International Journal of Core Engineering & Management
Volume-5, Issue-8, November-2018, ISSN No: 2348-9510

SOFTWARE DEFINED NETWORKS (SDN) BASED WIRELESS NETWORK SECURITY FOR CLOUD INTERNET OF THINGS (IOT)

Sai Krishna Reddy Mudhiganti

Abstract

Nowadays, Internet of things (IoT) is imminent technology which enables billions of devices connected with network to interchange real-time information. With development of smart devices related to Internet, network security is hardest challenges for IoT. Maintaining and securing in heterogeneous and large scale networks is a challenging chore. Thus, Software Defined Networking (SDN) presents numerous opportunities and provides prospective to beat those security challenges. In this paper, SDN framework was proposed for presenting network security in gateways of IoT. An experimental validation of framework is focuses on security problems among all other challenges and results in enforcement of security at network edge. Results of our evaluation shows SDN architecture model can efficiently and effectively meet the security challenges created by the network.

Keywords: Internet of Things, Software Defined Networks, Network Security.

I. INTRODUCTION

Currently, over seven billion customers in the world are linked to the Internet for browsing Web pages, accessing e-commerce services, sending and reading emails, sharing experience on social media and playing games. The wide-scale diffusion of the Internet has been the driving potency of an emerging trend, the utilization of such world-wide interaction infrastructure to allow machineries and smart stuffs to communicate, collaborate and create verdicts on real-world circumstances. This auspicious exemplar is recognized as the "Internet of Things" (IoT) and its progression goes hand-in-hand with the advancement of supporting technologies addressed to this novel hallucination of wireless interaction scenario, like wearable sensors, Wireless Sensor Networks (WSNs), NFC, actuators, FID, and Machine-to-Machine (M2M) devices. The word IoT was utilized for the initial time in the late 1990s by the entrepreneur Kevin Ashton, one of the inventers of Auto-ID Centre at MIT, represents to the connection of stuffs to the Internet by RFID tags (Madakam et al., 2015). The utilization of IoT allowed technologies discovers a great use for securing crucial infrastructure, like a bank, a stadium, an energy production infrastructure, a harbor or other community ambient. RFID or other identification technologies can detect if a person is authorized to stay within a restricted area.

Tewari and Gupta (2018) presents IoT Cross layer heterogeneous integration issues, I2NSF architecture(Hyun et al., 2018), an integrated Cloud-Fog architecture(Peng et al., 2018), CoAP in

an actual cloud connected IoT devices(Raza et al., 2017) and security challenges resultant from the exceptional characteristics of the IoT schemes are presented by Sha et al., (2018).Due to the federal verdict forming in SDN, controllers turn out to be the innate targets for attackers to advantage access to the whole network (Hoque et al., 2015).
Certain probable attacks comprise black-hole attack (Scott-Hayward et al., 2016), Denial of Service (DoS), deployment of spiteful controller utilization and world-wide network opinion alteration (Yoon et al., 2017).
SDN enable network managers to customize a given network as said by altering customer or corporate requests. In traditional networks, SDN decouples the control plane to logically federal control point named as controller. The devices in data plane, namedas switches, impose the forwarding functions according to the verdicts from controller (Dabbagh, et al., 2015). Control verdicts are stowed as flow-rules in switches' flow-tables. The switch-controller interaction is resulted utilizing Open Flow protocol. In terms of security, SDN replaces plans in firewalls with flow-rules at distinct switches and impose node-level security. In spite of the overhead specified benefits, SDN architecture itself can be subjected to diversity of security risks.
In this article, a security scheme for IoT based on SDN architectures was presents. The suggested security scheme was designed to found and secured for both wired and wireless network substructure. The main contributions of proposed system are given as follows:

- Utilize the SDN architecture to challenge security problems in IoT.
- Inspired by existing Network Access Control and security methods, a secured SDN-based architecture for the IoT was designed.

II. RELATED WORKS

Internet of Things (IoT) acts as an amazing role in altogether aspects of our day-to-day lives. It covers numerous fields comprising homes, automobiles, healthcare, industrial appliances, entertainments, sports, etc.

