Convergence of Software Defined Networking and Internet of Things for Supply Chain Environment

Arundhati V. Ubhad Department of Computer Engineering Smt Kashibai Navale College of Enginnering, Vadgaon Savitribai Phule Pune University Parikshit N. Mahalle Department of Computer Engineering Smt Kashibai Navale College of Enginnering, Vadgaon Savitribai Phule Pune University

ABSTRACT

Supply chains are widely used in todays world to meet up the requirementsofmarketsanduserdemands.Herethenewtechnology is being used which will integrate Internet of things and Software denednetworksothattraditionalsupplychainmanagementprocess can be enhanced. An application is developed that will maintain data transparency between retailer and manufacturer where manufacturer can continuously monitor the entire network activities . By integrating SDN and IoT, signicant quality of service improvements and greater efficiency is achieved which in turn lead to lower transport cost and reliable services to end user over a period of time.

Keywords

IoT, OpenFlow, SDN

1. INTRODUCTION

The Internet of Things concept is widely spreading these days and imposing various complicated requirements for the future networks specically to the internet. It also posses threats to the current network. In IoT , different devices are connected in a network through the internet, so network as well as device heterogeneity must be considered. The most basic essential requirement identied for IoT is Radio Frequency Identication (RFID). QR codes, Bluetooth, as well as digital watermarking can also be used for tagging of the things instead of RFID. Thus, IoT is the connection of several different components, heterogenous networks and the protocols which are being used as well as the environment in which they are running[7].

As the millions of devices are connected to the network, the complexity of connecting these millions of devices increases. Also, the networks has to nd these devices and connect with them and then route the trafc and make the rules about how each individual device will be used followed by monitoring each of these connections and the data that will be generated by them. So, Software Dened Networking comes into the picture and becomes important in the internet of things to avoid this growing level of complexity. SDN helps in nding and connecting these devices then route their trafc appropriately. Contrast to that with a single router we might have to write thousand lines of code to accomplish this but with SDN it can be handled with few mouse clicks. The value of Software-Defined Networks (SDNs) lies specially in their ability to virtualize the network, non-static network policy enforcement and dynamic decision making according to network. Also it has greater control over all the network entities. SDN also reduces the operational cost [4]. OpenFlow protocol is widely used with SDN concept and many new ideas are proposed in [10].

SDN proves to be promising for the future networks. Software dened networking has separated control and data plane. The SDN controller is centralized at one place managing whole network. SDN is designed basically to support the changing end users requirements. There are various switches present in the network. Each switch receives the command to be carried out but there are times when switch does not know how to handle the command and where to route it so the separated data plane asks the controller to take the appropriate action. OpenFlow controller introduces the considerable overhead using southbound protocol. Different studies are carried out on scalability issues [14] [15].

2. TRADITIONAL SUPPLY CHAIN MANAGEMENT

Supply chain management is the process of flow of goods and services which involves managing of all the activities from the point of origin to the point of consumption of goods and services. But there are some problems associated with traditional SCM, some of them are listed below. Problems associated with traditional supply chain management process:

(i)There is no direct communication between retailer and manufacturer.

(ii) Production of the product starts only when the product is purchased by the end user(customer).

(iii) Administration of products on the retailer end and as well as manufacturers warehouse cannot be done by the manufacturer.

(iv) Excess production of certain products requires storage, maintenance in the warehouse thus leading to the increased product cost to the end user(customer).

(v) Reordering cost increases if less products are produced.

Thus to overcome above stated problems we propose a mechanism which integrates SDN and IoT which will enhance supply chain management process.

3. RELATED WORK

[1] Vandana C.P,"Security improvement in IoT based on Software dened networking" explains the overview of the current state of the IoT with the security challenges like object identication, privacy and integrity, authentication and authorization and malware in IoT. Software-dened-networks concept along with the Softwaredened networks based IoT architecture is discussed. Also, the security mechanism based on the concepts of segment controller and gateway controllers are highlighted.

Eun Joo Kim, Jong Arm Jun, Nae-Soo Kim, The Method of Controlling Trafc Paths in IoT-based Software dened Network provides the method for conguring the data trafc paths in IoT based SDN and conguring function for each switch node constituting the congured data trafc paths. It also provides the terminal with path list information where the user can select the most appropriate path suitable for a service demanded by the user. Thus this over all activity enhances the performance and service quality.

[3] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and VijayMann, SPINX: Detecting Security Attacks in Software Defined Networks explains SPHINX - controller agnostic tool that takes advantage of the ow graphs to detect the security threats on network topology and data plane forwarding emerging within software-dened networks. SPHINX incrementally updates the ow graph and detects the attacks in real time that some controllers are vulnerable to.

