International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I2P201

Volume 70 Issue 2, 1-10, February, 2022

Original Article

A Novel SDNFV IoT Architecture Leveraging Softwarization Technology Services to Alleviate IoT Network Resource Restrictions

Ali Haider Shamsan[1], Arman Rasool Faridi[2]

[1,2] *Department of Computer Science, Aligarh Muslim University, Aligarh, India.*

[1]ahtshamsan@myamu.ac.in, [2]ar.faridi.cs@amu.ac.in

Abstract - *Softwarization is the latest network paradigm and technology in which the use of a software solution is preferred rather than traditional hardware. In terms of networking, the latest researches suggest the use of SDN and NFV. It offers the best experience of providing functions and services, managing network traffic, and a new way of control. It facilitates virtualization and the separation of data and control in network devices and also in software-based services. One of the most recent developments in the integration of Internet of Things (IoT) devices, wherewith softwarization, the resource limitation of IoT devices can be handled easily. The previous works on softwarization with IoT, which are found in the literature, are specific in nature, i.e. they are providing a solution to a particular problem instead of presenting an overall solution. Also, some work has just been given the architecture, and no simulation is performed. This work proposed a novel architecture to decrease the resource limitation of IoT by softwarization where IoT is integrated with SDN and NFV. After that, the proposed architecture is built and simulated using a mininet-IoT emulator that supports IoT, SDN, and NFV. For simulation RYU controller is used as an SDN controller, OVSwitch is used as Virtualization services, and 6LoWPAN hosts are used as IoT devices. To compare the novelty of the work and improvement in the network, simulation is also done in simple IoT architecture and compared with the proposed work. The results of the experiment show that there is a significant improvement in the performance of SDNFVIoT Architecture over the simple IoT system.*

Keywords - *Softwarization, IoT, SDN, NVF.*

I. INTRODUCTION

Because IoT components are meant to use less power, no computation, and bits of data transfer, the heterogeneity of IoT networks and devices stand alone weakly.

On a broad scale, IoT devices and networks with diverse protocols and data formats are used to link IoT addressable devices, either virtual or physical, in order to achieve various goals through particular applications [1].

Due to the variety of devices and their diverse objectives, addressing IoT devices in legacy networks and traditional ways is challenging. IoT networks should combine with other technologies to provide dynamic configuration, centralization, and flexibility in order to overcome these constraints. Software-Defined Network (SDN) and Network Functions Virtualization (NFV) are the suitable technologies that enable those functionalities. As a result, combining IoT networks with SDN and NFV may ensure these benefits while also addressing concerns.

The softwarization of the network is combining both SDN and NFV that aims to transform the telecommunication process and system components from legacy and traditional devices to general-purpose devices in order to provide a wide range of services and functions through virtualization and programmable network [2][3] in a cost-effective manner with low Capital and Operational Expenditures CAPEX and OPEX [4].

Software-Defined Networking (SDN) is a revolutionary networking solution that separates control and data devices into different planes and levels [5]. It centralizes the controller to make network management, configuration, and control easier in a dynamic, software-based environment [6]. The controller, which is centred in the control plane [7], enables additional flexibility and simplicity in establishing configuration and rules as well as administering the network [8].

To cope with the rapid increase of network infrastructure, virtualization technology allows virtual infrastructure resources to be reused and shared in a cost-effective manner [9]. NFV virtualizes the infrastructure to offer network services and functions utilizing general-purpose devices [10], and it makes resource management and providing Network Functions (NF) easier, as well as scaling the capacity of the function on-demand [11][12].

The time it takes to create services is decreased[13], and network flexibility is increased [14] when services and functions are installed in a software-based environment.

The prospects of combining SDN and NFV as a softwarization network with IoT are covered in this study. It offers a framework architecture for combining SDN and NFV with IoT. The proposed architecture is created by integrating three different technologies' architectures. The proposed architecture is software-based IoT, which would enable a variety of technologies and provide a variety of tasks that would be impossible to be applied in IoT networks without integrating with other technologies. This study appears to be promising in terms of demonstrating a proof of concept and the protocol stack as well as the results of simulating the proposed works

This work integrates Software-Defined Networking and Network Function Virtualization with the Internet of Things, regardless of the architecture's purpose, and can be applied to a variety of services to achieve various goals such as security, management, orchestration, and control. In this paper, the phrases network softwarization and SDN and NFV integration are used interchangeably.

The rest of the paper is structured as: The second section delves into the principles of softwarization for IoT. The previous related works are explored in Section III. The proposed architecture and its protocol stack are discussed in sections IV and V. Section VI covers the experiment with proof of concept and simulation. The results of simulating the proposed architecture are shown and discussed in Section VII. This paper concludes with some future works in Section VIII.

II. SOFTWARIZATION FOR IOT

Because of the Internet of Things properties, networks must be more interoperable, adaptable, and dependable [15]. In order to manage IoT devices through virtualization and central controllers, as well as provide services and functions for IoT, the best technical option is to connect with SDN and NFV [2][16].

IoT sensors offer limited configuration possibilities and flexibility. A wireless sensor network is an extensive network that requires advanced technology to be run, administrated, and conFig.d. Integrating IoT with SDN and NFV will promote protocol and IoT technology compatibility. Furthermore, virtualization technologies offer network functionalities to simplify IoT control and management at a lower effective cost [17] [18].

