INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2244 - 2248
RECEIVED : 15.04.2017 PUBLISHED : 06.05.2017
May 06, 2017

SECURITY IMPROVEMENT IN SOFTWARE DEFINED NETWORK USING ROUTING

[1]Premalatha.K, [2]Dr.S.Vasanthi,
[1]PG Scholar, Dept Of Information Technology, Sona College of Technology,
[2]Associate Professor, Sona College of Technology.

ABSTRACT

Security has become one of the major issues for data communication over wired and wireless networks. Proposed work is going to deal with a system which can automatically reconfigure the wireless network through membership track and routing. Along with the security which is introduced by making use of the dynamic routing also reduces the complexity of security implementation. With the evolving Internet of Things (IoT) technology, there is exponential growth in connectivity of heterogeneous devices to the internet. Securing such complex heterogeneous networks and their diverse access protocols is a real challenge leading to security risk. Integration of Software Defined Networking (SDN) with IoT can open up way for better security and access control mechanisms.

Keywords: IOT, Software Integration, Wireless Network.

1. INTRODUCTION

With the ever growing internet and interconnection among everything, the need for security is a demand of the time. Internet of things (IoT) [1] which connects every object or device with networking capabilities is an area of great concern related to security. Objects include home automation sensors, medical equipments, vehicular sensors, nuclear reactors and any life critical real time sensing devices [2]. This means that lack of security in IoT can pose a risk to human lives. IoT comprises of many heterogeneous devices which use diverse protocols. Each protocol follows different access mechanisms and security measures. But a unified security mechanism is still not in place in IoT. Conventional security approaches like Intrusion Detection and Prevention Systems (IDPS), Firewall are deployed at internet edge devices to protect from external attacks. But in case of IOT which is seamless and borderless network access control become more difficult. In this paper, we discuss the current state of IoT, security challenges in IoT. We describe the need for SDN and its evolution. Further we analyze architecture of IoT based on SDN. Finally a security framework has been proposed based on SDN-IoT architecture. Software Defined Networking (SDN) [3] which is the new intelligent networking paradigm provides opportunities to solve issues related to IoT. By applying SDN network configuration and management can be simplified significantly. Industries wide acceptance for SDN shows that SDN can establish a tighter connection within the ecosystem of IoT.

2. RELATED WORK

A formal definition of IoT is given “A world where physical objects are seamlessly integrated into the information network and where the physical objects can become active participants in business process.” as per [1]. Things can vary from physical objects to virtual objects which can be uniquely identified and connected via Internet. IoT consist of broad interconnection of several heterogeneous

networks like wired, wireless, adhoc etc, each comprising of heterogeneous devices and environment, protocols employed by them for connectivity. To make IoT feasible, a reliable adaptation to the common protocols used in the networking environment of IoT should be built. The role of IP for the Internet is significant and is proposed as the solution for IoT, especially with the advancement of IPv6. However, in real world, this approach has lot of challenges and drawbacks related to heterogeneity of the devices and networks involved in IOT. These objects and their protocols follow specific designs to meet specific user objectives. Trying to fit all these diversities of the objects into a common singular protocol is not a good option. On the other hand, the Software Defined Networking (SDN) approach focuses on the programmability of all network elements. In this process, the control and data plane are separated in routing devices whereby the intermediate network devices functionality has been simplified to mere packet forwarding. Due to the heterogeneity and complexity of the objects and networks in IoT, traditional authentication and authorization methods may not be applicable. Also the resource constrained devices in IoT restrict the usage of complex security mechanism. Some of the security challenges in the area of IoT are discussed.