[4]Y.Jararweh,M.AlAyyoub,A.Darabseh,E.Benkhelifa,M.Vouk, andR.Andy,Sdiot: a software dened based internet of things framework, proposes the framework for SDIoT exploiting the several software dened systems such as SDN, SDStore and SDSec. SDIoT solution accelerates and facilitates the IoT control and management operations. Also, the three main components of the proposed architecture i.e. physical layer, control layer and application layer are illustrated.

[5] Hai.Huang, Jiping Zhu, and Lei Zhang, An sdn based management framework for IoT devices, proposes a network management framework in which software-dened network is combined with IoT. The devices in the network can be managed and congured dynamically based on SDN. It also improves there conguration and exibility of devices and the proposed framework mainly focuses on M2M transactions. Thus, the authors addresses the integration solution between the IoT devices and SDN.

[6] Intidhar Bedhief, Meriem Kassarans Taouk Aguili, SDN-based Architecture Challenging IoT Heterogenity, authors showed how SDN and IoT are integrated to make the prot from their charactestics such as programmability and scalability. SDN architecture is mainly integrated to face network heterogenity and docker for device heterogeneity. Feasibility of the proposed architecture is tested and the connectivity between different devices is evaluated throughout managed SDN based network.

[7] Shiva Rowshanrad, Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary, A survey on SDN, the future of networking, presents the software-dened networks capabilities, de-

ployment, applications and the challenges faced giving the broader view of the concept. Also the brief introduction to the history of programmable networksanddifferentprotocolswhichareusedforcommunicationsuchasOpenFlow, XMPP, OnePk is given.

[8] Muhammad H.Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, A Comparison of Software dened network(SDN) Implementation Strategies ,presents the two types of SDN implementation strategies i.e. proprietary and open source. Author compares and comes out with some notable differences between them such as network control, feedback from physical layer to logical layer, stability and vendor support and standardization.

[9] Haopei Wang,Lei Xu, Guofei Gu FloodGuard: DoS Attack Prevention Extension inSoftware-А DenedNetworks, focuses on the reactive controllers and consequentsecurity threats against them. A defence framework for sdn networks known as oodguard which is scalable, efcient, lightweight and protocol independent is proposed in this paper to prevent data-to-control plane saturation. Floodguard system uses proactive ow rule analyser and proactive migration for preventing data-to-control plane saturation attack. Impact on bandwidth under different attack rates with and without oodguard is evaluated.

[10] Ola Salman Imad Elhajj Ayman Kayssi Ali Chehab, SDN Controllers: A Comparative study ,focuses on the control plane of the SDN architecture. A study is carried out on new controllers such as ONOS and Libuid based controllers are tested using Cbench, an OpenFlow testing tool in this paper. Also, the comparison of multiple controllers is carried out based on several different parameters and found that Open Daylight is a good choice as a full featured controller.

3.1 EVALUATION OF LITERATURE SURVEY

Existing System	PARAMETERS				
	Network Heterogeneity	Device Heterogeneity	Integrity	Security	
Security Improvement in IoT based SDN	NO	YES	NO	YES	
SDN- based architecture Challenging loT heterogeneity	YES	YES	NO	NO	
Empowering the Internet on things with SDN	YES	NO	NO	NO	
An SDN-based YES management framework for JoT devices		YES	NO	NO	
SDIOT: A software defined pased internet of things	YES	NO	YES	YES	

Fig. 1. Gap analysis table

Above table will help to understand and compare the existing systems and the proposed system by comparing the parameters in the system and marking the one which is not available in existing system. As stated above, parameters such as Network Heterogeneity, Device Heterogeneity, Integrity and Security are considered. Study of few exixting systems which uses these parameters (one or many) is done and compared this with proposed system and with this comparison it can be said that proposed system is efficient to use.

4. MOTIVATION

Existing networking architectures has decentralized network control and hence fails to have the complete network view and it also requires high level of expertise as it is vendor specic. Also, it is time consuming when it comes to adding or removing any particular device in a network. Motivated by this problem, Software dened networking approach is designed to dynamically achieve the differentiated quality levels to different IoT tasks in heterogenous wireless networking scenario. As SDN can be applied to vast areas this work studies supply chain management process and problems associated with it like there is no direct communication between retailer and manufacturer, administration problems associated with products and many more. So making use of SDN in supply chain management process will try to enhance the supply chain management process.

5. MATHEMATICAL MODEL

Let us consider S be a Systems such that S= R, W, M, J, Es, Ds,

where

 $[1]R = \{R1, R2, R3, Rn | R is a Set of all RETAILER\}$

As there are n number of retailers giving service to customers with different products, this is an innite set.