As a result, softwarization implements a function as software that can adapt to changes seamlessly and meet service requirements via software updates. By decoupling functionality from hardware and offering functions as software, softwarization makes hardware more autonomous [2][19].

To control IoT devices quickly, the IoT softwarization incorporates NFV and SDN. SDN orchestrates the flow of IoT network traffic from a central location, whereas NFV enables the delivery of on-demand IoT network services [2].

Network softwarization enabled by NFV and SDN improves performance and storage with cost-saving [20]. Softwarization, which reshapes and generates new options to erase limitations and preserve borderlessness between the Internet and its components, has an influence on IoT systems. As a result, IoT devices serve as network edge nodes, storing data and executing system services and operations locally [21].

III. RELATED WORKS

Some earlier efforts have merged SDN and NFV with IoT. Cerroni et al. [22] suggested an IoT reference architecture based on the ETSI MANO framework standard for managing and coordinating heterogeneous IoT network devices. Each SDN and IoT have their own VIM in this design. It focuses only on the service function chaining aspects of the NBI

Salahuddin et al. [18] presented a softwarization-based IoT healthcare system. The proposed architecture sought to make the smart healthcare system more secure and agile. Along with SDN and NFV, it employs blockchain and Tor. This study focuses on the healthcare system and how to use softwarization and blockchain to make it safe and beneficial. That work is a conceptual proposed with no implementation or simulation.

WSNs and UAVs, which are considered IoT applications, use the architecture described in [19]. This work creates a softwarization architecture using SDN and NFV to overcome the limitations of traditional networks and to make use of a pool of generic virtualization resources as well as cloud services.

SDN/NFV for IoT networks was proposed in a research paper [23] to customize switch behaviour in SDN networks. It only combines SDN and NFV technologies, leaving out the IoT network architecture. This study uses Mininet SDN simulation and Floodlight controller to test QoS in an SDN network by streaming video between hosts.

By interacting between real and virtual sensor networks, the architecture proposed in [24] Focus on Physical Sensor Cloud (PSC) for performance modelling of WSN virtualization and adopts the demands of demanded services. The cloud servers will be used to manage this IoT architecture remotely.

Ojo et al. [25] presented an SDN-IoT architecture with NFV implementation that may improve the IoT network's agility, efficiency, mobility, and scalability. Its proposed design is based on SD-IoT architecture in terms of IoT framework virtualization.

In [26], distributed IoT gateways with SDN and NVF are offered as an IoT architecture for disaster management provisioning. This architecture allows gateways to be reused and traffic to be routed between them.

In order to overcome IoT network difficulties, Alenezi et al. [27] combined the two designs of SDN and NFV. COTS

devices can be utilized to deliver a range of services and functionalities under the suggested architecture. This study examines the costs of utilizing various types of networks, including regular 4G and softwarization networks.

The approach presented in [28] [29] combines SDN and NFV technologies to address IoT security risks. The proposed framework is expected to provide security protection measures as integration between current IoT security mechanisms and software services of SDN and NFV. The orchestration layer allows it to communicate with a variety of security systems.

DistBlackNet [30] is a secure Black SDN-IoT and NFV architecture for smart cities presented by Islam et al. This design is based on the SDN-IoT architecture, but with the addition of NFV. It is suitable for constructing clusters with the assistance of distributed controllers, resulting in benefits such as integrity, confidentiality, and energy conservation. Similarly, The same authors have done the work [31] of SDN-IoT architecture with NFV implementation to enable smart city IoT applications. This paper proposes clustering as a viable technique with less power usage for managing the IoT network efficiently. The proposed architecture of SDN-IoT with NFV supports the distribution of controllers, and it increases the flexibility and efficiency of the network.

The work [32] proposes the notion of "Smart Device-as-a-Service" (SDaaS) to replace real IoT devices with virtual ones. SDaaS is designed to increase the scalability, flexibility, and reusability of physical device virtualization services. This paper recommended that NFV equipment be implemented in the Fog environment to reduce the number of network hops.

Table 1. Summary of Previous Works

Reference	Technologies	Purposes	Focus on	Shortcomings
[22]	SDN-IoT with VIM	Management	Focus only on the service function chaining aspects of the NBI	Use only VIM of NFV, not all services and focus on NBI only.
[18]	SDN, NFV, IoT with Blockchain, Tor	Security	Make the smart healthcare system more secure and agile	It is mainly for securing healthcare systems. It used the orchestration layer of NFV.
[19]	SDN and NFV orchestration for UAV and WSN	Management	To adapt an architecture of softwarization for UAV and WSN.	It mainly focuses on the request and response of the services with the cloud.
[23]	SDN/NFV	QoS	To enhance the quality of services.	The architecture is built based on SDN and NFV.
[24]	NFV and IoT	PSC	Focus on Physical Sensor Cloud (PSC) for performance modelling of WSN virtualization	It focuses on virtualizing WSN only for that architecture is built based on NFV and IoT
[25]	SDN-IoT	Conceptual	Focus on SDN-IoT	Add NFV orchestrator to SDN-IoT architecture.
[26]	IoT gateway	Disaster Mgt	Focus on distributed IoT Gateways	Focus on NFV to implement IoT gateways.
[27]	SDN and NFV	COTS	Combined the two designs of SDN and NFV	This study examines the costs of utilizing various networks, including softwarization networks.
[28] [29]	SDN/NFV	IoT Security	Security features to secure IoT	It couldn't be generalized to cover other services.
[30]	SDN-IoT	Security	Secure Smart cities	It's built based on [21] with adding black SDN.
[31]	SDN-IoT with NFV	Security	Smart cities	Focus on distributing controllers
[32]	Deployed architecture only.	Flexibility	Cloud-computing services and replace physical IoT Devices with their "Virtual Images	Bringing cloud-computing services much closer to the end-users
[4] [33] [34]	SDN, NFV , IoT	Security	Respond dynamically to IoT security risks and threats	Focus on security
[35]	SDN and IoT	Performance	Focus on performance	It doesn't propose any architecture; it only tests the performance of combining SDN with IoT.

