An Integrated Work Implemented In IoT Using Software Defined Network: A Review

Prof. Sonal Bhavsar[1] Prof. Chintankumar K. Bhavsar[2] Prof. Komal Thumar[3]
Prof. Deepali Jain[4] Prof. Pravina Parmar[5]
[1,3,4,5]Assistant Professor [2]Lecturer
[1,2,4,5]Department of Information Technology & Computer Engineering [3]Department of Information & Communication Technology
[1,4,5]LDRP-ITR, Gujarat, India [2]Government Polytechnic, Gujarat, India [3]Sal Institute Of Technology and Engineering Research, Gujarat, India

Abstract— The COVID-19 pandemic has impacted the industrial ecosystem in various sectors like education, IT-companies, healthcare and many more to an unprecedented degree due to large-scale contact restrictions. Therefore, since the beginning of the outbreak, there has been significant intervention in production and socio-economic processes that require human involvement. The result is due to online activities like work from home, online entertainment platforms, online business (e-commerce) etc are increasing Internet traffic drastically. Our research aims to examine the integration of the most innovative networking research area that the development of Internet of Things (IoT) application using software-defined networks (SDN). Software-Defined Networking (SDN) is networking approach that utilizes software-based controllers or application programming interfaces to communicate with the hardware infrastructure underneath. Infrastructure is the key distinction between SDN and traditional networking. Traditional networking is hardware-based while SDN is software-based, leading to greater flexibility. Administrators have the ability to manage the network, modify configuration settings, provide resources, and increase network capacity — using a centralized user interface; all functionality is available without the need for additional hardware. The Internet of Things (IoT) is a forthcoming technology that is rapidly gaining industry and research attention. Currently, there are more than 50 billion devices connected to the Internet, and this number is expected to increase to 75 billion by 2025. The data generated by these IoT devices is enormous, leading to resource allocation, flow management, and security risks in IoT networks. In this SLR, we covered the basics of SDN, different studies which provide SDN based solutions for IoT technologies, IoT applications using SDN, and various challenges encountered when implementing IoT applications using SDN.

Key words: Software Define Network, SDN, SDN Applications, SDN Challenges, SDN Future Work

I. INTRODUCTION

With the addition of new devices and content every day, today's computer networks become more and more complex. The equipment that is utilized in networks such as firewalls, switches, Intrusion Detection system, Load balancers are typically it is very difficult to manage without assistance from a network administrator, the solution for this is Software Defined Networking. It has changed the way we used to manage the networks. The two main basic principles of Software Defined Networking (SDN)

The control plane and data plane are separated by it, with the control plane containing intelligence and control logic and the data plane containing physical infrastructure.[1]

The control plane is the brain of the network, with complete control over the data plane. All the elements in the data plane are capable of being manipulated depending on the requirements, configuring every single element of the plane is not necessary.[1]

Programmable networks have been suggested to make network evolution easier. The new networking model is Software Defined Networking (SDN) in which the forwarding hardware is separated from the control decisions. [2] SDN enables innovation and evolution; also assure to significantly simplify network management. The objective is to allow software developers to rely on network resources in the same easy manner as they do on storage and computing resources.

In SDN, the network intelligence is software-based controllers (the control plane) which is logically centralized and network devices become simple packet forwarding devices (the data plane) that can be programmed via an open interface [3][4]

