ARCHITECTURAL OVERVIEW 0F SOFTWARE DEFINED NETWORKING AND CHALLEGES IN IoT ENVIRONMENT – A COMPREHENSIVE STUDY

Vidhi S.kakani[1] , Pallavi B. Shinde[2] , Siddharth V. Bora[3] ,Prof. Mohit K. Popat [4]

[1]*Student , Computer Science And Engineering, J.D.I.E.T, Maharashtra, India,* ***vidhikakaniytl@gmail.com***
[2] *Student , Computer Science And Engineering, J.D.I.E.T, Maharashtra , India,* ***pallavishinde38@gmail.com***
[3]*Student, Computer Science And Engineering, J.D.I.E.T, Maharashtra, India,* ***siddharth191299@gmail.com***
[4] *Assistant professor, Computer Science And Engineering, J.D.I.E.T, Maharashtra, India,* ***mohit.popat @rediffmail.com***

Abstract

*Internet of Things (IoT) and Software Defined Network (SDN) are two emerging technologies. Internet of things (IoT) facilitates billions of devices to be enabled with network connectivity to gather and exchange time period information for providing intelligent services. It is imminent technology grabbing industries and research attention with a fast stride. Currently, more than 15 billion devices are connected to the net and this range is expected to reach up to 50 billion by 2020. Unfortunately, traditional network technologies like enterprise networks and classic timeout-based transport protocols aren't capable of handling such requirements of IoT in an economical, scalable, seamless ,and cost-effective manner. Traditional networking infrastructure consists of different networking devices such as switches, routers, and intermediate devices, in which application-specific integrated circuits are installed to perform dedicated tasks. Therefore, the devices are pre-programmed with different complex rules (i.e. ,protocols), which cannot be modified in real-time, to perform the dedicated tasks .On the other hand, a Software Define Network (SDN) provides a centralized and programmable control and management for the underlying network without changing existing network architecture***.*** *The SDN provides flexibility and programmability within the IoT network without disturbing underlying design of existing implementations. In this respect, we provide a comprehensive survey of different SDN based technologies, which are useful to fulfil the requirements of IoT, from different networking aspects — edge, access, core, and data centre networking . In these areas, the utility of SDN-based technologies is discussed. We also present a synthesized overview of comparative analysis of the existing solutions of SDN based IoT implementation provides a straightforward and concise view of the emerging trends.*

Index Terms: *SDN, IoT, SDN Architectur,Integration of SDN/IoT, Challenges in IoT Environment*

--- *** ---

1. INTRODUCTION

The emergence of new technologies and communication networks offer new connectivity scenarios among every physical object. Machine-to-Machine (M2M), Device-to-Device (D2D), Vehicle-to-Vehicle (V2V), wireless sensor network, actuators, smartphone, embedded devices and even connections among infrastructures are developing new connectivity scenarios. Moreover, these devices will be allegedly connected to the net and can ultimately create a heterogeneous system of interconnected objects; called the Internet of Thing (IoT), and in broader sense Internet of Everything (IoE). Internet of Things (IoTs) is an emerging technology which enables smart ecosystem leveraging heterogeneous technologies. Generally, physical devices equipped with RFID tags, actuators, wireless sensors, and/or wireless communication devices are connected to the Internet to form IoT network Internet. IoT also facilitates billions of devices to be enabled with network connectivity to collect and exchange real-time information for providing intelligent services. Thus, IoT permits connected devices to be controlled and accessed remotely within the presence of adequate network infrastructure. The most attracted technologies in this domain are Software Defined Networking (SDN)

SDN is an emerging technology can which will meet the requirement of current IoT requirements of heterogeneity and flexibility. It provides a centralised control and global view of the entire network. Therefore, the main objective of the SDN is to separate the control plane from the data plane involving the forwarding devices. As a result, adequate control logic can be implemented on the physical devices, depending on the application-specific necessities in time period. in a generalized view, SDN consists of three layers — infrastructure, control, and application. additionally to the layer-wise design of SDN, multiple applications programme interfaces (APIs) conjointly exist — north, southbound, eastbound, and westbound. The control plane is decoupled from forwarding plane and communication between two planes is finished through Apis e.g. OpenFlow. data plane consists of dumb forwarding devices i.e. router & switches that solely forward information on the controller instructions. The controller acts as a brain and manages the network by having a worldwide view of the network. The client desires square measure abstracted over application layer which is communicated to the controller via northbound Apis.