Molina Zarca et al. [4] [33] presented an IoT architecture based on SDN/NFV. The proposed architectural framework is used to handle IoT network security. It responds dynamically to IoT security risks and threats [34]

The authors of [36] proposed a multi-layered IoT architecture that includes SDN and NFV. According to the authors, the suggested architecture is capable of eliminating and coping with IoT network difficulties. For this, NFV provides virtualized framework and orchestration, as well as VNF services that are addressed by virtualization infrastructure. While SDN is used to build communication between virtualized operations, it also manages the service infrastructure.

The authors discuss the performance of the 6LoWPAN device on an internet of things (IoT) network utilizing the SDN paradigm in their study [35]. They used the Mininet-IoT emulator and the Open Network Operating System (ONOS) controller to use IPv6 forwarding for the Internet of things (IoT). The performance of multiple topologies that included a host, switch, and cluster was put to the test. This paper looks at how to assess QoS performance in a more complex environment, such as one with a more complex topology, a higher number of hosts, and a more significant number of hosts [37].

The previous works on softwarization with IoT, which are found in the literature, are specific in nature, i.e., they are providing a solution to a particular problem instead of presenting an overall solution. Also, some work has just been given the architecture, and no experimental results are given.

The topic is analyzed based on the previous works. Then the found solutions are summarized along with the shortcomings, which are outlined in table 1. In light of the previous works, a comparison is made with the proposed system, and comparison results are presented in Table 4. The aforementioned previous works focus on specific purposes, either security, management, disaster management, etc. Meanwhile, the proposed architecture is the multi-purposed architecture built based on the standard architectures of SDN, NFV, and IoT. It can be applied for a variety of services leveraging the powerful resources of SDN and NFV. Moreover, SDNFVIoT architecture could be considered as reference model architecture of softwarization IoT.

IV. PROPOSED WORK

The most crucial step in meeting the massive demands of the smart environment is to integrate technologies with IoT. This work proposes an architecture for combining SDN and NFV with IoT in this paper. As shown in Fig. 1, the suggested design is made up of four primary layers, each of which contains sub-layers of the three technologies and the linkages between them.

The proposed work of this study comes in SDNFVIoT architecture that combines the three technologies. It also presents a proof of concept and the protocol stack of each technology in all layers.

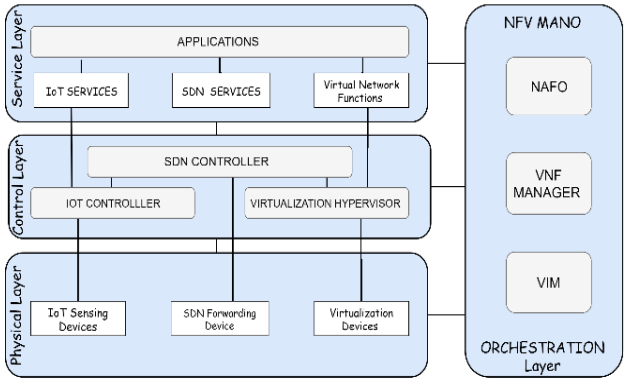

Fig 1. SDNFVIoT architecture.

This work is a novel attempt of integrating Software Defined Network and Network Function Virtualization with the Internet of Things regardless of the purpose of architecture, which can be applied to many services to achieve various goals such as security, management, orchestration, controlling, etc.

V. PROTOCOL STACK

Each layer of the proposed architecture has different protocols to communicate with other layers and to communicate in the same layer between different devices and applications. The protocol stack may consist of more than one protocol in the same layer as well as for the same devices. Moreover, it shows the possible list of protocols that can be applied and used.

To provide compatibility between devices and protocols from diverse suppliers with varying standards, the protocol stack allows interoperability across all components of the proposed IoT system with SDN and NFV, as shown in Fig. 2. Several protocols deal with various devices, ranging from simple protocols to support IoT devices to complex protocols to support SDN and NFV technologies.

A. Multi protocols possibilities

The proposed architecture may leverage IoT's limited resources to take advantage of SDN and Virtualization's capabilities. Multi protocols may support numerous devices in every layer, as shown in Fig. 1, and specific devices support multiprotocol.

SDN assists IoT networks with administration, security, and network monitoring services that need powerful resources. Simultaneously, virtualization may provide virtual IoT services to ensure a high degree of Quality of Service (QoS) and Quality of Experience (QoE) [4].

Furthermore, IoT uses many protocols to execute a single activity. Lower devices, like sensors, employ protocols enabled by the physical layer, such as Bluetooth or WiFi. Different protocols are used to send and format the data. Simultaneously, data format modifications at the next level

are dependent on the supporting transmission protocols, such as CoAP, MQTT, or HTTP. The packets are formatted, encapsulated, and de-capsulated using various protocols dependent on the middleware devices at the application level.

