IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Analysis of SDN-Orchestrated Solutions for Heterogeneous IoT in 6G Networks

Surekha Lanka[1], Shuvra Tripura[2]

Faculty of Business and Technology, Stamford International University, Thailand.

E-mail: [1]surekha.lanka@stamford.edu, [2]shuvra.tripura@stamford.edu

Abstract

The sixth generation (6G) networks facilitate the provision of large-scale, heterogeneous Internet of Things (IoT) applications with a variety of requirements such as latency, reliability, scalability and data rates that are higher than the limits of traditional network architectures. The drawbacks of current network architectures for implementing heterogeneous IoT applications increased in dynamicity and complexity connected to these kinds of networks. SDN Solutions provide an effective approach to implement the heterogeneous IoT for 6G Networks. The purpose of this review is to provide a comprehensive overview of SDN-based architecture, orchestration mechanism and control strategies includes to connect and improve the performance of related technologies such as NFV, edge and fog computing, network slicing and AI. This paper will explain the SDN-based orchestration improves interoperability, resource allocation, quality of service and security for heterogeneous IoT use cases. This study concludes with future research directions for smart, autonomous and resilient SDN-enabled IoT systems in next-generation 6G Networks.

Keywords: Software-Defined Networking (SDN), Heterogeneous Internet of Things (IoT), 6G Networks, Network Orchestration, Quality of Service (QoS).

1. Introduction

The sixth generation (6G) is the basis of Massive Intelligent Heterogeneous Environment of Things (also known as the Internet of Things) differs from previous generations to support a broad range of IoT applications such as Smart Cities, Industrial Automation, Healthcare Monitoring, Autonomous Transportation and Immersive Digital

DOI: https://doi.org/10.36548/jsws.2025.4.003
Received: 28.11.2025, received in revised form: 26.12.2025, accepted: 13.01.2026, published: 23.01.2026

Environments. Each application requires different service level requirements such as latency, reliability, scalability and data rate requirements.

Due to the large number of IoT services being deployed and their inbuilt complexity makes the demand for these services exceed the ability of traditional network architectures, designed for static configurations are unchangeable to rapidly adapting circumstances and significantly higher level than previous generation. [8]. As the scale of IoT deployments continues to expand and the dynamics of IoT deployments continue to increase, the limitations of existing networks become visible, particularly efficient resource management, interoperability and end-to-end quality of service.

In this research, Software-Defined Networking (SDN) is observed and developed as a potential solution for the challenges faced by various, heterogeneous Internet of Things (IoT) deployments in 6th Generation (6G) Networks. The primary benefit of SDN is separating the Control Plane from the Data Plane. SDN provides control over the whole network from a centralized location that enables global visibility of the network provides the ability to program dynamically to ensure their respond with smart changes in application demands and allows for orchestration and effective management of flexible network resources [9]. The flexibility and effectiveness with SDN facilitates network resource management supports a variety of traffic patterns and service levels required for IoT applications. When combined with other enabling technologies such as Network Function Virtualization (NFV), Edge and Fog Computing, network slicing, and Artificial Intelligence (AI), 6G Networks are able to provide scalable, low latency, and secure IoT services will increase significantly.

The literature review aims to provide a comprehensive overview of SDN-based architectures, orchestration mechanisms and control strategies designed for heterogeneous IoT environments in 6G networks. It examines the SDN-based orchestration improves interoperability, resource allocation, quality of service and security across diverse IoT use cases [10]. Finally, the paper highlights open research challenges and outlines future research directions toward intelligent, autonomous and resilient SDN-enabled IoT systems for next-generation 6G networks.

Networks can provide an integrated approach to manage all networks' resources (e.g., devices and services) using automation of configuration, control and optimization across all

networks in orchestration mechanisms. In general, orchestration allows for different types of devices and services to interact in heterogeneous environments such as IoT and 6th Generation (6G) networks [12]. Orchestration makes it possible to achieve the maximized utilization of all available resources, consistently enforce agreements between parties and deliver services reliably to users. A major advantage of orchestration technology is ability to dynamically adapt unchangeable conditions within the environments to operate. This makes the orchestration technologies highly improve the efficiency of all networks [13].