[2] M= M1, M2, Mn- M is a Set of Manufacturer

[3]Es = {EREG, EENC, EDEC | ES is a Set of Encryption Service }

(i) EREG: This service uses the AES algorithm for Encryption of a le. There are three services provided by this ENCRYPTION SERVER. So this is a Finite Set as this contains limited attributes. Whenever a retailer is registered for the rst time in a network it will also get registered on the Encryption Server.

(ii) EENC: The requests from the retailer to the manufacturer are encrypted using AES.

(iii) EDEC: Manufacturer end decrypts the request received using the same keys and processes it.

[4] Ws = {W1, W2, Wn | Ws is a Set of product stock in Warehouse}

As this set has finite attributes, it is also Finite Set.

[5] $E= \{E1, E2, E3.En | E \text{ is a Encryption Keys} \}$ This set is used for storing the encryption keys. The requests from the retailer to the manufacturer are encrypted for security purpose. As there may be number of keys this is an infinite Set.

 $[6]D = \{D1,D2,D3Dn | D \text{ is a Set of decryption Keys}\}$ The manufacturer end decrypts the request received from retailer end and processes it.

[7] Ds ={It Is The Decryption Server}

Encryption / Decryption Server will be used for temporary storing

of data for the separate encryption decryption process.

[8] J= {Jacobs algorithm}

Jacobs Algorithm is used to check similarity of data. If data is similar its not replicated on server.

6. EXPERIMENTAL SETUP

Arduino Wemos microcontroller is used with LCD of 16 X 2 display. Ultrasonic and pressure sensors are applied to the Arduino Wemos microcontroller and deployed at retailer and warehouse end so that liquid and solid products stock is continuously monitored by manufacturing end.



Fig. 2. Arduino Microcontroller Board equipped with Sensors

Ultrasonic Sensor

The HC-SR04 is an active ultrasonic sensor and contains a transmitter and a receiver. It is used to measure the depth at which, objects are place. The ultrasonic sensor transmits high frequency sound waves and waits for the receted wave to hit the receiver. The distance is calculated based on the time taken by the ultrasonic pulse to travel a particular distance. There are different types of ultrasonic sensors with different transmission ranges and angles of detection.

Pressure sensor

It is the best low-cost, less power consumption smaller in size and more accurate sensing solution for measuring barometric pressure and temperature . BMP-180 can measure pressure range from 300 to 1100hPa with an accuracy down to 0.02hPa (0.17m) in advance resolution mode

7. SYSTEM AECHITECTURE

Figure shows the system architecture for IoT based SDN for supply chain management. The architecture is divided in three layers manufacturing end, data processing end and retailer end.

(i) Retailer end layer The ultrasonic sensor and pressure sensor are applied at retailer end and sense the input data of liquid and



Fig. 3. Arduino Microcontroller Board equipped with Sensors

solid products respectively. The pressure sensor gives the weight of solid product and ultrasonic sensor gives the quantity of leftover liquid. The sensor values are displayed at the LCD.



(ii) Data processing layer Here the sensor data is encrypted using AES encryption algorithm and the encrypted data is passed on to the manufacturing end.

(iii) Manufacturing end layer The encrypted data is decrypted here and thus manufacturer can monitor all the activities of retailer and have the complete view of network. Here the similarity of data received from retailer is checked using Jacobs algorithm. If data is similar then it is not replicated on database and stored only if data is unique. The software dened network functionality is used here which monitors the product stock and servers the retailer in less time.





The retailers can have both solid and liquid products for sell and manufacturer will have warehouse for storing its products. So ultrasonic sensor and pressure sensor are applied to the Arduino Wemos microcontroller board and it is placed at both the retailer and manufacturer warehouse end which will give real time the product stock. As software defined network is implemented at manufacturing end which decouples control and data plane it can monitor complete activities of retailer and manufacturer and take actions accordingly.

8. RESULTS

In this section screenshots are displayed.

(a)Here in figure 6 manufacturer can monitor complete activities of retailer and warehouse on his dashboard and monitor the product stock at both the ends and take necessary action.



Fig. 6. Manufacturing end dashboard where SDN is implemented

(b)Warehouse kit data is shown below in figure 7 and solid and liquid products are distinguished separately . Here warehouse owner can have look at the current stock of solid and liquid products.