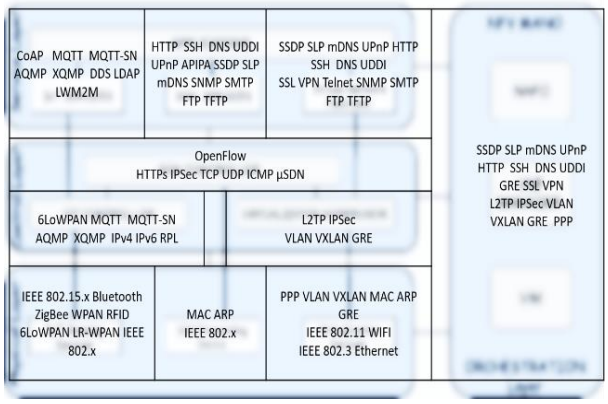

Fig 2. Protocol Stack

B. Interoperability Of Protocols

The massive IoT network should support all devices and sensors, as well as diversified wireless connectivity, with numerous devices that communicate heterogeneous data. The key to ensuring consistent communication among multiple devices and systems is interoperability. Nevertheless, the available systems and appliances are varied in data formats, protocols, and communication technology. Communication among such diversity is pretty challenging without interoperability. The proposed architecture of integrating IoT with powerful network technologies, namely; SDN and network virtualization, provides a high level of interoperability between IoT devices and various systems.

The proposed architecture's interoperability not only enables IoT devices but also multiple network devices in leveraging the benefits of NFV and SDN. As a result, IoT applications may employ a variety of devices, protocols, and data formats at each layer to fulfil their goals.

VI. THE EXPERIMENT

A. The Proof of Concept (PoC)

It is the stage of experimental development when theory solutions are tested and verified for their practical potential. It discusses how the offered solutions could accomplish the major goals. The method by which the results and outputs will be given in the end is determined by developing PoC's strategy, and the basic concept is viable.

PoC may be developed in a variety of ways. In this study, we took into concern the technological techniques that are suited for the nature of the proposed work. Demonstration and experimentation are successful ways in this field and with this type of work. In the proof of concept, we'll create a Demo of the proposed architecture and try to build it as a case study. The suggested solution will be validated by a study of the Demo simulation and its outcomes.

B. Simulation

The procedures of the experiment are separated into two scenarios, as shown in Table 2: the first is a simple IoT network with six IoT devices, two hosts, two access points AP, and a switch. Each three IoT device are connected to AP, APs are connected to OVSwitch, and the two hosts are connected to OVSwitch. As seen in Fig. 3, this scenario is a simple IoT system. The second scenario is integrated with SDN by adding a controller to the first scenario, as illustrated in Fig. 4.

Table 2. Experiment Scenarios

Scenario	IoT devices	AP	OV Switch	Host	SDN Controller
Simple scenario	6	2	1	2	-
integrated scenario	6	2	1	2	1

Mininet-iot [38] is used to simulate both scenarios, using a python application for each. Mininet is a well-known SDN emulator that covers the majority of SDN services, including host, OVSwitch, and controller. Mininet-iot is the name of the version that supports both SDN and IoT. Mininet-iot works with a variety of IoT devices and protocols, as well as all mininet and mininet-wifi services.

D-ITG [39] tools are used to generate the traffic in order to evaluate the latency and efficiency of SDNFVIOT architecture to a standard and basic one. As previously mentioned, two scenarios are simulated: one is a simple architecture, and the other is one that is integrated with the controller.

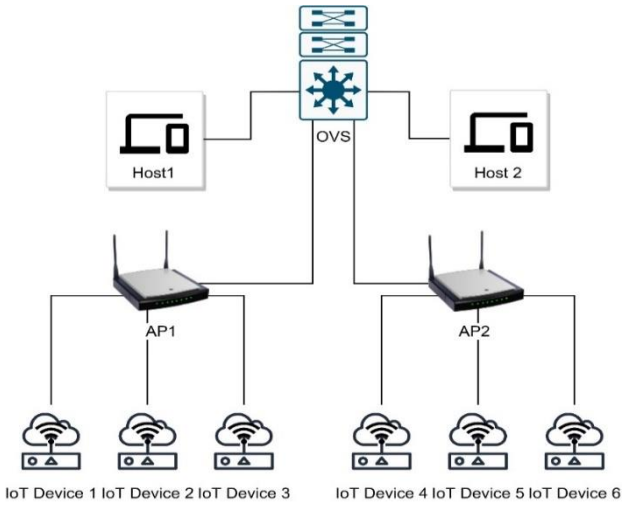

Fig 3. Simple IoT Scenario

Figs 3 and 4 depict the two scenarios that were tested in the same environment and set up for the same period of time. Fig. 3 depicts a conventional IoT topology with IoT

devices linked to access points and APs to switches through wireless connections. Fig. 4 depicts an RYU controller connected to the switches in the architecture. The D-ITG tool is used in both experiments to produce traffic between the sender and receiver. Both scenarios create traffic for thirty seconds at a rate of 30 packets per second with a packet size of 1024 bits.

