iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4123

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

A Security Layer Proposed for IOT Communication Model

Dr. Syeda Gauhar Fatima[1], Syeda Kausar Fatima[2], Dr. Syed Abdul Sattar[3]
[1]*Prof. DCET, Hyderabad, Associate Prof. SCET, Hyderabad, Principal NSAKCET , Hyderabad*

Abstract: ***Established on the IoT Communication Reference Model, this paper proposes a significant improvement to its layers through adding an additional level called "Security Layer". This suggested layer can be well thought-out as a phase forward to a consolidated administration of all security mechanisms into a single and influential layer. The Security Layer targets to authorize the uniqueness of the transmitter/receiver, and to aid to block connections to possibly susceptible services. Furthermore, this centralization would leave other IoT's Communication Reference Model Layers to accomplish their quantified purposes without paying consideration to any security glitches, consequently supporting the establishment of future troubleshooting procedures for such difficulties.***
Keywords: Internet of Things (IoT), IoT Architecture project (IoT-A), OSI, TCP, Security, IoT Communication Reference Model, Security Layer.

I. INTRODUCTION

It is no secret that in the progression of time there is a quick and rising worldwide development headed for the Internet of Things (IoT) at all levels of government and trade. The mutual definition was that the IoT comprises dissimilar objects and connectivity [1]. Nevertheless, to reach the aim of the IoT there is a requirement for a model labelling the statement between these heterogeneous objects, such as the TCP/IP model. Much discussion was done by a group of researchers from more than 20 large industrial companies and research institutions to lay a common "architecture" for the Internet of Things: the IoT Architecture project (IoT-A) [2]. The heterogeneity of smart devices along with the currently existing infrastructure raises the impossibility of having a single design protocol that fits all application domains. Therefore, a more abstract model is needed. The general Communication Reference Model suggested by [2] gives this general abstract framework that comprises a minimal set of unifying concepts, axioms and relationships for understanding significant relationships between the entities of an environment. However, the suggested Communication Reference Model is still unable to address the interoperability issues between heterogeneous objects; like security and privacy.

II. SECURITY REQUIREMENTS FOR IOT

In the security hierarchy of information transmission process, we have to guarantee the confidentiality, integrity, authenticity and instantaneity of data and information, which mainly refers to the security of telecommunication network and corresponds to the security of transmission hierarchy in the Internet of Things [3], Figure (1) illustrates these requirements.

Figure 1. Security Requirements for IoT.

III. THE PROBLEM HISTORY

The history of the OSI and TCP/IP reference models (Figure 2) to the IoT-A. As a step forward to address a solution for the security issues, this research proposes a new adopted security layer to be added to the IoT-A. The following sections give a brief introduction to the security requirements and a history for the OSI and TCP/IP reference models as roots to the IoT-A. The IoT Architecture Project (IoT-A) [4] [2], which is a project funded by the European Union and conducted between 2010 and 2013, was the startup for setting such IoT model. More than 50 scientists and researchers contributed to the development of the Communication Reference Model for the IoT which is called "IoT Communication Reference Model".

IoT-A team decided to focus on the ISO/OSI stack, the US Department of Defense 4 layer model (DoD4) , and the Internet stack, as roots to provide the IoT reference model. The previous models are not able to address the interoperability issues between heterogeneous objects like security. However, this model can be layered on top of one another with our vision to form a new model. The interoperability aspects required for the IoT-A model are illustrated in Figure 3.

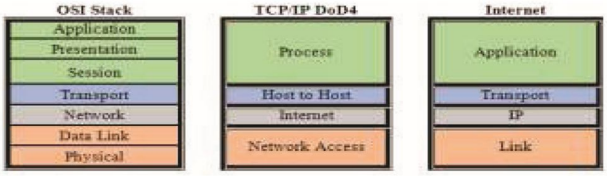


Figure 2. OSI Layers to TCP/IP Model and Internet Stack Model

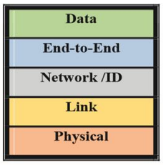


Figure 3. IoT-A Communication Reference Model

OSI Layers (ISO 7498-1)	Security Model (ISO 7498-2)
Application	Authentication
Presentation	Access Control
Session	Non-Repudiation
Transport	Data Integrity
Network	Confidentiality
Data Link	Assurance / Availability
Physical	Notarization / Signature

Table 1. The Security Model

IV. PROBLEM DEFINITION

From the security perspective, the current proposed research investigates the first of the roots of the IoT, which is the OSI model, the security reference model of which is defined in (ISO 7498-2), as illustrated in Table 1. The model is designed around the seven layers (based on OSI reference model ISO 7498-1) [5]. Although the security needs are well-recognized in traditional internet domains, it is still not fully understood how existing security protocols and architectures can be deployed in IoT [6].