The IoT comforts certain daily actions, enriches the method persons communicate with the environs, surroundings and enhances our social contacts with other persons and stuffs. However, security services in an intra-domain and inter-domain and multi-granularity security service method was provided by Shang et al., (2017).
The notion of IoT outline requires recognizing a structure which synchronizes and controls processes existence conducted by numerous IoT elements (Ammar et al., 2018). This structure is a set of guidelines, protocols and regulations that organize the way of processing data and exchange messages between all involved parties (e.g. embedded devices, cloud, end-users).High level implementation of IoT applications and hide the difficulty of infrastructure protocols and IoT layered architecture presented in Khan and Salah (2018).
Al-Fuqaha et al., (2015)investigation the IoT in over-all, talk about numerous IoT architectures, IoT elements, market opportunities, standard utilization protocols, communication technologies, prime tackle and open investigation difficulties in the IoT zone. A short-lived

overview of the present IETF standards for IoT was provided by Sheng et al., (2013).
Privacy and security problems in IoT and Cloud Computing had a lot of consideration by the investigation community and advantage of their integration presented by Stergiou et al., 2018. In Yanget al., (2017), the authors surveyed the privacy and security problems in IoT from four different perspectives. Kumar et al., (2014) instructed the privacy and security problems in IoT at every layer known in the three layer architecture surveyed utmost of the security defects existing in IoT, ensued from numerous communication technologies utilized in WSNs.

Fremantle et al., (2017) revised the security and challenges problems of IoT middleware, where a great quantity of existing schemes inherits security possessions from the middleware outlines. Depending on the renowned security and privacy intimidations, writers scrutinize and assess the obtainable middleware methods and demonstrate how security is handled by every method (Mukherjeea et al., 2018).
In this paper, the proposed system was focused specially on the SDN environs, in which the controller is competent to assemble and analyse traffic statistics bangs from switches. Therefore, SDN based network security for IoT was proposed to identify the appearance of compromised devices in control plane utilizing Open Flow touches, i.e., the control traffic and provisioning security services over IoT network.

III. METHODOLOGY

3.1 Software Defined Network

SDN has emerged as a novelexemplar for enabling innovation in networking research and development. The data and control planes are decoupled; network intellect and state are logically centralized. A novel device named controller joins to the switch through a secured OpenFlow passage and copes this switch by means of the OpenFlow protocol. Three dissimilar planes namely management, control and data planes in the SDN architecture are exposed in Figure 1.
The controller can update,add and delete flow entries, both reactively in reply to packets and proactively with predefined guidelines. Moreover, SDN allowsquick response to security intimidations, grainy traffic filtering and dynamic security plans deployment. Table 1 demonstrates the sources of vulnerabilities in SDN framework.

3.2 Software defined network (SDN) based IoT architecture

In novel exemplar of SDN based virtualization, altogether IoT network elements are just forwarding devices without any intellect instilled in them which can control and onward information traffic. The whole network control and management operations exist in this software which is normally named SDN controller. SDN controller is viewed as the brain of whole network. SDN controller resides on manifold physically disseminated servers in an enormous cloud network. Moreover residing on manifold servers, SDN controller software be good to logically control the network in a federal way. The management and control planes are

appeared to be practical at the central position that reflects on whole span of network. This logical central control of the network will massively decrease the encumbrance of network machinists as it will evade configuration mistakes across the network which is relatively communal in today's networks. Open and standard interfaces are technologically advanced amongst the management, data and control plane that allow heterogeneous devices link to the network without any exertion.
The data plane is connected to the control plane through a southbound interface. Figure 2shows the SDN based IoTarchitecture.SDN controller consists of both control and management planes as separate layers. These control and management planes communicate with each other utilizing the northbound interface. The control plane likewise comprises the network operating scheme that controls the whole network as a unique logical unit.