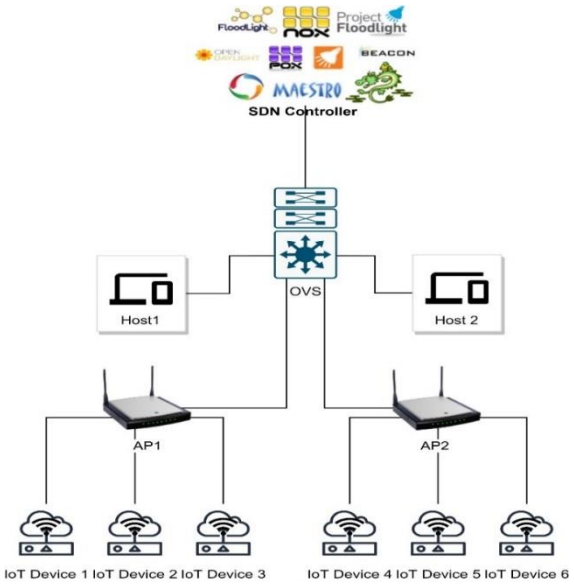

Fig. 4. Integration Proposed SDNFVIoT Scenario

To make the emulation more faithful to IoT networks, the data traffic type is UDP.

First, a common IoT scenario is simulated and then use the D-ITG tool to create data flow from device 2 (IoT device 2) to device 4 to verify the network's quality (IoT device 4). IoT devices are 6LoWPAN-supported devices with IPv6 in the simulation. Similarly, we've done the same with the integrated scenario, which includes IoT devices, OVSwitches, and an RYU controller. Both devices are connected to separate Access points that are connected to the OVSwitch. D-ITG keeps track of the transmission information in a log file and generates reports from it.

VII. RESULTS

Based on the experiment scenarios, the average results are categorized, as indicated in table 3 of the D-ITG transmission report. However, the experiments have been done twenty times for the aforementioned scenarios in the same environment. The final results have been considered from the average values.

The results of both tests are shown in table 3 of the D-ITG report: basic IoT scenario and SDNFV-IoT scenario.

The report indicates that values differ in both tests; the SDNFV-IoT scheme's values are better than those of a simple IoT scenario. Starting from total packets, there are about four packets in total packets, while the total time of a simple scenario is more with (0.000103) s, which should lead to more packets due to packet per seconds rate.

Minimum, maximum, average, and delay standard deviation are the four types of delays that are used as testing criteria. In both scenarios, minimum delay values differ from

Table 3. D-ITG report of experiments

		Simple IoT scenario		Integrated SDNFV-IOT scenario	
From:		2001::2		2001::2	
To:		2001::4		2001::4	
Total time	=	29.987115	s	29.987012	s
Total packets	=	1469		1473	
Minimum delay	=	0.000554	s	0.000530	s
Maximum delay	=	0.030207	s	0.029674	s
Average delay	=	0.004185	s	0.003763	s
Average jitter	=	0.003923	s	0.003476	s
Delay standard deviation	=	0.003692	s	0.003691	s
Bytes received	=	1504256		1508352	
Average bitrate	=	401.374219	Kbit/s	402.401413	Kbit/s
Average packet rate	=	48.995876	pkt/s	49.121266	pkt/s
Packets dropped	=	0	0.00%	0	0.00%
Average loss-burst size	=	0	pkt	0	pkt

one another. The SDNVFIoT experiment is (0.000530 s), whereas the basic IoT scenario is (0.000554 s). The difference is (0.000024 s) counted less for SDNVFIoT topology.

Both the basic IoT and SDNFVIoT scenarios have maximum delay values of (0.030207 s) and (0.029674 s), respectively. SDNFVIoT is shown to have a smaller maximum delay, with a difference of (0.000533 s). Both the Minimum and Maximum delays are depicted in Fig. 5.

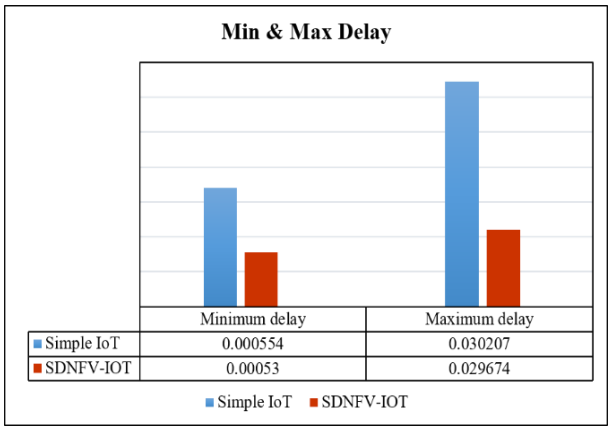

Fig 5. Minimum and Maximum Delay

In a basic IoT experiment, the average delay values are (0.004185 s), whereas the SDNVFIoT value is (0.003763 s). The average latency in the SDNFV-IoT experiment is less with (0.000422 s) than the simple IoT, as shown in Fig. 6. Similarly, the average jitter shows the superiority of SDNFVIoT with (0.000447 s).

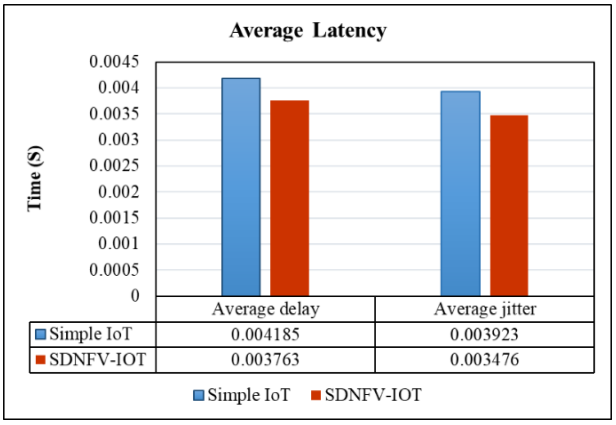

Fig 6. Average Delay and Average Jitter

When it comes to data rate, the SDNFV-IoT outperforms basic IoT topology tests. The purpose of the test is to look at the topology and transmission medium. As a result, the bytes received, average bitrate, and average packet rate demonstrates SDNFVIoT's supremacy. The byte is received in the basic scenario (1504256 bytes) and the SDNFVIoT scenario (1508352 bytes). The average bitrates (401.374219 Kbit/s) and (402.401413 Kbit/s) of basic IoT and SDNVFIoT, respectively.

