid	Proposed a real-time monitoring technique to recover failures in the smart grid.
[21]	Smart Grid	Increased the resiliency of the smart grid by presenting SDN-microSENSE architecture.
[25]	Vehicles	IoV improves its performance, such as latency, reliability by integrating NFV and SDN.
[26]	Vehicles	Proposed a routing protocol to maintain connectivity during the mobility of the vehicles.

We have found that most of the researchers have worked significantly in the smart city domain, while the voting system field has seen comparatively less progress. By leveraging the benefits of SDN, various IoT-based applications can also be improved in various sectors, including agriculture and parking systems. However, one of the significant security challenges of the SDN-based IoT network is device authentication. As multiple devices are working together to carry out a specific task, proper authentication is required. Without robust authentication mechanisms, the network may lead to data leakage, data theft, unauthorized access and vulnerable to the system.

V. Conclusion

In this paper, we have explored the diverse domains which are benefitted from SDN-based IoT networks. We have also discussed about the various benefits that have received from the hybridization of SDN in IoT in various domains. Moreover, this paper pointed out any necessary enhancements essential for optimizing network performance. It is found that the integration of Network Function Virtualization (NFV) and SDN significantly boosts the performance of IoT-based networks. NFV separates network functionality from the hardware devices [2]. NFV can support SDN by virtualizing the SDN controller. Furthermore, the utilization of Black SDN exhibits better potential to tackle various security issues in the network. To further improve network management and security, a proper device authentication mechanism is essential to prevent from any possible threats. Besides, Artificial Intelligence (AI) can also play a critical role in mitigating any attacks and provide a possible response to minimize the mutilation in the network. By harnessing the power of these technologies, we can realize a future where interconnected systems, data-driven decision-making, and enhanced efficiency shape our daily lives for a better lifestyle.

References

[1] N. Khandelwal and S. Gupta, "A Review: Trust based Secure IoT Architecture in Mobile Ad-hoc Network," *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC).* IEEE, pp. 1464–1472, 2022.

[2] 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, 2020.

[3] A. A. Abdulsamad and T. A. Salih, "IoT security improvement based on SDN Controller," *Eurasian Journal of Engineering and Technology*, vol. 14, pp. 49–56, 2023

[4] P. Thorat, S. Singh, A. Bhat, V. Lakshmi Narasimhan, and G. Jain, "SDN-enabled IoT: ensuring reliability in IoT networks through software defined networks", *Towards Cognitive IoT Networks*, Springer, pp. 33-53, 2020.

[5] M. Mamdouh, A. I. Awad, A. A. Khalaf, and H. F. Hamed, "Authentication and identity management of IoHT devices: achievements, challenges, and future directions," *Computers & Security*, vol. 111, p. 102491, 2021.

[6] S. Badotra, D. Nagpal, S. N. Panda, S. Tanwar, and S. Bajaj, "IoT-enabled healthcare network with SDN," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO).* IEEE, pp. 38–42, 2020.

[7] A. Srilakshmi, P. Mohanapriya, D. Harini, and K. Geetha, "Iot based smart health care system to prevent security attacks in sdn," *2019 Fifth International Conference on Electrical Energy Systems (ICEES).* IEEE, pp. 1–7, 2019.

[8] S. Misra, R. Saha, and N. Ahmed, "Health-flow: Criticality-aware flow control for sdn-based healthcare iot," *GLOBECOM 2020-2020 IEEE Global Communications Conference.* IEEE, pp. 1–6, 2020.

[9] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Symposium on Usable Privacy andSecurity (SOUPS)*, vol. 220, 2017.

[10] S. M. M. Gilani, M. Usman, S. Daud, A. Kabir, Q. Nawaz, and O. Judit, "SDN-based multi-level framework for smart home services," *Multimedia Tools and Applications*, pp. 1–21, 2023.

[11] P. K. Sharma, J. H. Park, Y.-S. Jeong, and J. H. Park, "Shsec: sdn based secure smart home network architecture for internet of things," *Mobile Networks and Applications*, vol. 24, pp. 913–924, 2019.

[12] P. Bellini, P. Nesi, and G. Pantaleo, "IoT-enabled smart cities: A review of concepts, frameworks and key technologies." *Applied Sciences*, vol. 12, no. 3, p. 1607, 2022.

[13] U. Ghosh, P. Chatterjee, S. Shetty, and R. Datta, "An SDN-IoT-based framework for future smart cities: Addressing perspective," *Internet of Things and secure smart environments: successes and pitfalls*, pp. 441–468, 2020.

[14] M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, "Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities," *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, pp. 1–6, 2019.

[15] B. K. Mukherjee, S. I. Pappu, M. J. Islam, and U. K. Acharjee, "An SDN based distributed IoT network with NFV implementation for smart cities," *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*. Springer, pp. 539–552, 2020.

[16] 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, 2020.

[17] N. Indrason, W. Khongbuh, and G. Saha, "Blockchain-based boothless e-voting system," *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 1*. Springer, pp. 779–788, 2021.

[18] N. Indrason, F. H. Pohrmen, S. Z. Marshoodulla, and G. Saha, "Blockchain and SDN-IoT based secured voting system," *2023 4th International Conference on Computing and Communication Systems (I3CS)*. IEEE, pp. 1–6, 2023.

[19] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," *Computers in industry*,vol. 101, pp. 1–12, 2018.

[20] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial internet of things driven by SDN platform for smart grid resiliency," *IEEE Internetof Things Journal*, vol. 6, no. 1, pp. 267–277, 2017.

[21] P. R. Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz, and A. Sarigiannidis, "Sdn-based resilient smart grid: The sdn-microsense architecture," *Digital*, vol. 1, no. 4, pp. 173–187, 2021.

[22] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 2014.

[23] X. Wang, S. Mao, and M. X. Gong, "An overview of 3gpp cellular vehicle-to-everything standards," *GetMobile: Mobile Computing and Communications*, vol. 21, no. 3, pp. 19–25, 2017.

[24] A. Hakimi, K. M. Yusof, M. A. Azizan, M. A. A. Azman, and S. M. Hussain, "A survey on internet of vehicle (iov): A pplications & comparison of vanets, iov and sdn-iov," *ELEKTRIKA-Journal of Electrical Engineering*, vol. 20, no. 3, pp. 26–31, 2021.

[25] W. Zhuang, Q. Ye, F. Lyu, N. Cheng, and J. Ren, "SDN/NFV-empowered future IoV with enhanced communication, computing, and caching," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 274–291, 2019.

[26] L. Alouache, N. Nguyen, M. Aliouat, and R. Chelouah, "Toward a hybrid SDN architecture for V2V communication in IoV environment." *2018 fifth international conference on software defined systems (SDS)*. IEEE, pp. 93-99, 2018.