3.2.1 Sensor Openflow Switches
IoT nodes are generally laid out in clusters with Cluster Head (CH) which is a resource sufficient device that communicates with IoT gateway.
To implement SDN methods the IoT nodes performing as relays or switching device play the role of sensor openflow switches. In contradiction of traditional network components over the Internet, IoT nodes are constrained in resources and require a lightweight openflow protocol for communication with low power devices.

3.3 **SDN security framework for IoT**
IoTscheme, huge Internet linked physical stuffs creates the bulk of information within few milliseconds whose processing, storage, mechanization and management is an intensive task. These strategies are potentially underneath threat owing to unbounded connectivity and interaction over wireless and wired transmission medium due to non-appearance of standard security protocol/architecture for IoTs. SDN is deliberated a powerful technology of having federal control over the data flow in the network and deliver a pre-emptive security strategy. IoT scheme turn out to be additional vulnerable to security hazards when they are watched from a federal controller as SDN based IoT network.
Our proposed IoT security architecture comprises three major blocks which are shown in Figure 3. The SDN edge node is a scattered computing substructure in which certain facilities are handled at the network edge. This is frequently completed for improving the efficiency of network, but it might too be executed for security and compliance reasons. This node has the capacity to performance as:

- An Open Flow-enabled switch so as to switch the dissimilar IoT gateways that are related. Moreover connectivity to aggregation and transportation networks is too delivered.
- Virtual machineries running dissimilar facilities, like an IoT database, where the measurements of the dissimilar sensors are stored for local processing.

To address the SDN based framework for providing security services to IoT network is

proposed. The framework consists of an IoT controller and SDN based security controller. Both of these controllers are situated in IoT gateway, which interconnects with IoT devices. Most generally utilized topology by IoT network is cluster based topology. Where cluster head copes a cluster of IoT devices.

The suggested SDN based IoT frameworks essentially comprise of three major modules.

- IoT Controller.
- SDN based Security Controller.
- Sensor Open flow Switches.

3.3.1 IoT Controller

An IoT controller performs as a central tier collecting data from IoT tactics and conveying it to utilization facilities for information analytics. It is responsible for informationassortment, aggregation and transmission of data to the back end. This is realized through a monitoring agent that collects data across the IoT network.

3.3.2 SDN based Security Controller

SDN based security controller is toolocated in the IoT gateway and run on topmost of the IoT controller. In order to realize security provisioning with the IoT network the SDN based security controller interacts with the IoT controller to monitor the flows. The security controller utilizes SDN techniques to provide different security services across IoT network. SDN based controller interminglesw with security utilization at the application plane to provision i) Privacy ii) Key Management iii) Trust. The network manager will impose security strategies by the security utilization through using custom API.

Security services at application plane will require status of the network nodes in IoT. Flow samples required by the network application are given by SDN based controller at the control plane which has the whole internationalopinion of the network. IoT controller SDN based have facilities which are executed as modules to provision security facilities across IoT network.

IV. DESIGN FLOW

4.1 Privacy Module

Step 1: IoT devices joining the network by delivering their request to the gateway which is composed by the IoT controller and passed on to the SDN controller which registers the device.

Step 2: Cryptographic credentials for confidentiality, integrity and Secure Multiparty Computation (SMC) is generated by the privacy application which is stored for a registering device.

Step 3: Encoded packets are sent from a device as a flow which is accounted by the SDN controller and along with privacy application. The calculated outcome over inputs from IoT device is then delivered to the back end utilization or information analytics perhaps introduced in a cloud or if wanted to the IoT devices for additional processing.

4.2 Key Management

Step 1: Device joints the network and gets registered.
Step 2: Key generation request is then initiated via SDN controller for a device from key management application.
Step 3: Crypto keys are generated and stored in the storage for a device.
Step 4: Generated keys are distributed to the devices using a key distribution algorithm.
Step 5:Key renewal and revocation process is carried out on the recommendations of flow analyser to revoke list of nodes. Keys stored in the storage are expired and any information encoded with the expired keys will not be considered valid.
Step 6:Keys generated are stored in the storage and distributed to the devices using a distribution algorithm.