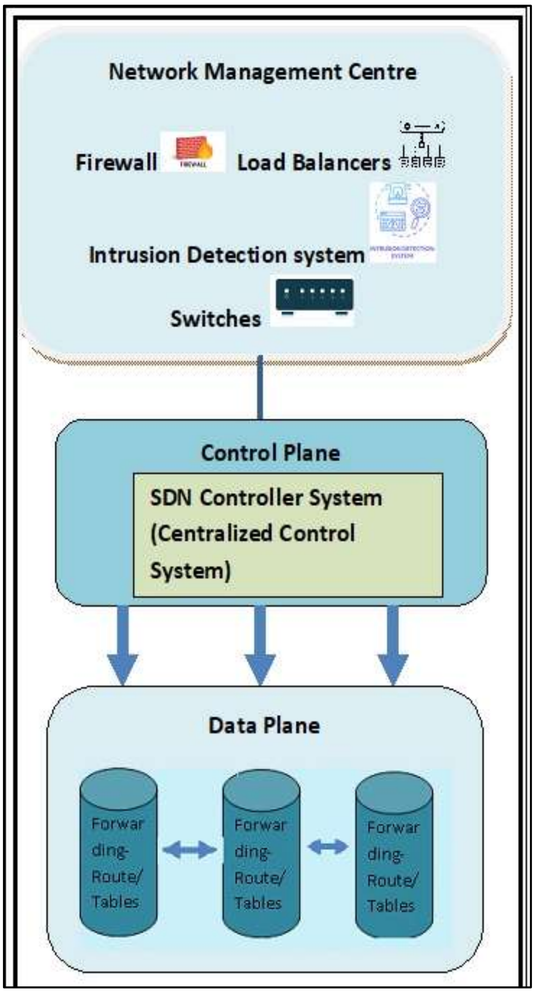
Network Management Centre
Firewall
Load Balancers
Intrusion Detection system
Switches
Control Plane
SDN Controller System (Centralized Control System)
Data Plane
Forwar ding-Route/ Tables
Forwar ding-Route/ Tables
Forwar ding-Route/ Tables

Fig. 1: Basis Architecture of SDN

II. WORKFLOW OF SOFTWARE DEFINE NETWORK OR HOW SDN ARCHITECTURES WORK

More stated earlier than, SDN separates the control plane and the data plane from being on a single device like a router. The separated control plane is now identified as the SDN controller. The advantage of SDN controller is network administrator have to manage only one controller, its gives freedom to manage or control individual device. An SDN network allows for centralized, dynamic and efficient networks configuration. [6]

Dynamic network configuration is possible through the use of SDN applications. SDN applications are used to configure the network and are created with specified network requirements and desired network behavior. Applications are in the management plane and they are deployed by the SDN controller to the switches and routers in the data plane. The applications allow SDN controllers to autonomously control the network and its behavior. In order for this to be possible there needs to be a way for the SDN controller to communicate with every device on the network.[5] The 3 SDN planes use dedicated interfaces to interact with each other. There are two interfaces named the northbound and southbound interfaces. The northbound interface connects the SDN controller/control plane to the management plane which is where applications are deployed and handled, while the southbound interface connects the controller to the underlying forwarding devices. The southbound interface allows for control of the devices, forwarding operations, and other services [5]

The function of the data plane in a SDN controlled network does not change fundamentally compared to a traditional network with a distributed control plane [4]. The main purpose of the data plane is to forward arriving datagrams from their respective input port to the correct output port as determined by the forwarding or flow tables.

Here we are also going to review main two protocol which are mostly used to develop SDN:

A. *ForCES [1] and 2) OpenFlow [2]*

1) ForCES: ForCES is under active development by the Transmission and Control Separation (ForCES) working group of the IETF since 2003. ForCES network element (ForCES NE) is divided into forwarding elements (FE) and control elements (CE) while the ForCES protocol is used to communicate between the two. Unlike the SDN architecture, this approach is still presents the connected entity (FE and CE) to the outside world as a single network element (ForCES NE). [1][7][8]
2) OpenFlow : The OpenFlow [9] switch specification describes the communication protocol for the infrastructure layer and the control layer. The controller uses a secure channel to communicate with the switch. OpenFlow packets are sent through

this channel. Latest version The OpenFlow protocol supports SSL encryption. The message types supported by OpenFlow are As Follows. [2][9]

a) Controller to Switch Message: This type contains a handshake, the output message of a packet to create a stream. It also deals with switch configuration, role configuration, configure asynchronous messages, and more. The controller starts a message exchange and sends it to exchange the established TCP connection switch and controller. This type of message may or may not require a response from the switch. [9]

b) Asynchronous Message: This type contains messages like packet_in to send a packet to the controller if the flow fails, flow is removed, port status or an error message. These messages are sent without the controller requesting them from the switch.[9]

c) Symmetric Message: It contains messages commonly used for handshakes, such as Hello, echo request, echo reply, and Experimenter. Symmetric messages are sent in both directions without prompting. [9]