The average packet rate in an IoT topology (48.995876 pkt/s) against (49.121266 pkt/s) in the experiment scenario of the proposed architecture is shown in Fig. 7. The difference (4,096 bytes), (1.027194 Kbit/s) and (0.12539 pkt/s) respectively. As a result, the byte received, average bitrate, and average packet rate demonstrate SDNFVIoT's supremacy

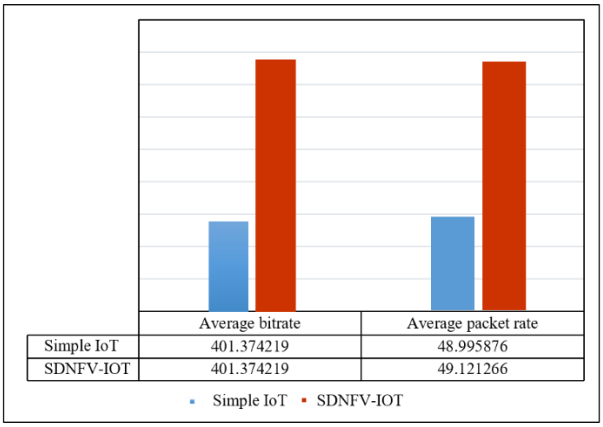

Fig 7. Average Bitrate and Packet Rate

However, no packets were lost or dropped in any scenario. The SDNFVIoT topology is credited with the preference in the above-mentioned items. It demonstrates that the proposed SDNFV-IoT framework outperforms the simple IoT network topology structure using the report's values.

In addition, Fig. 8 decodes and displays the log file of transmission traffic for both cases. To decrease the chart due to the number of entire packets of the log file, the average of each twenty packets is summed into one item.

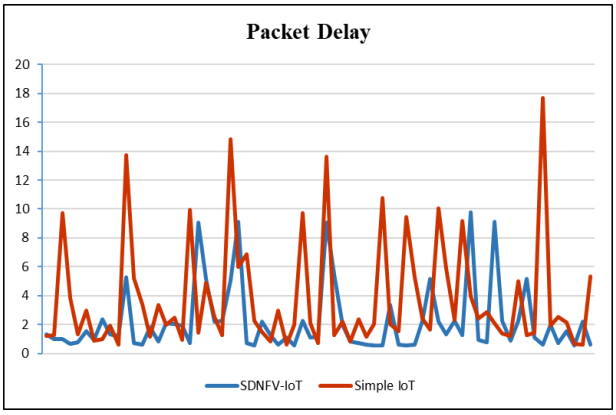

Fig 8. Packet Delay

During the experiment simulation, the delay of a packet delivered from sender to receiver and between two received packets is illustrated in Fig. 8. In the overall plot, the packet latency of SDNFVIOT architecture is less than that of the simple IoT one. The significance of minimizing packet transmission latency is that it improves the transmission medium's dependability.

Overall, the experiment results and analysis denote that the proposed integration of SDN and NFV with IoT network architecture is more reliable besides the tremendous service and applications that SDN and NVF can provide to IoT.

different, so the results are also different. Anyway, their results show that there are some packet losses, and the delay is more than in the experiment.

The work [23] proposed architecture of IoT SDN/NFV

Table 4. Comparison of Proposed Solution

Work	SDN	NFV	IoT	Application independent	Performance improvement	Experiment
[22]	□		□	X	X	X
[18]	□	□	□	X	X	X
[19]	□	□	X	X	X	□
[23]	□	□	X	□	X	□
[24]	X	□	□	X	X	□
[25]	□	□	□	□	X	X
[26]	X	□	□	X	X	□
[27]	□	□	X	X	X	X
[28] [29]	□	□	□	X	X	X
[30]	□	□	□	X	X	X
[31]	□	□	□	X	X	□
[4] [33] [34]	□	□	□	X	X	X
[35]	□	X	□	X	□	□
SDNFVIoT	□	□	□	□	□	□

VIII. DISCUSSION

In comparison to constrained IoT networks, this may build various SDN and NFV applications in IoT networks, leveraging their robust network resources.

Table 4 has compared the proposed system with the existing ones, and it checked whether a system is based on SDN, NFV, or IoT. In addition, whether the solutions discussed belong to just an application or an overall solution. Moreover, the experimentation is checked with it has been done, or only conceptual design is given. The Comparison shows that the proposed architecture solution is better than the previous works compared to the literature with respect to performance enhancement. The architecture proposed in this study encompasses all levels of the three technologies: SDN, NFV, and IoT. Previously, they had only integrated particular layers of both SDN and NFV technologies with IoT in related works. This work attempted to include the three technologies in the experiment. Also, due to the lack of previous results and most of the previous works were only conceptually proposed, in the experiment, we suggested simulating proposed architecture and simple IoT architecture to examine the superiority of SDNFVIoT architecture.