V. RESULTS AND DISCUSSION

The results of proposed SDN-IoT has evaluated and compared the outcomes with existed LTE-WiFi, LWA-SA by using MATLAB simulator. The simulation results give the parameters energy efficiency, throughput and average delay. The simulation has performed by using SDN-IoTSMC algorithm. Table 2 displays the summaries of different IoT security technologies.

Efficiency

The performance evaluation of our proposed SDN-IoT is done by efficiency. Figure 4 demonstrates the efficiency of aggregation in relation with WiFi residence time. The more users reside inside the WiFi reportage, greater throughput is attained by SDN. Energy used by the network is proportional to the diameter of the network. By using SMC algorithm, network efficiency was found to be increased. Efficiency of SDN-IoT as 30, 35, 42, 52, 60, 70, 75, 80 and 95 was compared greater than existing algorithm. The amount of packets received by the base station from non-base station nodes is called through put.As number of nodes increases throughput will increase in all other data aggregation and SDN-IoT SMC algorithm data aggregation provides throughput as 95 Mbps. The proposed SDN-IoT provides maximum throughput when compared to existing algorithm (Liu et al., 2018).

Delay

End-to-End Delay denotes the time engaged for a packet to be transferred through a network from origin to endpoint.
Software Defined Networks (SDN) based wireless network security for cloud Internet of Things (IoT).
It is a general word in IP network watching and varies from Round-Trip Time (RTT). As the integer of nodes upsurges the end to end delay will decrease in all other data transmission and SDN-IoT SMC algorithm data transmission provides maximum end to end delay as 3.2, 3.5, 3.8, 4and 4.2ms was compared lower than LTE-WiFi, LWA-SA approach respectively for 100 nodes. Figure 5 illustrates the end to end delay time of the IoT application is considerably minimum in SDN-IoT. It also infers that under constant arrival, delay remains constant. The end to end delay

time of proposed SDN-IoT scheme is lower than that of LTE-WiFi scheme (Zhiqun et al., 2017).

VI. CONCLUSION

In this paper, the architectures of SDN-IoT and identify challenges in designing SDN in IoT was presented. Heterogeneity, scalability, interoperability, designing efficient routing protocols, security and privacy pose a greater challenge in SDN-IoT. The security challenges in SDN-IoT were also analyzed along with threat modeling. It is value talk about that the security challenges in SDN-IoT can be handled implementing the following strategies: proper trust relationship management, access policies enforcement in real-time based on the network and device behavior, dynamic traffic rerouting and network reconfiguration, application of cryptography, greater network intelligence and data analytics and sharing capacity, fault tolerance, auto system restoration and also achieved high throughput, less delay.

REFERENCES

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
2. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.
3. Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015). Software-defined networking security: pros and cons. IEEE Communications Magazine, 53(6), 73-79.
4. Fremantle, P., & Scott, P. (2017). A survey of secure middleware for the Internet of Things. PeerJ Computer Science, 3, e114.
5. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
6. Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2242-2270.
7. Hyun, S., Kim, J., Kim, H., Jeong, J., Hares, S., Dunbar, L., & Farrel, A. (2018). Interface to Network Security Functions for Cloud-Based Security Services. IEEE Communications Magazine, 56(1), 171-178. Jiang, H., Shen, F., Chen, S., Li, K. C., & Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. Future Generation Computer Systems, 49, 133-141.
8. Kar, J., & Mishra, M. R. (2016). Mitigating Threats and Security Metrics in Cloud Computing. Journal of Information Processing Systems, 12(2).
9. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems.82, 395–411.Kumar, J. S., & Patel, D. R. (2014).