As a comprehensive overview of Software Defined Networking (SDN)-based architectures, orchestration mechanisms and control strategies used in Heterogeneous Internet of Things (IoT) Environments. This review focuses on the role of SDN orchestration in improving interoperability, resource allocation, QoS (Quality of Service) and Security within multiple use case in 6G Networks.

2. Literature Review

In general, the Internet of Things (IoT) is a vast network of technologies and services that are integrated together to create a system of connected devices. IoT can present some challenges regarding the quality of service (QoS) introduces security risks due to different components and technologies. Software-defined networks (SDNs) can be combined with IoT networks to create innovative solutions for managing the complexities associated with large-scale distributed systems. By integrating the SDN architecture with IoT, it is possible to create new and innovative ways to deal with the extreme heterogeneity of IoT systems. Researchers are currently looking at various methods for utilizing SDNs to manage heterogeneity within IoT systems. In this article, we will investigate the SDN-IoT domain to assist in improving the quality of service in heterogeneously composed SDN-IoT networks. Heterogeneity effects on SDN-IoT networks can cause an increase in controller response times. [1]

Many industries in 2022 is created by the Internet of Things (IoT), is excepted to be an expensive field to create many opportunities for Hackers/Cybercriminals to attack insecurely connected devices. This creates multiple entrances into connected devices and other networks & allows Cybercriminals to utilize new advanced forms of malware via IoT connectivity. To prevent these cyber attacks, it will be necessary to develop security strategies to protect the Internet of Things environment from cyber-attacks and malware attacks. [2]

SDN increases flexibility in our ability to communicate but it also increases the risk of being attacked by hackers. To address this issue, new methods of detecting abnormal communications will need to analyse large amounts of multi-dimensional data, react to abnormal communications behaviour as they happen, and be able to react quickly once a threat is identified. The proposed response to this problem is the creation of an ensemble of algorithms to detect attacks on computer networks using both time-sequence models and classification techniques. The algorithms will standardise the representation of data from the SDN using structure and classification to support incremental learning. The learning process will occur in two phases. [3]

In this research paper, we present a review of new technologies for Command and Control (C2) systems within the military using networked systems. Most of the paper will contain a thorough literature review on the topic of network-enabled or networked C2 systems. Furthermore, we will conduct a thorough analysis of the C2-related paradigm by utilizing the concepts of C2 as well as providing insight through the framework of the various Networked Command and Control Systems through our research and analyses of these technologies. [4]

The purpose of this research is to improve the accuracy of DDoS detection using a combination of hyper-parameter tuning with Machine Learning (ML) algorithms, along with Cross Validation (CV). We have deployed our trained model to the edge of the SDN-IoT network to reduce latency by enforcing mitigation policies via the SDN controller. We also assessed four different classifier types (K-Nearest Neighbor (K-NN), Random Forest (RF), eXtreme Gradient Boosting (XGBoost), and Feed Forward Neural Network (FFNN)) using two benchmark datasets, CICIDS2017 and Edge-IIoT, for binary and multi-class classification. [5]

The analysis found that deep learning and hybrid-based intrusion detection systems are excellent ways for identifying and mitigating cyberattacks within IoT and IIoT networks. These methods performed well within all criteria (Recall, Accuracy, Precision & F1 Score) for detecting attack types. However, the need remains for further examination of other important areas such as computational efficiency, lightweight IDS, hybrid IDS, and real-time anomaly detection capabilities on IIoT devices. [6]

The rise of the Internet of Things (IoT) has been met with an increased emphasis on academic research and commercial interest surrounding IoT security. This is due to many

factors, including the wide variety of devices that are included in the IoT, the different protocols used to communicate with these devices, the nature of data carried by IoT devices, and the sensitivity of that data, and includes all major aspects of security and privacy concerns. It provides a detailed overview of intrusion detection in the IoT, including foundational concepts, such as types of IDS, Tools/Techniques for building IDS, and latest technologies enhancing the performance of IDS can demonstrate that a comprehensive approach is necessary for securing the IoT. [7]