3. PROPOSED SYSTEM

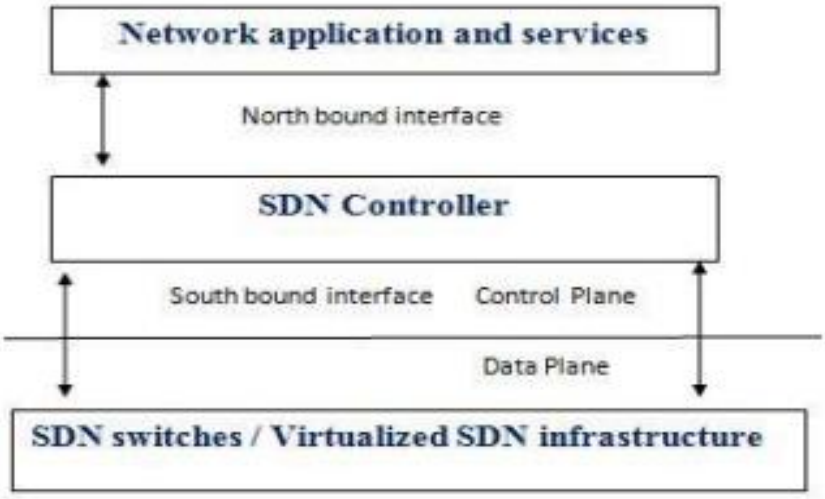

Fig.1. Proposed Concept

As shown in Fig 1, SDN moves the control plane outside the switches. It enables an external centralized control of data through a logical software entity known as the SDN controller. SDN decouples software from hardware. SDN centralizes network state in the control layer. This makes the network management, provisioning, configuration, resource optimization and network security flexible using automated SDN programs. SDN architecture includes a set of API (Application Programming Interface) that supports the implementation of common network services like device discovery, address allocation and mapping, security, routing, access control, bandwidth allocation and resource optimization, energy usage management, storage support, QOS and other business related services. Controller can update, add/delete the flow entries in the flow table either reactively in response to packets or proactively using predefined rules. The controller interface can be executed on any vendor hardware and operating system with high performance.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2244 - 2248
RECEIVED : 15.04.2017 PUBLISHED : 06.05.2017
May 06, 2017

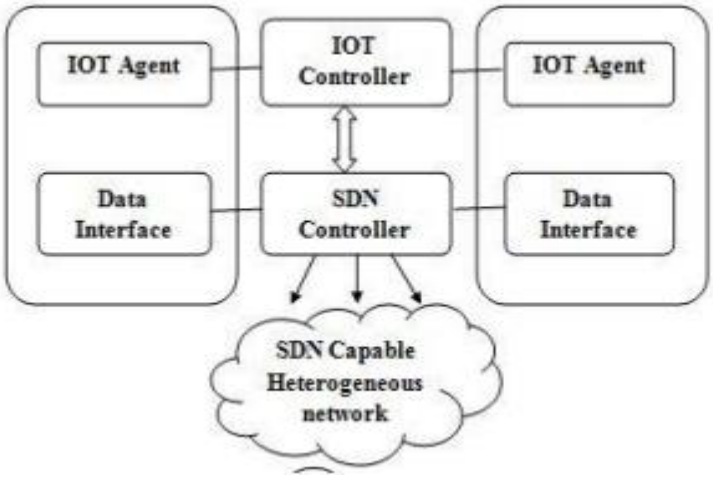

Fig.2. System Structure

agent and IoT controller as discussed in section 4. We assume that such resource constrained device can be associated to one neighbour node which is SDN capable. We segment the heterogeneous network of IoT into various segments as shown in Fig 4. In each segment there will be resource constrained devices like senor nodes, mobile nodes, smart object etc. Also there will be devices which have enough resources and are SDN capable. These are Open Flow capable nodes. These resource constrained nodes needs to be associated with Open Flow capable nodes in their segment. Each segment has its SDN controller which controls all the traffic in that segment. These Open Flow capable nodes must be connected to its segment's SDN controller. The job of the SDN controller in each segment is to authenticate the network devices. After successful establishment of Open Flow secure connection between the switch and the controller, the controller blocks switch ports directly connected to the users. Once the user is authenticated, based on user authorization level the SDN controller will enable the corresponding flow entries to the switch.