Only two works [23][35] have experimented with testing performance, but both have different tools and scenarios, but both are similar in the concept of simulation, such as transmitting data traffic from one device to another and testing the quality of services and delay. The work [35] experimented with IoT with SDN only, and the experiment was simulated using mininet-IoT, which is used in the experiment; however, the testing scenarios and tools were that contained the three technologies together, but it differs from ours that control plane contains the controllers of all SDN, IoT and Virtualization hypervisor, while theirs putting the virtualization layer with the controller without IoT controller. In the application layer, applications haven't been categorized based on the technologies. The authors simulated their architecture using the main SDN mininet simulator with a floodlight controller. The topology is built as a hierarchal tradition network. It tested the quality of services by sending video streams from one device to another. The hosts that were used in their experiment were classical network hosts.

In the experiment, two scenarios are experienced to show the superiority of the proposed architecture on the simple IoT architecture. SDNFVIoT architecture comes out with more results and compares both scenarios. The report of the experiments contains many criteria such as packet number, delay, jitter, packet size, bit received, and dropped packets.

Other previous publications either presented a conceptual framework and architecture without conducting any experiments or experiment with them application-wise. Each of these had been proposed for a specific purpose. On the other hand, SDNFVIOT may be used for a variety of objectives, including management, security, and data flow.

IX. CONCLUSION

The proposed softwarization of IoT architecture (SDNFVIoT) is intended to be more agile and adaptable since this architecture is more universal and may be used in a variety of applications and services for diverse reasons. As

a result, it addresses the scalability concerns that plague IoT networks. New devices and nodes may be simply added, dynamically configured, and managed virtually.

Network softwarization, which is the outcome of merging SDN and NFV, is regarded as a best practice in networking for offering low-cost and adaptable functions and services. These technologies' strength is in regulating networks and providing high-quality services on general-purpose devices using virtualization technologies.

Integrating technologies is the most acceptable approach for dealing with the rapid expansion of technological sectors. It may assist overcome the inadequacy of one technology. In this context, this research suggests combining SDN and NFV with IoT to address the inadequacy of IoT networks that were created with limited capabilities. It advocated merging the architectures of SDN, NFV, and IoT. On the other hand, it is the process of integrating SDN and NFV to achieve softwarization or network softwarization. As a result, this study may be classified as merging softwarization with IoT.

Softwarization IoT (SDNFVIoT) is the proposed architecture, enabling several technologies and providing a variety of activities that would be hard to deliver in IoT networks without linking to other technologies. This research seems promising in terms of providing a proof of concept and the protocol stack. It simulated the proposed works and discussed the results that showed the superiority of the proposed architecture compared to previous work and standard simple IoT architecture

REFERENCES

[1] C. Mouradian, S. Kianpisheh, and R. H. Glitho, Application Component Placement in NFV-based Hybrid Cloud / Fog Systems, 2018 IEEE Int. Symp. Local Metrop. Area Networks, (2018) 25–30.

[2] B. Yi, X. Wang, K. Li, S. k. Das, and M. Huang, A comprehensive survey of Network Function Virtualization, Comput. Networks, vol. 133 (2018) 212–262.

[3] F. Marino, L. Maggiani, L. Nao, P. Paganoy, and M. Petracca, Towards softwarization in the IoT**,** Integration and evaluation of t-res in the oneM2M architecture, IEEE Conf. Netw. Softwarization Softwarization Sustain. a Hyper-Connected World en Route to 5G, NetSoft (2017).

[4] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, Enhancing IoT security through network softwarization and virtual security appliances, Int. J. Netw. Manag., 28(5) (2018) 1–18.

[5] A. H. Shamsan and A. R. Faridi, SDN-assisted iot architecture**,** A review, in 2018 4th International Conference on Computing Communication and Automation, ICCCA,(2018).

[6] E. Haleplidis, J. H. Salim, and D. Meyer, Software-Defined Networking (SDN)**,** Layers and Architecture Terminology, 1–35 (2015).

[7] A. H. Shamsan and A. R. Faridi, Security Issues and Challenges in SDN, in Advances in Cyber Security. ACeS 2021. Communications in Computer and Information Science, N. Abdullah, M. Anbar, and S. Manickam, Eds. Springer, Singapore,1487 (2021) 515–535.

[8] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, Integrated NFV/SDN Architectures**,** A Systematic Literature Review, (2018).

[9] A. J. Gonzalez, G. Nencioni, A. Kamisi, B. E. Helvik, and P. E. Heegaard, Dependability of the NFV Orchestrator **,** State of the Art and Research Challenges, XX(c) 378–383 (2018) 1–23.

[10] S. Il Kim and H. S. Kim, Semantic Ontology-Based NFV Service Modeling, Int. Conf. Ubiquitous Futur. Networks, ICUFN, (2018). 674–678.

[11] Y. T. Woldeyohannes, A. Mohammadkhan, K. K. Ramakrishnan, and Y. Jiang, ClusPR**,** Balancing Multiple Objectives at Scale for NFV Resource Allocation, IEEE Trans. Netw. Serv. Manag., 378–383 (2018) 1–1.

[12] B. Zhang, P. Zhang, Y. Zhao, Y. Wang, X. Luo, and Y. Jin, Co-Scaler**,** Cooperative scaling of software-defined NFV service function chain, 2016 IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Networks, NFV-SDN , (2016) 33–38.