Two interfaces shall be used by a controller that operates as a network operating system: the “southbound" interface to allow switches to connect with controllers, and the “Northbound” interface which provides an API for control of networks and higher level applications. [3][9]

III. SOFTWARE DEFINED NETWORKING IN IOT

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with software, sensors, and additional technologies for the use of linking and data exchange with other devices and systems over the internet.[10]

In simple words we can say, IoT is a very important technology that has become popular now a days. It allows us to connect normal things like TV, kitchen appliances, cars, and baby monitors and other home / office appliances, smart toys to the internet. This means that these things can talk to each other and to us easily. With the help of cheap computers, big data, the cloud, analytics, and mobile devices, objects can talk to each other and collect information without needing people to do it. In this super connected world, computers can keep track of and control how things interact with each other. The real world and the digital world work together.

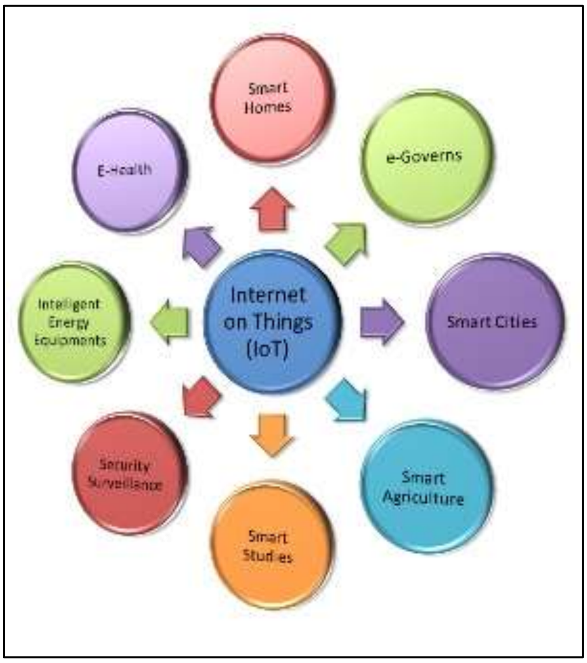

Fig. 2: General areas using IoT

IoT connected devices generate a ton of information, which makes it hard to keep track of and control them all. This is a problem for people who study and make these devices. The way networks are usually set up doesn't work well with all these different devices, and it takes a long time to make improvements. So, we need to change how the network and devices are set up to make the most of these internet-connected things. There are technologies, like Software Defined Networking and Network Function Virtualization that are really interesting and can help with this.[10]

Paper goal and approaches	Challenges / Future Scope	Authors	Year	Paper Number
SDN-IoT: SDN-based efficient clustering scheme for IoT using improved Sailfish optimization algorithm: A Software Defined Network (SDN) based efficient cluster model for the Internet of Things (IoT) using Improved Sailfish optimization	Optimization algorithms and fuzzy logic methods will be used to determine the best CH nodes for SDN-IoT for next future work.	Ramin Mohammadi1, Sedat Akleylek and Ali Ghaffari	2023	12