2. SDN Architecture

SDN may be a layered architecture, consisting of 3 basic layers; application/services layer, controller layer (control plane), and data plane layer known as forwarding layer consisting of forwarding devices. These SDN layers communicate with every other via open apis known as northbound Interface (NI) API and Southbound Interface (SI) API. The SDN controller provides programmability and versatile management for flow forwarding state within the data plane by having a worldwide view of the network SDN can facilitate high data transmission, spectral efficiency, resource allocation and network management for the IoT devices for fulfilling growing need of the client demands. IoT conjointly follows a layered architecture comprising of 3 main layers; Perception layer: consists physical objects and sensing devices, Network layer: responsible for sending data from physical objects to the gateway/edge of the network, and Application layer deals with application/services of the user demand. IoT is solely the point in time when a lot of things or objects were connected to the Internet than individuals. IoT devices are used to sense, collect, process, infer, transmit, notify, manage, and store data; however, its boundaries aren't restricted to sensor devices solely. Billions of connected devices, thousands of communication protocols and network architectures are contributing in IoT creating complexity and inoperability. the overall architecture for SDN is shown in Fig. 1

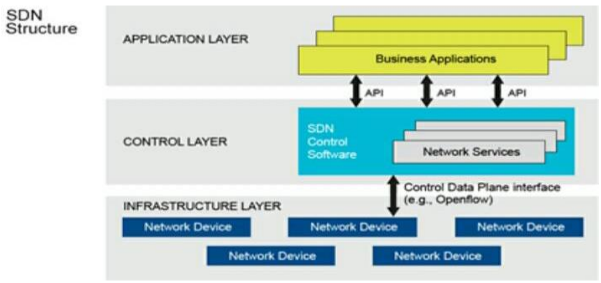

Fig-1: SDN Architecture

2.1 SDN architectural components

SDN is a layered architecture, consisting of 3 basic layers; application/services layer, a controller layer, and data plane layer known as forwarding layer consisting of forwarding devices. These SDN layers communicate with one another via open APIs known as northbound Interface (NI) API and south Interface (SI) API.SDN layered components are represented below:

SDN layered components are described below:-

- *Application layer (AP):* the application plane conjointly called management plane contains applications that leverage the functions offered by the Ni to implement network control and operation logic. Essentially, a management application defines the policies, which are ultimately translated to southbound-specific instructions that program the behaviour of the forwarding devices installed within the forwarding devices by the SDN controllers implementing the southbound protocols.

- *Control Plane (CP):* control plane is the decoupled entity from the distributed forwarding devices and logically centralised on a server. CP programs the forwarding devices through southbound interfaces. CP defines rules/instruction set for forwarding devices therefore control plane is the __network brain‘‘ and all control logic rests within the applications and controllers, which form the control plane.

- *Data Plane (DP)/Forwarding Plane*: Forwarding devices (routers, switches, gateways etc.) are interconnected through a physical medium like wireless radio channels or wired cables. And defined a physical interconnection In a a networkIn addition to the layer-wise architecture of SDN, multiple application program interfaces (APIs) conjointly exist —northbound, southbound, eastbound, and westbound.

In addition to the layer-wise architecture of SDN, multiple application program interfaces (APIs) also exist — northbound, southbound, eastbound, and westbound.

SDN application program interfaces (APIs) are described below:-

- *Northbound Interface (NI):* The interaction between application AP and control plane is provided through Ni. The Network OS (NOS) facilitate application developers to coordinate through these Ni Apis. Typically, an NI Apis abstracts the low-level instruction sets and implementation of forwarding devices. so far Ni Apis isn't well studied Generally, RESTFull Apis are used as an interface between applications and control plane.

- *Southbound Interface (SI):* Southbound interfaces provide a communication protocol between CP and forwarding device though the SI instruction set. Well established SI protocol help controller in programming forwarding devices and formalise rules for interaction between the two planes (CP & DP). Some examples are OpenFlow , Forwarding and Control Elements (ForCES) , Protocol-oblivious forwarding (POF)

The *eastbound* and *westbound* APIs are responsible for interfacing between multiple controllers, so that they can take coordinated decisions.

The SDN controller provides programmability and flexible management for flow forwarding state in the data plane by having a global view of the network. SDN can facilitate high data transmission, spectral efficiency, resource allocation and network management for the IoT devices for fulfilling growing need of the customer demands. IoT is simply the point in time when more things or objects were connected to the Internet than people. IoT devices are used to sense, collect, process, infer, transmit, notify, manage, and store data; however, its boundaries are not limited to sensor devices only. Billions of connected devices, thousands of communication protocols and network architectures are contributing in IoT creating complexity and inoperability.