S	Supply Chain Managment								
Kit Data									
	#	Solid Product Name	Current Stock	Liquid Product Name	Current Stock	Date			
	1	Wheat		Oil	2141.82	2018-07-21 14:05:42.0			
	2	Wheat	40	Oil	5	2018-07-21 13:41:14.0			
	3	Wheat	40	Oil	15	2018-07-21 13:39:58.0			
	4	Wheat	56.72	Oil	0.91	2018-06-15 11:06:00.0			
	5	Wheat	56.72	Oil	0.91	2018-06-15 11:06:00.0			
	6	Wheat	56.73	Oil	0.9099999999999966	2018-06-11 16:30:46.0			
	7	Wheat	56.69	Oil	104.55	2018-06-11 16:30:37.0			
	8	Wheat	56.73	Oil	103.64	2018-06-11 16:30:33.0			
	9	Wheat	55.57	Oil	36.37000000000005	2018-06-11 16:30:29.0			
	10	Wheat	54.54	Oil	181.82	2018-06-11 16:30:24.0			
	11	Wheat	55.57	Oil	145.45	2018-06-11 16:29:59.0			

Fig. 7. Warehouse kit data

(c)Retailer kit data is shown below in figure 8 and solid and liquid products are distinguished separately .

Supply Chain Managment										
Kit Data										
#	Solid Product Name	Current Stock	Liquid Product Name	Current Stock	Date					
1	Wheat	155.25	Oil	869.09	2018-06-11 16:19:47.0					
2	Wheat	155.20	Oil	869.09	2018-06-11 10:56:14.0					
3	Wheat	155.23	Oil	869.09	2018-06-11 10:55:01.0					
4	Wheat	155	Oil	869.09	2018-06-11 10:48:30.0					
5	Wheat	100	Oil	869.09	2018-06-11 10:44:07.0					
6	Wheat	227.09	Oil	-0.0	2018-06-08 20:09:50.0					
7	Wheat	224.08	Oil	-0.0	2018-06-08 20:08:51.0					
8	Wheat	225.16	Oil	-0.0	2018-06-08 20:08:32.0					
8	Wheat	225.16	Oil	-0.0	2018-06-08 20:08:32.0					

Fig. 8. Retailer kit data

9. CONCLUSION

Thus it can be concluded that SDN and IoT are two technologies that are very much dependent on each other. SDN technology can betterprepareanetworkforasuccessfulandrobustIoT.Itprovides the agility and elasticity which IoT demands. Moreover it provides and open environment for application developers to develop innovative

10. REFERENCES

[1] Vandana C.P, Security improvement in IoT based on Software dened networking ISSN:2278-7798.

[2] Eun Joo Kim, Jong Arm Jun, Nae-Soo Kim, A Packet scheduling Strategy for Heterogeneous Trafc of Internet of Things.In IEEE Conference 2016

[3] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and Vijay Mann. SPHINX: Detecting Security Attacks in Software Dened Networks. InNDSS15, 2015.

[4] Seungwon Shin ,Lei Xu , Sungmin Hong, Guofei Gu, Enhancing Network Security through Software Dened Networking (SDN).

[5] JY. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and R.Andy,Sdiot:a software dened based internet of things frame work, In Journal of Ambient Intelligence and Humanized Computing, 2015.

[6] H. Huang, J. Zhu, and L. Zhang, An sdn based management framework for iot devices, in Irish Sils Systems Conference 2014 and 2014 ChinaIrelandInternationalConferenceonInformationand-CommunicationsTechnologies (ISSC 2014/CIICT 2014). 25th IET. IET, 2013, pp. 175179.

[7] Intidhar Bedhief, Meriem Kassar ans Taouk Aguili, SDN-based Architecture Challenging IoT Heterogenity. In IEEE Conference-2016

[8] Shiva Rowshanrad, Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary, A survey on SDN, the future of netwoking Journal of advanced computer science and technology, doi: 10.14419/jacst.v3i2.3754.

[9] Muhammad H. Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, A Comparison of Software dened network(SDN) Implementation Strategies doi:10.1016/j.procs.2014.05.532.

[10] Haopei Wang, Lei Xu, Guofei Gu, FloodGuard: A DoS Attack Prevention Extension in Software-Dened Networks.

[11] Ola Salman Imad Elhajj Ayman Kayssi Ali Chehab, SDN Controllers: A Comparative study doi:10.1109/MELCON.2016.7495430.

[12] B. Eleonora, The internet of things vision: key features, applications and open issues, Computer Communications, 2014 - Elsevier, 2014.

[13] Shiva Rowshanrad , Sahar Namvarasl, Vajihe Abdi, Maryam Hajizadeh, Manijeh Keshtgary, A survey on SDN, the future of

netwoking Journal of advanced computer science and technology, doi: 10.14419/jacst.v3i2.3754.

[14] Muhammad H. Razaa, Shyamala C. Sivakumarb, Ali Nafarieha, Bill Robertsona, A Comparison of Software dened network(SDN) Implementation Strategies doi:10.1016/j.procs.2014.05.532.

[15] R. S. Braga, E. Mota, and A. Passito. Lightweight DDoS Flooding Attack Detection Using NOX/Open Flow. In Proceedings of the35th Annual IEEE Conference on Local Computer Networks, LCN, 2010.