(ISFO) algorithm in the proposed model, IoT devices are clustered using the ISFO model. The ISFO model is installed on an SDN controller and is used to manage the Cluster (CH) node(s) of IoT devices. The performance of the proposed model was evaluated based on two scenarios (150 and 300 nodes). For 150 nodes, the ISFO model reduced energy consumption by approximately 21.42% compared to the LEACH algorithm. For 300 ISFO nodes, the LEACH-E algorithm decreased energy consumption by approximately 37.84% compared with the LEACH algorithm (approximately 27.23%). ISFO is a cluster protocol designed to achieve energy-efficient use in a SDN – IoT network. In ISFO, appropriate CHs are selected based on energy threshold and distance from CHs to member nodes. A comparison between ISFO and other models shows that ISFO model has a longer network life than other models. ISFO model improves the solution vectors and selects the best cluster based on various factors. ISFO model is tested with 2 scenarios including 150 or 300 sensor nodes according to different factors. Results show that ISFO model gets more live nodes than other models as well as SFO and also delivers more packages than others In general, ISFO model with 150 or 300 nodes has an improvement of 23.41%, while SFO model has an improvement of 28.79%.				
Software Defined Network as Solution to Overcome Security Challenges in IoT: The goal of this research to achieve a quality of service where the data among the devices should be as high as possible without degrading the performance. Team proposed application based model for better security and confidentiality compare to the traditional networks. An algorithm which is based on SDN and can be used to prevent different attacks in Internet of Things(IoT) environment. Cluster head selection process is proposed and cluster head is enabled & managed with SDN and control different security issues for particular domain.	Forthcoming research the proposed algorithm helps to analyses the result for different security attacks including neighbor attack, black hole, and other related attacks.	Fatma AL Shuhaimi1,Manju Jose2,Ajay Vikram Singh3	2021	11
Software Defined (SDN) Based Internet of Things (IoT) networks: This paper talks about how technology is changing the way we communicate with devices. Here SDN helps to make IoT devices easier to manage and more secure. Also illustrated benefits and challenges of combining SDN and IoT. It explains the different parts of this technology and how it has evolved over time.	One of challenges is existing ways of connecting devices and controlling traffic doesn’t work well for IoT. It can use up a lot of power and make the devices less efficient. It also makes it harder to keep the network secure from attacks.	S. Bîrleanu, M. Preda, C. Răcuciu	2021	14

Finally, it mentions some problems like secure connection, traffic control, energy, cost etc that still need to be solved in this area. As per analysis here different groups are trying to come up with a standard way of doing things, but they haven't found a concrete or perfect solution yet.	Frameworks that fully integrated with IoT-SDN are one of major challenge.			
SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic: In this research, team proposed architecture for intelligent and efficient management during COVID-19 of the smart industry considering. Moreover, the article presents the effective SDN-enabled layer, such as data, control, and application with any remote location it's easy to monitor IoT application. Here team proposed for managing IoT Sensor data using Network functions virtualization (NFV) and SDN convergence that gives an efficient control method. Team compares different architectures with their proposed system and summarized performance evaluations upon appropriate simulation setup and environment that verifies proposed system model able to provide enormous automation with security and privacy within the networking system that will make the industry 4.0 application efficient and reliable in order to effectively manage the pandemic situation	Data Security, Data capturing and monitoring, Time-Management, Energy consumption are various challenges explained in this paper with relative solutions In future to achieve more security using the inclusion of distributed Block chain technology.	Rahman, Anichur, et al	2021	15
An Ontological Security Framework To Secure The SDN Based IoT Networks Utilizing the core attributes represented by SDN, they provide ontology-based security architecture. In their security architecture limits access to independently verifiable IoT devices through the network. Secure the flows in IoT network infrastructure by adding an additional layer and providing a lightweight protocol to verify IoT systems. This advanced strategy to protect IoT networks, including IoT device authentication, and enabling approved flows, can help secure IoT networks against malicious devices and threats. In sort, they proposed a standard technical architecture for monitoring and remediation of IoT application pipelines and technology assets using IoT security domains ontology. The proposed module will be physically implemented and evaluated in the light of general overhead cost and resource consumption in the future.	For future work suggested module will be physically introduced and assessed in the context of general overhead costs and resource consumption	Hossain, Nazmul, Md Zobayer Hossain, and Md Alam Hossain	2021	17
Software-Defined Networks (SDNs) and Internet of Things (IoTs): A Qualitative Prediction for 2020: This paper is about looking at how people communicate with different things from 2010 to 2016. It also talks about new technologies like the Internet of Things (IoT) and Software-Defined	Handle battery power and Bandwidth consumption Need improved solution for denial of services attack and man in middle attack	Sahrish Khan Tayyaba, Munam Ali Shah, and et. All	2016	13

Networking (SDN), and how they could change the way we live in the future. Also provided Comparison Of Existing Sdn Based Management Solutions For Iot and explain descriptive summary of important SDN-IoT solution Frameworks The paper compares different ways of using SDN for the IoT and discusses the advantages and challenges. It also makes some predictions about what the world might be like in 2020.				