3. SDN Based IOT Architecture

IoT and SDNs are two distinct technologies. IoTs mainly consist of sensing devices attributing different communication networks; whereas SDN is associated with network routing and act as an orchestrator for network level management. SDN is a separation between the control plane and data plane and provides vendor independence, whereas IoT is layered architecture consisting of multiple technologies at each level. Hence IoT can leverage benefits from SDN control plane due to the fact, SDN promise to hold the traditional network with new service demands. In this section, an architectural detail of SDN and SDN enabled IoT is presented.

In a heterogeneous network like in IoT, where diverse technologies are interplaying and exchange information. In such networks, the management becomes very complex. The configuration, reconfiguration, resource allocation and even the pattern of intercommunication becomes extremely difficult. SDN, because of its decoupled nature, separate control plane from data plane offer programmability and management from a centralised server having a global view of the network status. SDN play a vital role in the management of such heterogeneous network. M2M communicating devices are managed through leverage SDN control plane in . The proposed framework is a two-tier architecture consisting of control plane and data plane and devices are IP enabled. These devices are populated with routing table as in the SDN-enabled switches. Controller has a complete view of the network. If a breakdown observed between devices and gateways, the controller does network reconfiguration. The communication between devices is used three reference points Mx, Gx, Gnx. The device kept its information and its neighbour information in the form of a file such that any change in the file is manipulated on controller instruction.

In this Section, we present some of the key requirements of IoT applications, which can be potentially fulfilled by SDN technologies to realize the concept of software-defined IoT.

3.1 Network Management: Network management is an important factor for managing such an enormous collection of devices and the huge information generated by them. Thus, adequate technologies are required to distribute and control the traffic flows in the network for load balancing and minimization of network delay. Such requirements can be fulfilled by the SDN-based technology, as it leverages the global view of the network in a centralized manner. Thus, the SDN-based technologies can be applied for IoT network management such as load balancing, fine-grained traffic forwarding, and improved bandwidth utilization content goes here.

3.2 Energy Management: Huge number of data centers will be involved in processing the huge volume of data collected from billions of devices in IoT. Therefore, huge amount of energy will be consumed to power the data centres. Consequently, smart energy management systems also need to be ensured for energy-efficient data centre networking. In SDN-based data centre networking, traffic can be mapped to the adequate servers efficiently. Thus, the devices at the data canter can be switched ON/OFF dynamically, depending on the requirements, which, in turn, establishes an energy efficient data centre networking. This feature can be used from the perspective of IoT network.

3.3 Network Function Virtualization: The concept of network function virtualization (NFV) allows the devices to perform multiple tasks, while changing their functions in real-time, depending on application-specific requirements .Due to these parathion of the control plane from the physical devices from the perspective of SDN, NFV is made easier to the Internet service providers.

Consequently, SDN-based approaches play an important role in realizing the concept of NFV in a large scale IoT network

3.4 Accessing Information from Anywhere: As discussed in the above points, billions of devices are envisaged to be connected in IoT. Further, the owners of the devices should be able to access them from anywhere and at any time, so that they are able to control and change the functions of their devices, depending on requirements, in a seamless manner . It is possible to control such devices in the network with the help of SDN-based technologies, while preserving the privacy of others

3.5 Resource Utilization: Under-utilization or over-utilization may decrease the network performance, which, in turn, minimizes the network utility. Therefore, efficient mapping of user's requests is required for improved resource utilization to maximize the utility of the network. In SDN, flow-rule based traffic forwarding helps in improved network resource utilization. Consequently, request from multiple users can be forwarded through the desired path according to the flow-rules decided by the SDN controller.

3.6 Security and Privacy: Securing the devices and network is an important consideration for allowing multiple devices, vendors, and users to participate in a single platform .For example, a set of devices is associated with a particular service provider. Therefore, the control of such devices should only be allowed to the particular service provider. Moreover, other service providers should not be able to get access to the data generated by the devices although they have the data. The general scenario of iot is shown in Fig. 2.

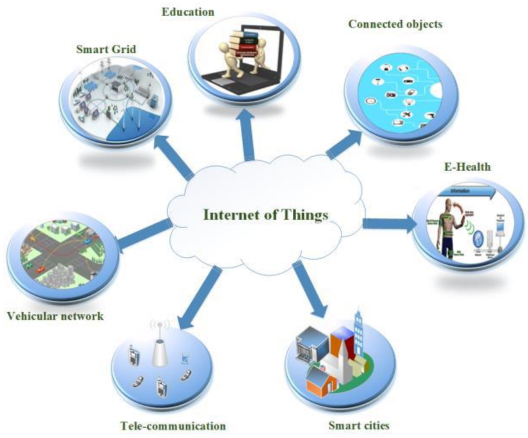

Fig. 2. Overall IoT scenario

4. Security Challenges in IoT Environment

Wide distribution of IoT nodes and private nature of data that are collected and transferred by IoT devices made security a major challenge. In this section, we are briefly looking at major security challenges that exist in IoT environments.