10. A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).
11. Liu, Y., Kuang, Y., Xiao, Y., & Xu, G. (2018). SDN-Based Data Transfer Security for Internet of Things. IEEE Internet of Things Journal, 5(1), 257-268.
12. Luo, T., Tan, H. P., & Quek, T. Q. (2012). Sensor OpenFlow: Enabling software-defined wireless sensor networks. IEEE Communications letters, 16(11), 1896-1899.
13. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.
14. Mukherjeea, B., Wangb, S., Lua, W., Neupanea, R. L., Dunna, D., Rena, Y., & Calyamb, P. (2018). Flexible IoT Security Middleware for End-to-End Cloud-Fog Communication.
15. Future Generation Computer Systems, https://doi.org/10.1016/j.future.2017.12.031Nunes, B. A., Santos, M. A., de Oliveira, B. T., Margi, C. B., Obraczka, K., & Turletti, T. (2014).
16. Software-defined-networking-enabled capacity sharing in user-centric networks. IEEE Communications Magazine, 52(9), 28-36.
17. Peng, L., Dhaini, A. R., & Ho, P. H. (2018). Toward integrated Cloud-Fog networks for efficient IoT provisioning: Key challenges and solutions. Future Generation Computer Systems.https://doi.org/10.1016/j.future.2018.05.015
18. Raza, S., Helgason, T., Papadimitratos, P., & Voigt, T. (2017). SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. Future Generation Computer Systems, 77, 40-51.
19. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.
20. Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1), 623-654.
21. Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, 326-337.
22. Shang, F., Li, Y., Fu, Q., Wang, W., Feng, J., & He, L. (2017). Distributed controllers multi-granularity security communication mechanism for software-defined networking. Computers & Electrical Engineering, 1–19.
23. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6), 91-98.
24. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975.
25. Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems.https://doi.org/10.1016/j.future.2018.04.027
26. Wang, Y., Chen, H., Wu, X., & Shu, L. (2016). An energy-efficient SDN based sleep scheduling algorithm for WSNs. Journal of Network and Computer Applications, 59, 39-45.

27. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 4(5), 1250-1258.
28. Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, 49, 104-112.
29. Yoon, C., Lee, S., Kang, H., Park, T., Shin, S., Yegneswaran, V., & Gu, G. (2017). Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined
30. Networks. IEEE/ACM Transactions on Networking, 25(6), 3514-3530.
31. Zhiqun, H., Zhaoming, L., Shangjuan, L., Xiangming, W., & Hen, X. (2017). Performance analysis of LTE-U coexistence network with WiFi using queueing model. The Journal of China Universities of Posts and Telecommunications, 24(5), 1-7.

Tables

Table 1 The sources of vulnerabilities in SDN framework

Source of Vulnerability	Description
Application	An application accessing the resources provided by the SDN controllers
SDN controller	A machine that controls network devices
Network device	Devices in charge of traffic forwarding
Management console	A console for applications, controllers, and network devices; supports remote management tasks
Northbound interface	Communication channel between applications and the SDN controller
Southbound interface	Communication channel between the SDN controller and network devices
East/west interface	Communication channel between distributed SDN controllers
Management interface	Communication channel between the management console and applications, controllers and network devices in each plane

International Journal of Core Engineering & Management
Volume-5, Issue-8, November-2018, ISSN No: 2348-9510

Table 2 Summary of different IoT security technologies

References	Technologies	Limitations	Domain
Gubbi et al., (2013)	Cloud implementation using Aneka computing platform	Security and personality protection is a serious issue in Hybrid clouds.	Smart Environment.
Yao, Chen, and Tian (2014)	Lightweight no-pairing Attribute-based encryption (ABE) scheme based on elliptic curve cryptography (ECC)	Poor scalability Poor flexibility in revoking attribute	Single-authority Applications.
Jiang, Shen, Chen, Li, and Jeong (2015)	Revised secret-sharing scheme (Shamir's secret-sharing scheme)	It generates computational overheads that bring potential bottlenecks.	Data mining and Analytics.
Wang et al., (2016)	Generic IoT	Lacking proof for concept, not evaluated.	Authentication, security policy at security controller.
Luo et al., (2012)	Embedded devices/System	Processing slows down	Security Integrity.