4. ANALYSIS

controller in its segment to authenticate its user request and corresponding traffic. Once authorized, the SDN controller establishes the flow entries and sends the traffic to the Gateway controller. The Gateway controller then sends request to its neighboring controllers to determine if the destination address exit in their respective segments. The destination Gateway Controller carries of the same authentication procedure in its destination device segment.Only the authorized devices can communicate with the Gateway controller at destination segment. If the intended recipient is not present, then appropriate response is sent back to the source Gateway Controller. Thus SDN based IoT architecture can be employed to establish security frameworks. The traditional heavy cryptographic techniques are not required to be installed on resource constrained devices in IoT. Instead SDN controllers can play a vital role in ensuring the security. In a distributed environment, the Gateway Controllers will ensure the authorization and enforce security.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2244 - 2248
RECEIVED : 15.04.2017 PUBLISHED : 06.05.2017
May 06, 2017

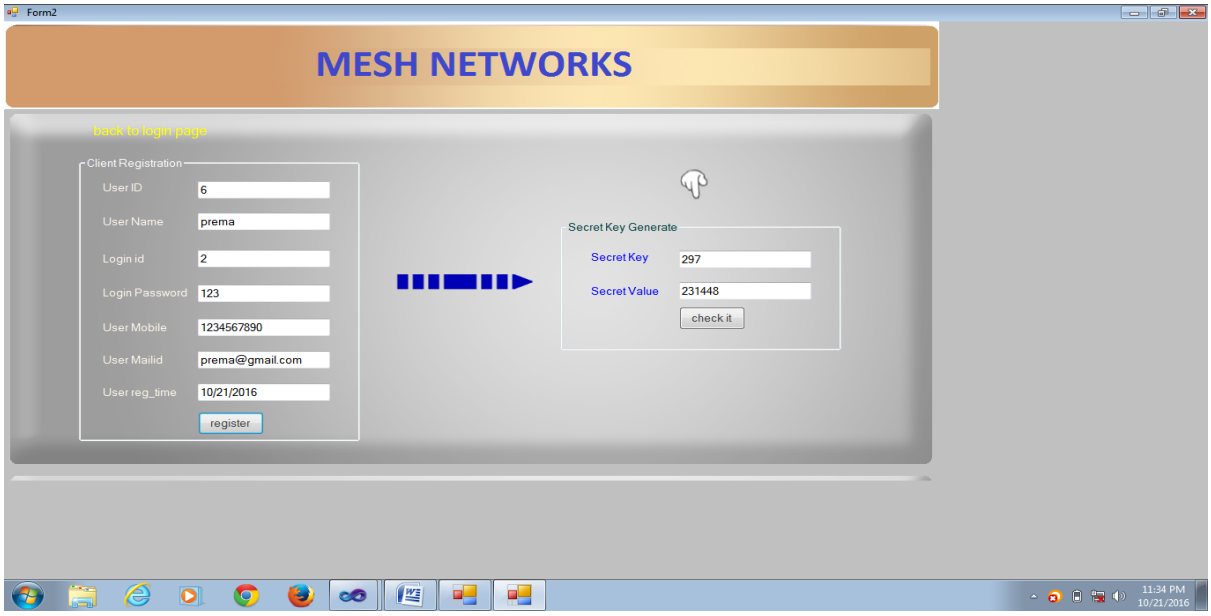

Fig.3.Analysis output

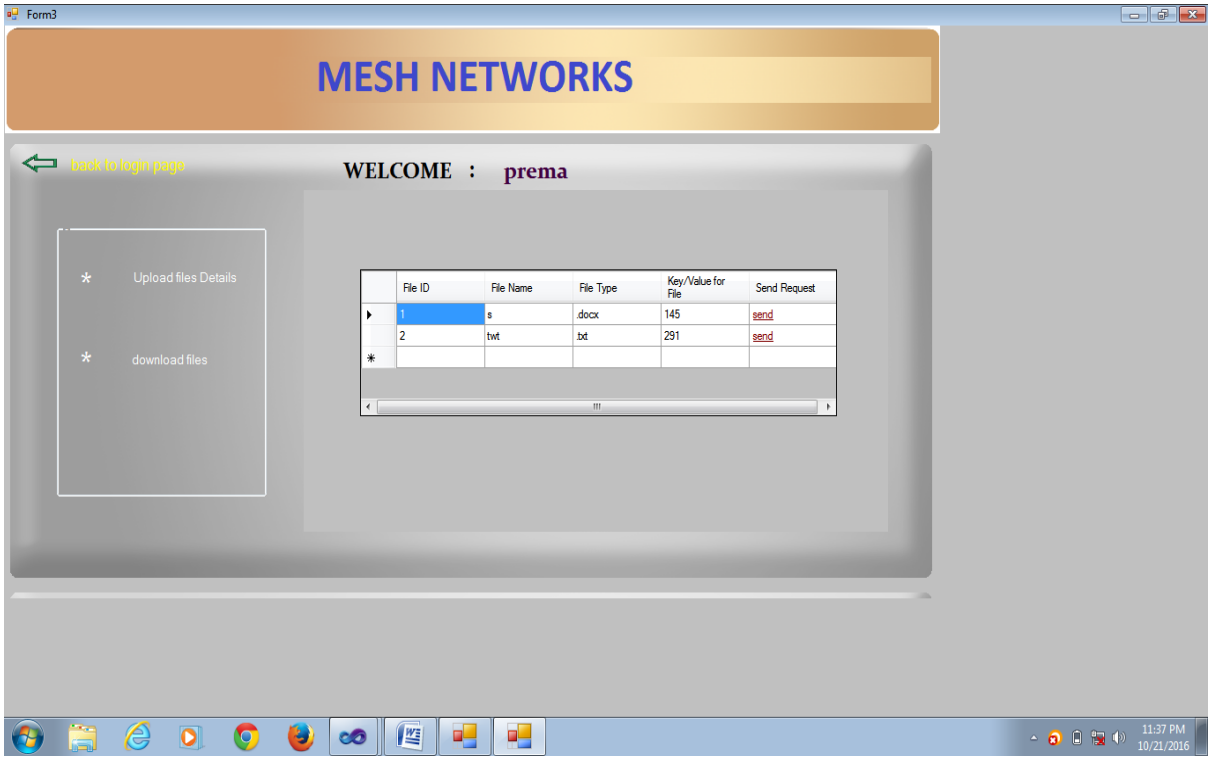

Fig.4. Analysis Result

Each controller of each segment exchanges their security rules. SDN controllers now behave as security guards on the edge of the network segment. An SDN controller provisions safety connections between segments and accepts only authorized traffic. When a node wants to communicate with another node of another segment, the flow has to be forwarded to the SDN Controller,