Table 1: Implemented work analysis in IoT using SDN

IV. CONCLUSION

After a critical situation of COVID-19 pandemic the use of IoT is increases rapidly to develop smart ecosystem. The way of communication with an entity in outer environment is changing, becoming smart and is connected with the help of IoT Applications. IoT applications producing large amount of data and it's critical for programmability, security, management of data and alertness is challenge for developers. The SDN control plane and data plane are decoupled, which hide the high-level implementation of the low-level forwarding devices and is very good platform to implement futuristic IoT Applications.

REFERENCES:

[1] A. Doria, J. Hadi Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal, and J. Halpern. Forwarding and Control Element Separation (ForCES) Protocol Specification. RFC 5810 (Proposed Standard), March 2010.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2):69–74, 2008.

[3] Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks, IEEE Communications Surveys & Tutorials · January 2014, DOI: 10.1109/SURV.2014.012214.00180

[4] K. Benzekki, A. El Fergougui and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): a survey," Security and Communication Networks, vol. 9, no. 18, pp. 5803-5833, 2016.

[5] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," arXiv.org, 2014. [Online

[6] Alexander Nunez, Joseph Ayoka, Md Zahidul Islam, Pablo Ruiz, A Brief Overview of Software-Defined Networking, eprint arXiv:2302.00165,2023,DOI: 10.48550/arXiv.2302.00165

[7] S.Hassas Yeganeh and Y. Ganjali. "Kandoo: a framework for efficient and scalable offloading of control applications". In Proceedings of the first workshop on Hot topics in software defined networks, HotSDN '12, pages 19-24, New York, NY, USA, 2012. ACM

[8] A. Doria, J. H. Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal, and J. Halpern. "Forwarding and Control Element Separation (ForCES) Protocol Specification". RFC 5810 (Proposed Standard), Mar. 2010.

[9] Pritesh Ranjan and et all, A Survey of Past, Present and Future of Software Defined Networking, Profile image of International Journal of Advance Research in Computer Science and Management Studies [IJARCSMS], Volume 2, Issue 4, April 2014, ISSN: 2321-7782 (Online)

[10] Tayyaba, Sahrish Khan, et al. "Software defined network (sdn) based internet of things (iot) a road ahead." Proceedings of the international conference on future networks and distributed systems. 2017, https://doi.org/10.1145/3102304.3102319

[11] Software Defined Network as Solution to Overcome Security Challenges in IoT

[12] Mohammadi R, Akleylek S, Ghaffari A. 2023. SDN-IoT: SDN-based efficient clustering scheme for IoT using improved Sailfish optimization algorithm. PeerJ Computer Science 9:e1424 https://doi.org /10.7717 /peerj-cs.1424

[13] Sahrish Khan Tayyaba, Munam Ali Shah, Naila Sher Afzal Khan, Yousra Asim, Wajeeha Naeem and Muhammad Kamran, "Software-Defined Networks (SDNs) and Internet of Things (IoTs): A Qualitative Prediction for 2020" International Journal of Advanced Computer Science and Applications(IJACSA), 7(11), 2016. http://dx.doi.org/10.14569/IJACSA.2016.071151

[14] S. BÎRLEANU, M. PREDA, C. RĂCUCIU, Scientific Bulletin of Naval Academy, Vol. XXIV 2021, pg.103-110.

[15] Rahman, Anichur, et al. "SDN–IoT empowered intelligent framework for industry 4.0 applications during COVID-19 pandemic." Cluster Computing (2021): 1-18.

[16] Ja'afreh, M., Adhami, H., Alchalabi, A.E. et al. Toward integrating software defined networks with the Internet of Things: a review. Cluster Compute 25, 1619–1636 (2022). https://doi.org/10.1007/s10586-021-03402-4

[17] Hossain, Nazmul, Md Zobayer Hossain, and Md Alam Hossain. "An Ontological Security Framework to Secure the SDN based IoT Networks." American Journal of Agricultural Science, Engineering, and Technology 5.1 (2021): 4-18. DOI: https://doi.org/10.5281/zenodo.4701562

[18] Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). Computers 2020, 9, 8. https://doi.org/10.3390/computers9010008