International Journal of Core Engineering & Management
Volume-5, Issue-8, November-2018, ISSN No: 2348-9510

Figures

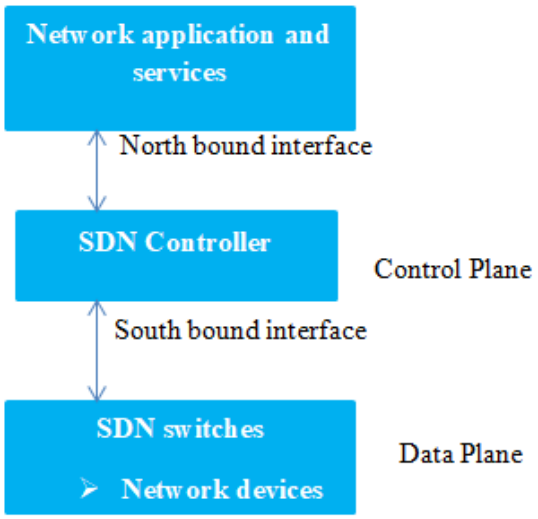

Figure. 1 SDN Architecture

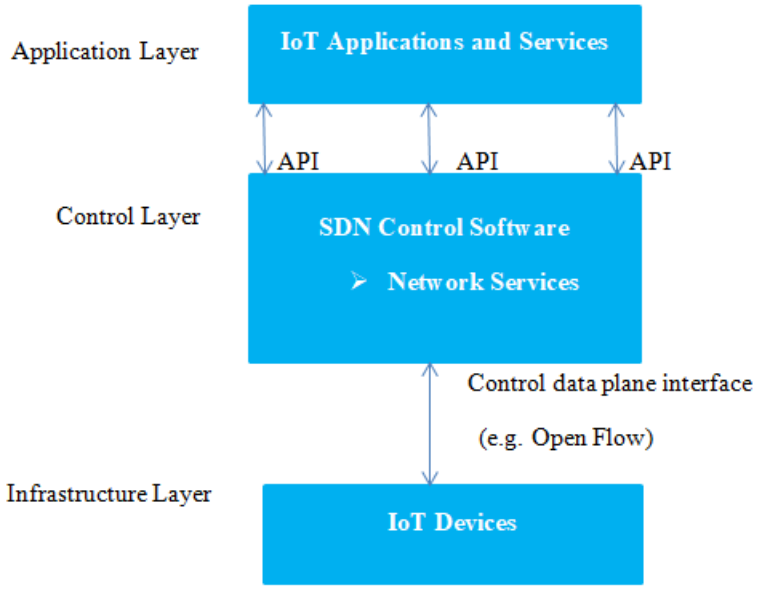

Figure. 2 SDN Architecture for IoT

International Journal of Core Engineering & Management
Volume-5, Issue-8, November-2018, ISSN No: 2348-9510

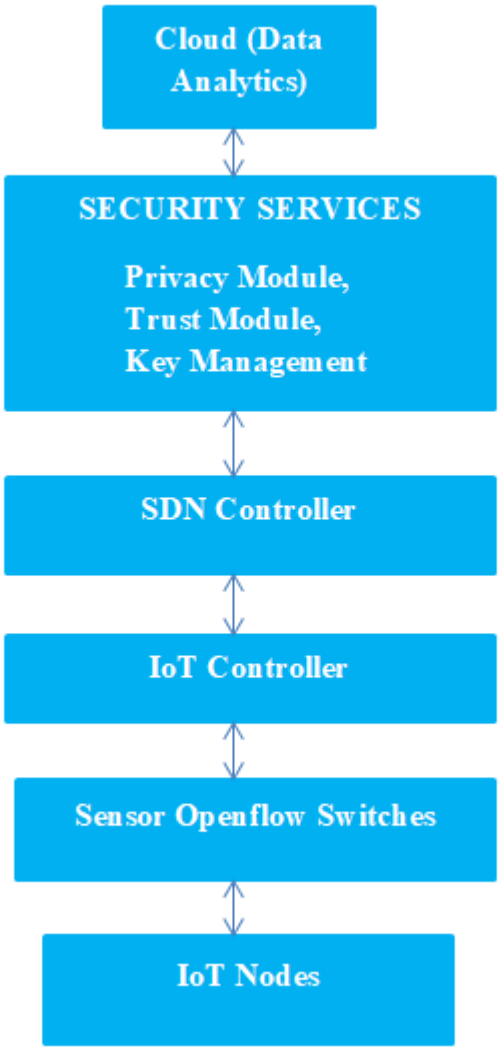

Figure. 3 Proposed SDN based security framework for IoT

International Journal of Core Engineering & Management
Volume-5, Issue-8, November-2018, ISSN No: 2348-9510