CONCLUSION

It contributes to hiding the complexity of the network to security operators, that only need to focus on defining the policies. The evaluation describes moving the analysis of traffic away from the controller and into the processing units makes our framework more scalable. The scope of SDN in IoT to provide solution for various challenges is discussed. The various security issues in IoT are analyzed. A framework to improve the security in IoT based on SDN architecture has been proposed.

REFERENCES

[1] A. Lara and B. Ramamurthy, "OpenSec: a framework for implementing security policies using OpenFlow," in IEEE Globecom Conference,Austin, Texas, USA, December 2014.

[2] H. Kim and N. Feamster, "Improving network management with software defined networking," IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, February 2013.

[3] A. Lara and B. Ramamurthy, "Simplifying network management using Software Defined Networking and OpenFlow," in IEEE International Conference on AdvancedNetworks and Telecommuncations Systems (ANTS), Bangalore, India,December 2012.

[4] "Open network foundation", Website, https://www.opennetworking.org/about/onf-overview.

[5] "Open flow spec 1.3," https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf.

[6] S. Scott-Hayward, G. OCallaghan, and S. Sezer, "SSDN security: A survey", in Proceedings of the IEEE SDN for Future Networks and Services. pp.1-7, 2013.

[7] S. Son, S. Shin, V. Yegneswaran, P. Porras, and G.Gu, "Model checking invariant security properties in openflow", in Proceedings of the IEEE International Conference on Communications. pp. 1974-1979, 2013.