IoT has a broad spectrum of applications, ranging from the industrial sector to virtually all significant sectors of our lives. IoT will lead to a new era of communication. However, due to its ease of configuration and acquisition, IoT is at risk for various types of cyber-attacks and therefore requires extensive defence against such attacks. The extensive levels of interconnectivity between different classes of devices in industrial networks that lack the resources available to most computer networks necessitate creating a framework for designing a robust, cost-effective, and compatible security system for such pivotal anomalies. [8]

As a branch of the Internet, the IoT is a type of communication that enhances standard internet fundamentals through not only human-to-human communication, but also through machine-to-machine communications and devices that connect to the IoT. Many devices can now communicate with each other, everywhere in the world at the same time, and therefore from almost anywhere and at any time. The development of Software Defined Networking (SDN) has been driven by the rapid growth of the IoT. SDN is completely a new form of networking, helped to address many of the structural limitations of existing network architectures. SDN is designed to be programmable and offers a flexible way to manage the challenges of diverse IoT environments. The greatest challenge when using an SDN-based IoT ecosystem is ensuring the highest possible level of service; specifically, the threats posed by denial-of-service-type (DoS) attacks and their potential for service interruptions and diminishing network reliability due to the escalating sophistication levels of these attacks. [14]

3. SDN Architectures

Fig. 1 illustrates the architecture presents a secure SDN-enabled IoT framework that integrates intrusion detection and intelligent attack classification across multiple network planes. The infrastructure plane consists of heterogeneous IoT devices such as smart homes,

wearable devices, vehicular nodes, routers and unmanned aerial vehicles to generate diverse traffic patterns and security requirements. These devices communicate through the data plane that forwarding elements and wireless access points transmit the traffic under the control of the SDN paradigm. The separation of the data plane from the control plane enables centralized and programmable network management is essential for handling the dynamic and large-scale IoT environments [2].

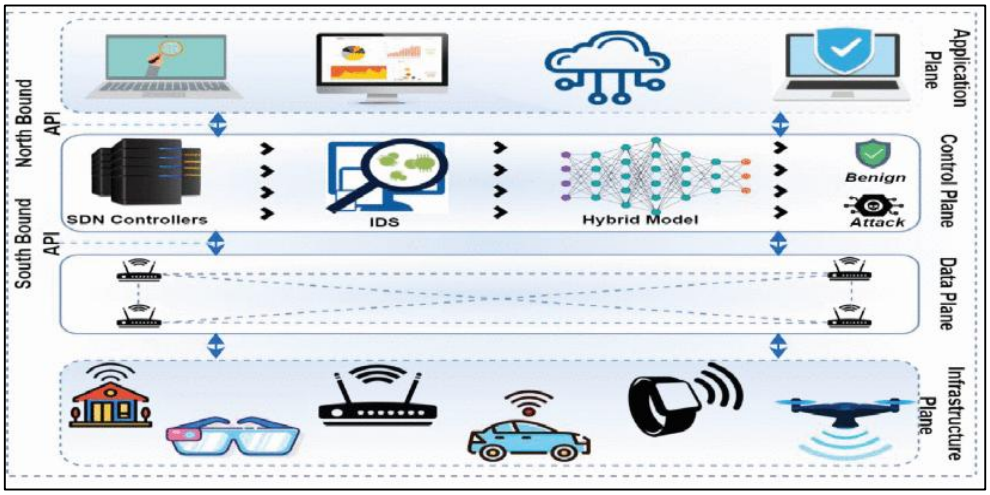

Figure 1. SDN-Enabled IoT Framework [2]

At the control plane, SDN controllers maintain a global view of the network and interact with an Intrusion Detection System (IDS) to monitor traffic flows. The IDS analyses network behavior and forwards extracted features to a hybrid intelligent model that combines multiple learning techniques to accurately classify traffic as benign or malicious. This hybrid approach enhances the detection of accuracy by using both signature-based and anomaly-based detection capabilities. The SDN controller dynamically enforces security policies such as flow blocking, rate limiting or traffic rerouting based on the classification results allows for preventing attacks in real time. The application plane provides interfaces for network monitoring, visualization, cloud-based analytics and security management that enables the administrators to define policies and observe system performance through northbound APIs. Overall, the architecture demonstrates the SDN, IDS and intelligent hybrid models can be effectively integrated to provide scalable, adaptive and secure IoT network management. Figure 2 shows the SDN-Edge-IoT architecture.