4.1. Authentication

In IoT domain, authentication allows integration of different IoT devices that are deployed in different contexts. Authentication process involves authentication of routing peers that involve in transferring data as well as authentication of the source of data route (data origin node) [7]. Efficient key deployment and key management is a challenge in IoT devices authentication. Any cryptographic key

Generation and key exchange should not cause a major overhead on IoT nodes . Moreover, in the absence of a guaranteed Certificate Authority (CA), other mechanisms are required for validating cryptographic keys and ensuring integrity of key transfer.

4.2 Authorization and Access Control

Authorization involves specification of access rights to different resources while Access Control mechanisms should guarantee access right of only authorized resources. Each and every IoT node may only support limited mechanisms for access verification which could be different from other connected objects to the same node. Therefore, deployment and management of a variety of authorization and access control mechanisms which are tailored to different nodes capabilities is a challenge in a heterogeneous IoT network.

4.3 Privacy

Deployment of autonomous objects in IoT that sense people private information (such as health data) pose a new level of threat to individuals' privacy. Unlike conventional scenarios in which users have to take some actions (i.e. searching for a keyword or posting some data) to put their privacy at stake, IoT nodes are collecting people's private data without them even noticing. Existing mechanisms are providing user centric privacy, content oriented privacy or context oriented privacy. However, IoT networks are naturally contains autonomous nodes that collect information and require object-oriented privacy models. Moreover, majority of privacy regulations mandate keeping users informed about how their private data is managed and administered. Identifying nodes that may have access to passively collected users' private information is a huge challenge in heterogeneous IoT networks.

4.4 Secure Architecture

Building an architecture that overcomes aforementioned security challenges in IoT environments is not trivial. Any IoT architecture should not only address previously mentioned security issues but deal with challenges that are introduced by deploying IoT devices over Software Defined Networks (SDN) and cloud infrastructure. Majority of SDN and cloud environment security issues would inevitability inherited to underlying IoT sensors. Moreover, Complexities that involve in securely connecting object-oriented IoT networks to data-oriented cloud infrastructures would introduce many unprecedented security challenges [1]. Finally, detection of malicious traffics rerouted over networks with different natures (i.e. SDN, Cloud and IoT) and hunting for malicious actors is a very challenging task for existing intrusion detection and prevention systems administered. Identifying nodes that may have access to passively collected users' private information is a huge challenge in heterogeneous IoT networks

5. CONCLUSION

The new era of IoT is changing the way of communication between human and machines. Now thinking are getting beyond the connectivity among every physical object with the Internet. However, IoT have a lack programmability, security and data management to meet the need of customer requirement, it is highly anticipated to use programmability, and centralized control for IoT management and integration with SDN is required. In this paper, we also provided a detailed overview of existing SDN-based technologies in the context of IoT applications ,in order to offer seamless, cost-effective and reliable service delivery to users. Additionally, we presented some of the challenges in IoT environment.

In sum, the integration of SDN schemes in IoT is envisioned to be useful for evolving scalable, energy-efficient, and cost effective IoT architecture.

ACKNOWLEDGEMENTS

We would like to sincerely thank all the authors and reviewers for their efforts toward the success of this special issue.

REFERENCES

[1] Sahrish Khan Tayyaba, Naila Sher Afzal Khan, Wajeeha Naeem "Software-Defined Networks (SDNs) and Internet of Things (IoTs): A Qualitative Prediction for 2020," Vol. 7, No. 11, 2016

[2] H. Farhady, H. Lee, and A. Nakao, "Software-Defined Networking: A survey," Computer Networks, vol. 81, pp. 79–95, Apr. 2015.

[3] Sahrish Khan Tayyaba , Munam Ali Shah, "Software Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead," ICFNDS '17, July 19-20, 2017

[4] Mauro Conti1, Ali Dehghantanha, Katrin Franke3, Steve Watson, " Internet of Things Security and Forensics: Challenges and Opportunities," http://doi.org/10.1016/j.future.2017.05.048

[5] Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. Future Generation Computer Systems, 72, 327–338. http://doi.org/10.1016/j.future.2016.06.003

[6] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25–37. http://doi.org/10.1016/j.jnca.2017.02.009

[7] Giaretta, A., Balasubramaniam, S., & Conti, M. (2016). Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks. IEEE Transactions on Information Forensics and Security, 11(4), 665–676. http://doi.org/10.1109/TIFS.2015.2505632