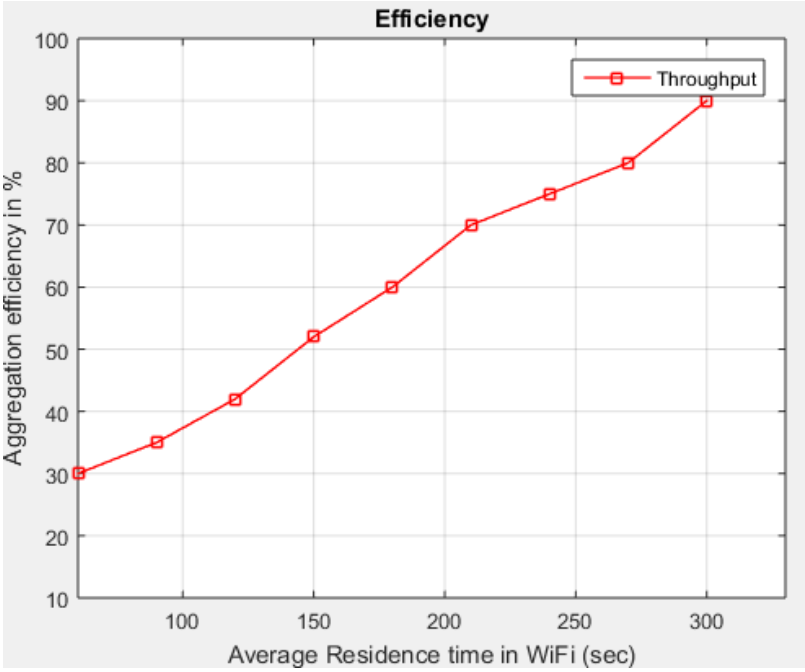

Figure. 4 Aggregation efficiency

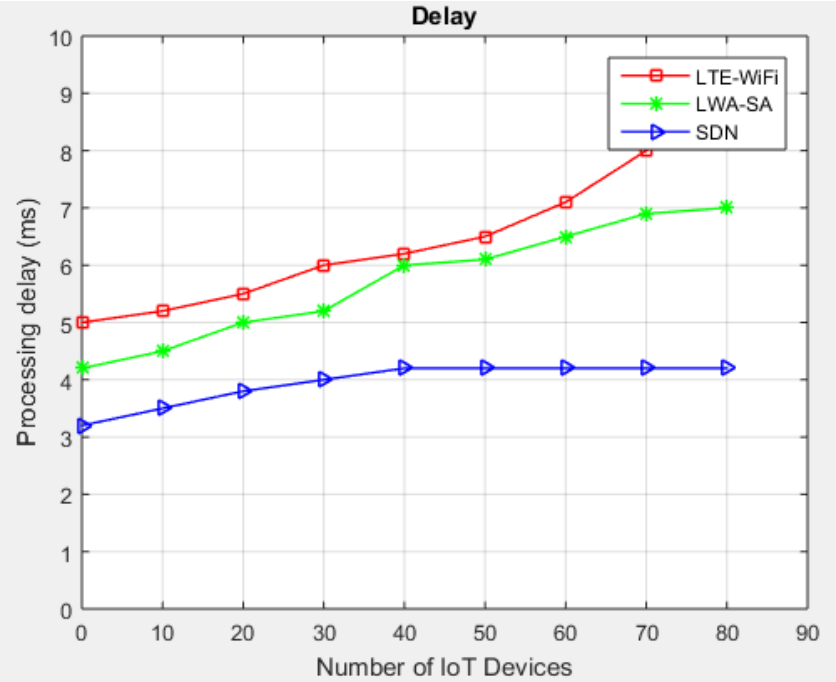

Figure. 5 Processing delay