The SDN-Edge-IoT architecture consists of three distinct layers. The brief description of these three distinct layers is explained.

1. Application layer: This layer includes the IoT application server in the data centre as well as the controller where developers can use the controller's REST-API to create intelligent IoT applications [5].

2. Control Layer: This Layer contains SDN IoT Controller to serve as prevention controller for DDoS Attack Mitigation via Model Prediction output using REST-API sent to the Controller by an Edge server. The Controller is the primary target for DDoS attackers and single point of failure during an attack.

3. Infrastructure Layer: This Layer contains various kinds of network devices, IoT and end user devices included in the infrastructure layer. In this Layer, there are number of OF Switches that could easily become Targets for DDoS attackers trying to attack the buffer and flow table.

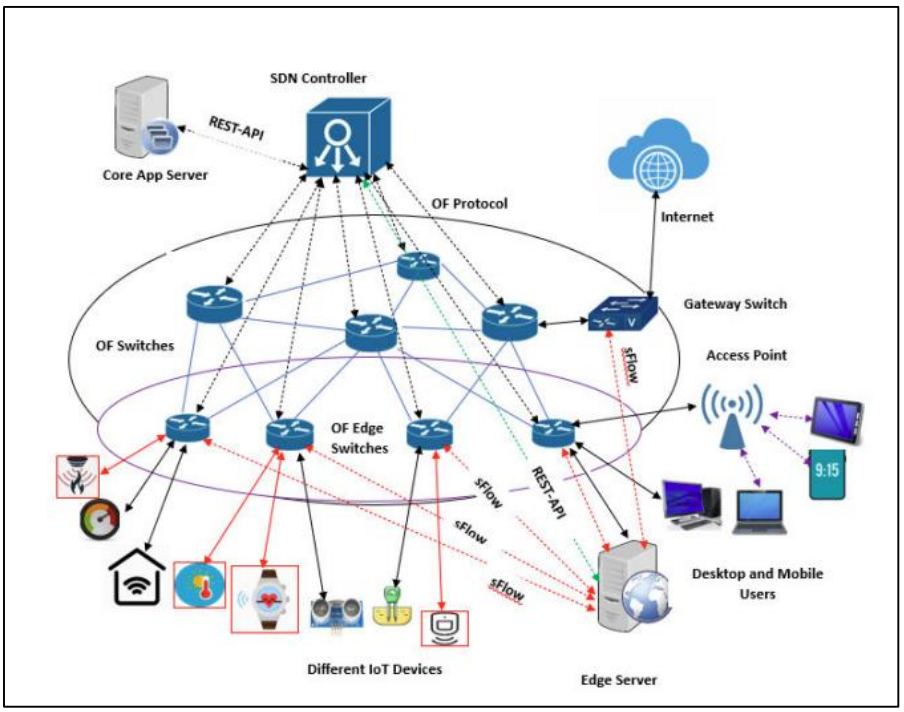

Figure 2. SDN-Edge-IoT Architecture [5]

The components within this layer include:

- **OpenFlow Switches:** This device is used to combine with software-defined networking (SDN). They are located at the end of the provider's (ISP) network and used to forward packets through the ISP's network.
- **Gateway Switch**: This is also an OpenFlow switch. It routes the flow of traffic that enters and exits the ISP.
- **OF Edge Switches:** An A-type OF switch is one that combines IoT Gateway functions and OF switch functions Gateways of the various types of IoT devices are stored at the edge server. Flow statistics received from IoT traffic is uploaded to the edge server using the sFlow protocol. The sFlow protocol is used to detect DDoS attacks.
- **Access Point (AP):** It is a part of the A-type switches.
- End-User Device/User Device: This category of device includes desktop and other devices used by authorized users to provide access services by the Core and/or Edge Servers. The end-user devices/users are unable to access services from the targeted server when a DDoS attack occurs.
- **IoT Devices:** This includes different types of IoT devices such as activity sensors, smart lights, wearables, smart home sensors, etc. All of these devices connect to the edge switches provides simple approach for DDoS attackers to attack them.
- **Edge Server:** Edge server consists of device with a lot of processing power that is located near to IoT devices [10]. The best model is installed on the edge server and will classify traffic sent to the edge server from edge and gateway switches. When the model makes a prediction, it alerts the controller to take appropriate action based on the results of the prediction [11].

The use of sFlow introduces sampling biasthat affect detection accuracy and controller decision-making. The sFlow enables scalable and monitoring considers the sampling bias. It is necessary to ensure the reliable security and traffic management in SDN-orchestrated IoT networks.

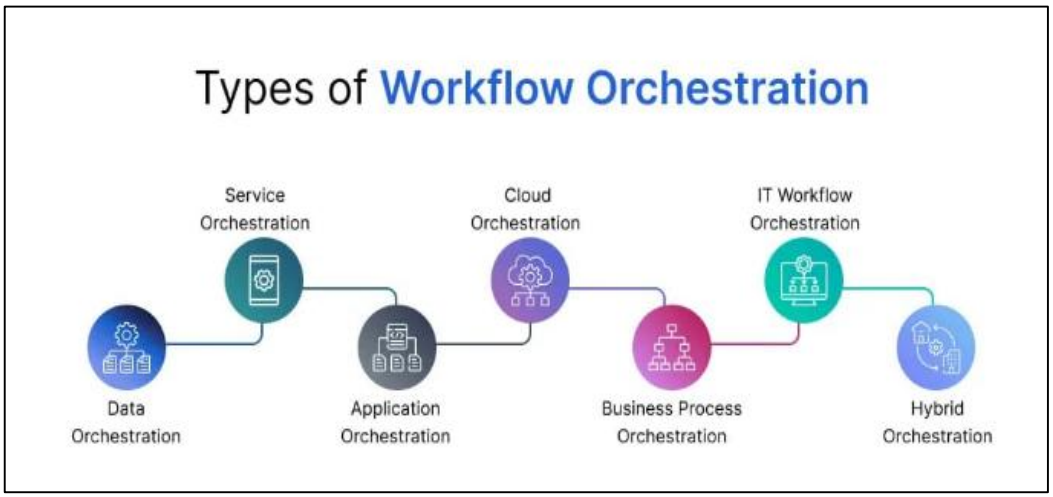

Figure 3. Workflow Orchestration [16]

Workflow orchestration handled the various automated tasks, technology systems and people across complicated workflows. [16] Workflow orchestration involves more automated activity or process; instead of creating interactions between operations occur and their capacity to adjust individually when the entire workflow changes. Fig 3 shows the orchestration workflows

The orchestration workflows have many categories. The data orchestration is focused on managing, transforming and integrating data between systems ensures to operate in a secure way. Service orchestration allows the interaction between various domain level services (based on architectures like Microservices) to occur in an efficient manner. It also determines the sequence of actions are happened when the communication occurs and handle any errors when raised. Application orchestration consists of managing the various applications that operate together. It includes deploying applications to appropriate environments, managing the dependencies of those applications and ensuring the applications operate correctly in the production environments. Cloud application orchestration required to create infrastructure/resources and configuring/maintaining/monitoring same infrastructure/resources used to run applications in the cloud. Business process Orchestration implements all technical workflows, business rules, approvals and human interaction to automate the whole intra-departmental business process. IT workflow orchestration enables the automation of workflows used to process transactions, monitor systems for issues and respond to queries. Hybrid orchestrating allows both local and cloud systems to operate as a part of integrated and

organized workflows in a complex business environment. Table 1 represents the comparative analysis of SDN-Orchestration architectures for heterogeneous IoT.