[13] M. Xie, C. Banino-Rokkones, P. Grønsund, and A. J. Gonzalez, Service assurance architecture in NFV, 2017 IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Networks, NFV-SDN, 378–383 (2017) 229–235.

[14] Y. Cheng, L. Yang, and H. Zhu, Deployment of service function chain for NFV-enabled network with delay constraint, Int. Conf. Electron. Technol. ICET (2018) 383–386, 2018.

[15] A. H. Shamsan and A. R. Faridi, Network softwarization for IoT**,** A survey, in Proceedings of the 6th International Conference on Computing for Sustainable Global Development, INDIACom (2019) 1163–1168.

[16] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, A Vision of IoT**,** Applications, Challenges, and Opportunities With China Perspective, IEEE Internet Things J., 1(4) 378–383 (2004) 349–359.

[17] L. Valdivieso, A. Peral, A. Barona, L.García, Evolution and Opportunities in the Development IoT Applications, Http**,**//Journals.Sagepub.Com/Doi/Full/10.1155/2014/735142, (2014).

[18] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare, IEEE Comput., 378–383 (2017) 74–79, .

[19] S. Mahmoud, I. Jawhar, N. Mohamed, and J. Wu, UAV and WSN softwarization and collaboration using cloud computing, 3rd Smart Cloud Networks Syst. SCNS (2016) (2017).

[20] A. J. Ramadhan, T-S3RA**,** Traffic-aware scheduling for secure slicing and resource allocation in SDN/NFVEnabled 5G Networks, Int. J. Eng. Trends Technol., 69(7) 378–383 (2021) 215–232.

[21] H. Khazaei, H. Bannazadeh, and A. Leon-Garcia, End-to-end management of IoT applications, IEEE Conf. Netw. Softwarization Softwarization Sustain. a Hyper-Connected World en Route to 5G, NetSoft (2017).

[22] W. Cerroni et al., Intent-based management and orchestration of heterogeneous OpenFlow/IoT SDN domains, IEEE Conf. Netw. Softwarization Softwarization Sustain. a Hyper-Connected World en Route to 5G, NetSoft , (2017).

[23] Á. L. V. Caraguay, P. J. Ludeña-González, R. V. T. Tandazo, and L. I. B. López, SDN/NFV Architecture for IoT Networks, in Proceedings of the 14th International Conference on Web Information Systems and Technologies, (2018).

[24] I. S. Acharyya and A. Al-Anbuky, Towards wireless sensor network softwarization, IEEE NETSOFT, IEEE NetSoft Conf. Work. Software-Defined Infrastruct. Networks, Clouds, IoT Serv.,

[25] M. Ojo, D. Adami, and S. Giordano, An SDN-IoT architecture with NFV implementation, IEEE Globecom Work. GC Wkshps 2016 - Proc., 378–383 (2016).

[26] C. Mouradian, N. T. Jahromi, and R. H. Glitho, NFV and SDN-Based Distributed IoT Gateway for Large-Scale Disaster Management, IEEE Internet Things J., 5(5) 378–383 (2018) 4119–4131.

[27] M. Alenezi, K. Almustafa, and K. A. Meerja, Cloud based SDN and NFV architectures for IoT infrastructure, Egypt. Informatics J., 20(1) 378–383 (2019) 1–10.

[28] I. Farris et al., Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems, IEEE Conf. Stand. Commun. Networking, CSCN, (2017) 169–174.

[29] I. Farris, T. Taleb, Y. Khettab, and J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surv. Tutorials, 21(1) 378–383 (2019) 812–837.

[30] 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, 2nd Int. Conf. Electr. Comput.

Commun. Eng. ECCE, (2019) 1–6.
[31] B. K. Mukherjee, S. I. Pappu, and J. Islam, An SDN Based Distributed IoT Network with NFV Implementation for Smart Cities, 2nd Int. Conf. Cyber Secur. Comput. Sci. (ICONCS 2020)At Daffodil Int. Univ. Dhaka, (2020) 1–13.
[32] L. Atzori et al., SDN&NFV contribution to IoT objects virtualization, Comput. Networks, 149 (2019) 200–212.
[33] A. Molina Zarca et al., Security Management Architecture for NFV/SDN-Aware IoT Systems, IEEE Internet Things J., 6(5) (2019) 8005–8020.
[34] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, Managing AAA in NFV/SDN-enabled IoT scenarios, 2018 Glob. Internet Things Summit, GIoTS , (2018) 1–7.
[35] D. Y. Setiawan, S. N. Hertiana, and R. M. Negara, 6LoWPAN Performance Analysis of IoT Software-Defined-Network-Based Using Mininet-Io, in IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), (2021) 60–65.
[36] N. Omnes, M. Bouillon, G. Fromentoux, and O. Le Grand, A Programmable and Virtualized Network & IT Infrastructure for the Internet of Things, Int. Conf. Intell. Next Gener. Networks, 378–383 (2015 64–69.
[37] A. H. Shamsan and A. R. Faridi, A Conceptual Architecture for Integrating SDN and NFV with IoT, in Press, 1–11.
[38] GitHub - ramonfontes/mininet-iot. [Online]. Available**,** https**,**//github.com/ramonfontes/mininet-iot. [Accessed**,** 06-Sep-2021].
[39] A. Botta, W. De Donato, A. Dainotti, S. Avallone, and A. Pescap, D-ITG Manual, COMICS (COMputer Interact. Commun. Gr. Dep. Electr. Eng. Inf. Technol. Univ. Napoli Federico II, (2019)1–35.