V. PROPOSED SECURITY LAYER

The proposed idea [7] is intended to create an independent single layer that will meet most of the required security mechanisms which have been distributed over other layers. The proposed layer will be placed between the Link layer and Physical layer as a filtration layer before the processes of sending and receiving data. Moreover, the proposed layer planned to be lightweight to be suitable for constrained and limited resources devices (those having limited CPU processing capability, a small footprint memory, and limited energy sources) Figure 4. Figure 5 illustrates a scenario of End-to-End Communications through the IoT Communication Reference Model with the proposed security layer.

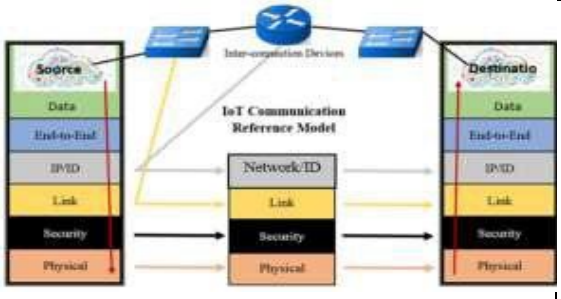


Figure 4. Illustration of the model with the proposed Security Layer.

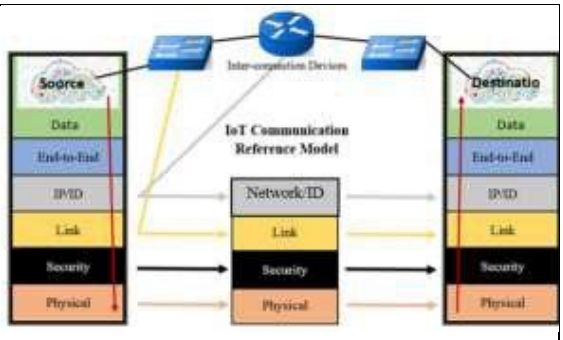


Figure 5. Security scenario from End-to-End

VI. EVALUATION PROCESS

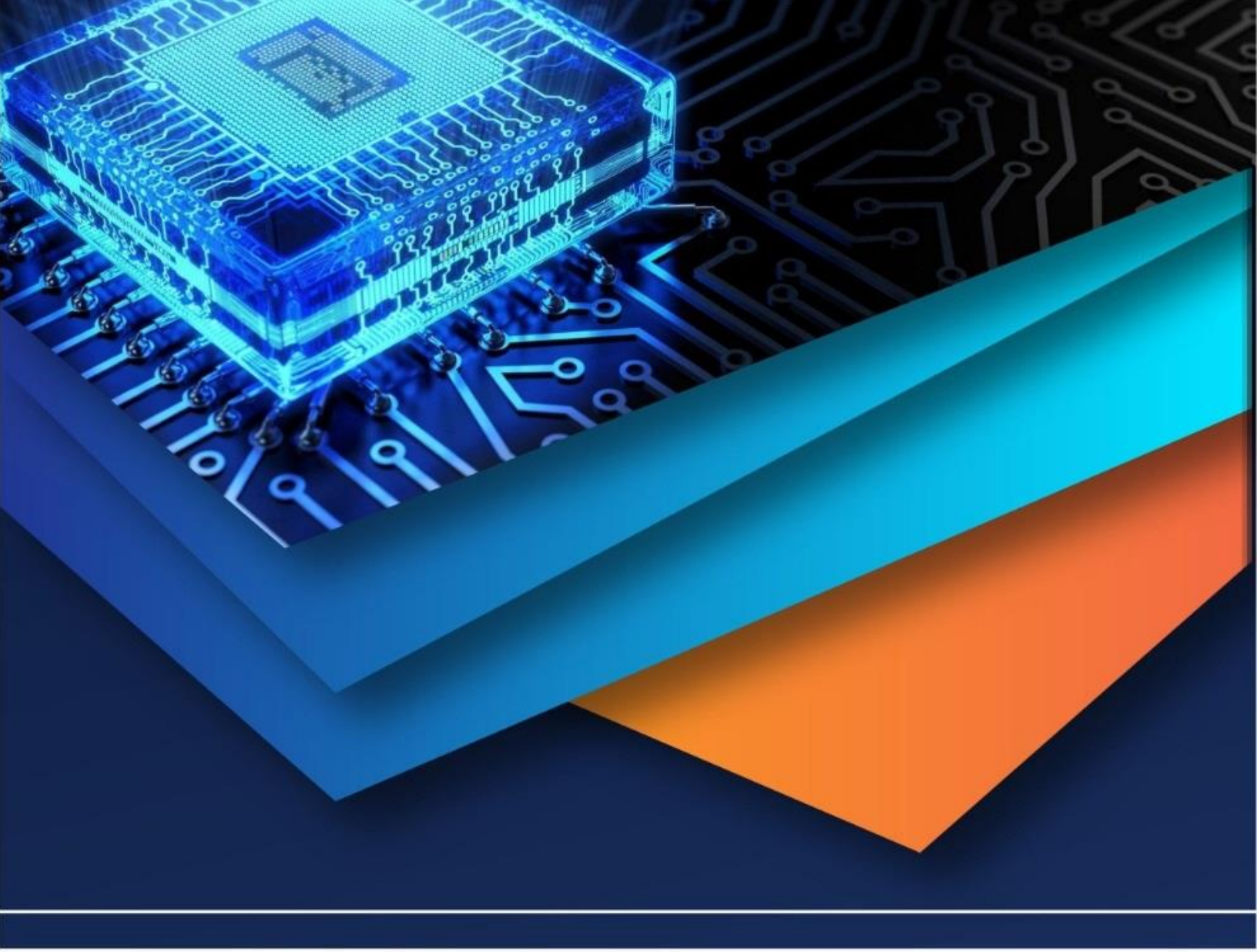
For the evaluation of the efficiency of the proposed Security Layer, it is planned to build such layer in one of the root reference models for the IoT (either OSI Model or TCP/IP Model). The evaluations of process will be tested through a number of measurements related to the change in the behavior of the reference model after such application. The functionality of the proposed layer is intended to be studied through a number of experiments. In such experiments, the Quality of Service (QoS) will be also evaluated through a number of parameters including: JITTER, End-to-End delay, MSE, MOS, PSNR, and Throughput.

VII. CONCLUSIONS