Table 1. Comparative Analysis of SDN-Orchestrated Architectures for Heterogeneous IoT

Ref	SDN-Orchestrated Architecture	Control & Orchestration Model	Heterogeneity Handling Mechanism	6G-Oriented Capabilities	Representative Use Cases	Key Advantages
[1]	Centralized SDN with IoT Orchestrator	Single global SDN controller with centralized orchestration	Device abstraction and flow-based management	Basic QoS support, limited network slicing	Smart homes, small-scale industrial IoT	Simple design, easy policy enforcement
[2]	Distributed SDN Orchestration	Multiple coordinated SDN controllers	Localized control with device-aware routing	Ultra-low latency, edge-level decision making	Smart cities, vehicular IoT	High scalability, reduced control latency
[5]	Hierarchical SDN-Edge Orchestration	Multi-tier controllers (access–edge–core)	Edge-aware service differentiation	Supports edge intelligence and latency-sensitive services	Industrial IoT, healthcare IoT	Balanced scalability and control efficiency
[8]	AI-Enabled SDN Orchestration	SDN integrated with AI/ML-based orchestrators	Traffic prediction and adaptive resource allocation	Self-optimization, intelligent slicing, automation	Autonomous systems, XR, smart manufacturing	Enhanced adaptability, proactive decision making
[11]	SDN with Network Slicing for IoT	Slice-aware SDN orchestration	Service-specific logical networks	Native support for mMTC, uRLLC, eMBB	Massive IoT, critical communications	Strong isolation, QoS assurance

[12]	Cross-Domain SDN Orchestration	Federated controllers across multiple domains	Unified control of heterogeneous networks	End-to-end orchestration across access, transport, and cloud	Smart grids, multi-operator IoT	Seamless service continuity, global optimization

A machine learning-based latency optimization integrates the multiple advanced paradigms for proactive traffic management, intelligent routing and efficient task offloading while ensuring data privacy. Latency routing is managed using an average of less than 5ms per decision inference latency on edge hardware [15]. Overall, ML inference at the edge improves response, but the latency values depend on efficient model design, hardware acceleration and intelligent orchestration methods.

In the analysis, attributes are evaluated based on the literature review instead of experimental evaluation. The key attributes are orchestration model and control, scalability, latency, heterogeneity handling and 6G-oriented mechanisms. These attributes are derived from architectural design, controller, use of edge or fog computing, integration of AI/ML and support for features like network slicing and cross-domain orchestration.

4. Discussion

As shown in the comparative analysis of the data in Table 1, there is no standard SDN architecture designed for the heterogeneous IoT use cases predicted in 6G networks. The different forms of architecture include various strengths and weaknesses when compared to certain requirements such as scalability, latency, complexity of orchestration and support for multiple IoT services. The centralised SDN architecture provides worldwide control and policy enforcement makes it suitable option for more specific or controlled deployments of IoT. The proposed architecture able to extent the limitation by the size/scope of the controller, their practical use of ultra-dense, highly adaptable characteristics are limited in 6G networks.

The hierarchical and distributed control planes in Software Defined Networking (SDN) is designed to satisfy the requirements of emerging large-scale Internet of Things (IoT) applications that require low latency by allowing locations of the controllers to be nearer to the networks' edges. The comparative performance of data will support when measuring improved response and scalability with large number of devices connecting and transferring around the

network. However, the benefits of a distributed model are balanced by the drawbacks involved with synchronizing, coordinating and increasing the control-plane traffic at the controllers result in low optimal operation of the overall system when it is not managed properly.

Hybrid SDN architectures are aim to combine the benefits of centralized intelligence with the flexibility of distributed execution. This makes the hybrid SDN models to work well in the future 6G network model when there is different types of networks and technologies used in a single domain or between multiple domains. The hybrid SDN models are effective to enable advanced features such as network slicing and differentiated QoS for many heterogeneous IoT services. However, hybrid SDN models are challenging due to the managing complexity, require advanced orchestration tools and higher levels of computation and interoperability support across the different domains when they operate.

The comparative table used in this study reveals that SDN-based orchestration has significant opportunities over future 6G IoT applications due to their improved programmability, more flexible resource allocation capabilities, and they allow enhanced support for heterogeneous types of traffic, compared with existing models. However, among the biggest hurdles to overcome with SDN-based orchestration are building scalable controllers, providing secure and reliable controllers, providing interoperability support for different IoT technologies, and maintaining energy efficiency on constrained nodes to keep future 6G IoT applications operational. It is essential that researchers address these four issues to transition SDN-based orchestration from promising theoretical to proven practical/scale deployment within many heterogeneous deployments of future 6G-enabled IoT networks.

Controller scalability is a crucial challenge in SDN-enabled heterogeneous IoT environments. Because of the enormous number of devices, dynamic traffic patterns, and various QoS requirements expected in 6G networks. Distributed and hierarchical controller designs controls the responsibilities across multiple controllers installed at access, edge, and core layers. By reducing the single point of failure associated with conventional centralised controllers, fault tolerance is addressed. SDN orchestration frameworks identify the controller overloads or failures and reassign control tasks by utilising AI-driven monitoring and predictive analytics.

5. Future Scope

The future of SDN-based solutions for heterogeneous IoT devices in 6G Networks will change from fixed network management to improve autonomous methods of network orchestration. Artificial intelligence (AI) and machine learning will continue to integrated with SDN controllers providing networks to predict user bandwidth requirements and automatically distribute the required resources. Networks will also respond automatically to make changes in the behavior of connected networks and the associated service requirements in real-time. Many different organizations, operators and technologies will be involved in creating a single 6G environment. The design of orchestration solutions will create common, interoperable and standardized control interfaces for multiple domains. Security, privacy and trust is the core design elements particularly for important home IoT devices. Finally, researchers and developers have to verify the new 6G IoT orchestration architecture using various methods such as creating large-scale models or validating via real-time simulations to show the feasibility and enable further use and implementation of 6G IoT.

6. Conclusion

The review of recent advances in SDN-based architecture enables diverse range of devices used in heterogeneous IoT environments under future networks of 6G indicates that SDN provides significant benefits for IoT providing the user with more opportunities to manage their networks effectively and improving the ability of the provider to manage different types of traffic flow from a wide range of devices through a single control (and management) plane. While SDN has proved to provide many benefits, however it is important to recognize the limitations related to the types of SDN architectures accessible. For example, scalability and latency combined with centralized or hierarchical architectures has limitations with distributed and hybrid SDN architectures. This requires substantial planning because of the increased complexity and collaboration required between multiple service providers and users to use the various options provided for developing Scalable Orchestration for SDN enable end-to-end architecture of ultra-dense and ultra-low latency-based 6Gs. There are numerous challenges including scalable control & monitor, security & privacy, interoperability among devices, energy-efficiency in resource management for Low power IoT nodes, etc., have to be solved using this comprehensive research. These challenges illustrate significant gaps in this

comprehension of SDN orchestration for IoT applications. As a result, future research will focus on intelligent SDN orchestration with edge support and developing standardized multi-domain interaction systems to enable the benefits of SDN in a 6G environment.

References

[1] Zafar, Abuzar, Fahad Samad, Hassan Jamil Syed, Ashraf Osman Ibrahim, Manar Alohaly, and Muna Elsadig. "An advanced strategy for addressing heterogeneity in SDN-IoT networks for ensuring QoS." Applied Sciences 13, no. 13 (2023): 7856.

[2] Muthanna, Mohammed Saleh Ali, Reem Alkanhel, Ammar Muthanna, Ahsan Rafiq, and Wadhah Ahmed Muthanna Abdullah. "Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT)." IEEe Access 10 (2022): 22756-22768.

[3] Marmat, Antimbala, and Dolly Thankachan. "Design of an integrated unified intelligence-driven method for low-latency, energy-efficient, and secure cloudintegrated optical broadband access networks." International Journal of Information Technology (2025): 1-13.

[4] Gomes, João Eduardo Costa, Ricardo Rodrigues Ehlert, Rodrigo Murillo Boesche, Vinicius Santosde Lima, Jorgito Matiuzzi Stocchero, Dante AC Barone, JulianoAraujo Wickboldt, Edison Pignaton de Freitas, Julio CS dos Anjos, and Ricardo Queiroz de Araujo Fernandes. "Surveying emerging network approaches for military command and control systems." ACM Computing Surveys 56, no. 6 (2024): 1-38.

[5] Belachew, Habtamu Molla, Mulatu Yirga Beyene, Abinet Bizuayehu Desta, Behaylu Tadele Alemu, Salahadin Seid Musa, and Alemu Jorgi Muhammed. "Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning." IEEE Access (2025).

[6] Ibrahim, Umar, and Mutasem Jarrah. "A Comprehensive Review on Intrusion Detection in Internet of Things (IoT) and Industrial Internet of Things (IIoT) Systems." Journal of King Abdulaziz University: Computing and Information Technology Sciences 14, no. 1 (2025): 22-40.

[7] Rawat, Mamta, and Gaurav Singal. "Surveying Technology Fusion in IoT Networks for IDS: Exploring Datasets, Tools, Challenges, and Research Prospects." ACM Transactions on Intelligent Systems and Technology 16, no. 5 (2025): 1-45.

[8] Min, Wei, Waleed Almughalles, Mohammed Saleh Ali Muthanna, Mohamed Amine Ouamri, Ammar Muthanna, Seungho Hong, and Ahmed A. Abd El-Latif. "An SDN-Orchestrated Artificial Intelligence-Empowered Framework to Combat Intrusions in the Next Generation Cyber-Physical Systems." Human-Centric Computing And Information Sciences 14 (2024).

[9] Doumal, Zouhir, Hakim El Fadili, and Saad Bennani Dosse. "A Review of recent IDS proposals based on Ensemble Learning in IoT Networks." In 2023 7th IEEE Congress on Information Science and Technology (CiSt), pp. 187-192. IEEE, 2023.

[10] Zang, Mingyuan, Eder Ollora Zaballa, and Lars Dittmann. "SDN-based in-band DDoS detection using ensemble learning algorithm on IoT edge." In 2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN), pp. 111-115. IEEE, 2022.

[11] Chauhan, Pinkey, and Mithilesh Atulkar. "A framework for DDoS attack detection in SDN-based IoT using hybrid classifier." In Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021, pp. 889-900. Singapore: Springer Nature Singapore, 2023.

[12] Min, Wei, Waleed Almughalles, Mohammed Saleh Ali Muthanna, Mohamed Amine Ouamri, Ammar Muthanna, Seungho Hong, and Ahmed A. Abd El-Latif. "An SDN-Orchestrated Artificial Intelligence-Empowered Framework to Combat Intrusions in the Next Generation Cyber-Physical Systems." Human-Centric Computing And Information Sciences 14 (2024).

[13] Rožić, Ćiril, Marco Savi, Chris Matrakidis, Dimitrios Klonidis, Domenico Siracusa, and Ioannis Tomkos. "Application-centric dynamic multi-layer resource allocation in availability-aware SDN-orchestrated networks." In 2017 European Conference on Optical Communication (ECOC), pp. 1-3. IEEE, 2017.

[14] Zeleke, Esubalew M., Henock M. Melaku, and Fikreselam G. Mengistu. "Efficient intrusion detection system for SDN orchestrated Internet of Things." Journal of Computer Networks and Communications 2021, no. 1 (2021): 5593214.

[15] Marmat, Antimbala, and Dolly Thankachan. "ML-driven latency optimization for mobile edge computing in fiber-wireless access networks." MethodsX 15 (2025): 103594.

[16] https://www.invensislearning.com/blog/what-is-workflow-orchestration/