Entirety everybody will someday be attached to the Internet of Things. The history of networks is known and the security problems which still occur are noticeable. This scheme specified a brief summary of the existing IoT communication security alongside with the significant security necessities for the upcoming of this new era. Furthermore, the suggestion stated the necessity for a novel security layer to be added to the existing IoT Communication Reference Model. The supposed possible benefits of that layer may comprise link and end to end security. Also, it may raise the throughput performance of other layers, since they will rely on the security layer for the data authentication and authorization of its sources. Additionally, it would be very cooperative for the troubleshooting engineers as all difficulties will be collected in one place.

REFERENCES

[1] Van Kranenburg, Rob, and Alex Bassi. "IoT challenges." Communications in Mobile Computing vol. 1, no. 1, pp. 1-5, 2012.
[2] Bassi, Alessandro, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob Van Kranenburg, Sebastian Lange, and Stefan Meissner. Enabling things to talk. Springer, 2013.
[3] Li, Lan. "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), International Conference on, vol. 1, pp. 374-377. IEEE, 2012.
[4] http://www.iot-a.eu/public
[5] Oladayo Bello, Sherali Zeadally: Communication Issues in the Internet of Things (IoT) Springer-Verlag, London, 2013.
[6] Glenn Surman: Understanding Security Using the OSI Model. SANS Institute InfoSec Reading Room, 2002.
[7] Adel H. Alhamedi, Hamoud M. Aldosari, Vaclav Snasel, Ajith Abraham. "Internet of things communication reference model." Computational Aspects of Social Networks (CASoN), 6th International Conference on. IEEE, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY