iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 5 **Issue:** V **Month of publication:** May 2017

**DOI:**

www.ijraset.com

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

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Security Framework for Internet of Things (IOT) Cloud Data Sync

Ms. Manavi M[1], Dr. G. Raghavendra Rao[2]
[1]P G scholar, [2]Professor
Department of Computer Science and Engineering, National Institute of Engineering (NIE), Mysuru, Karnataka, India

***Abstract: The Internet of Things (IoT) is an important topic in technology industry, policy and engineering circle has become headline news in both the specialty press and the popular media. A lot of important questions has been solved but some remain opened. One of the critical issue remained unsolved in IoT is security. This paper proposes solution for security challenges authorization and authentication access of data in IoT environment. The solution is based on central identity store (Service provider). Each user get registered to the central identity store (Service provider). Once registered, the user will get Credentials from central identity store (Service provider). When user needs a data, he will uses the credentials to request the data from central identity store (Service Provider).***
***Keywords : Internet of Things, Credentials, authorization, authentication.***

## I. INTRODUCTION

Today the Internet of Things has become a popular term for describing scenarios in which internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items. The IoT [1] is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunication. The IoT enables these objects to collect and exchange data.

In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting things based on existing and evolving interoperable information and communication technologies" and for these purpose a "thing" is an "object of the physical world, which is capable of being identified and integrated into communication networks".

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. Experts estimates that the IoT will consists of about 30 billion objects by 2020.

Today there are billions of internet connected devices being deployed into mission critical systems. The potential security risks and implications have grown exponentially because anyone with a web connection has the potential to compromise these systems. Currently threats to IoT devices have moved beyond simple proof-of-concepts, and its expected attackers will continue to explore the developments in technology and accelerate ways potential threats can be realistically exploited. Once the signal of IoT is stolen or interrupted, it will directly affect the security [2] of the entire information of IoT. If IoT cannot have a good solution for security issues, it will largely restrict its development.

However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized. One of the issue is security in IoT .While security considerations are not new in the context of information technology, the attributes of many IoT implementations presents new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be fundamental priority.

Users' needs to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points for cyber-attacks and user data to theft by leaving data streams inadequately protected.

This paper propose a security framework for IoT cloud data. The main objective of paper is making proper authentication between IoT environment and users whoever requires data. It also allows authorization by examining the user information.

The rest of the paper is organized as follows. Section II provides related work in this area and information needed to understand the framework. Section III describes the problem definition and Section IV describes Security Framework proposed. Finally, we conclude a paper in a Section v.

## II. RELATED WORK

Zhang et al [3] describes distributed privacy preserving for sensors network. To preserve users' privacy tokens are used. So that if

data is required users have to take tokens from owner of devices. Such that users' privacy is preserved. But this paper does not resolve fine grained access control on the devices.

Thomas kothmayr et al [4] introduces the 2-way authentication security scheme for IoT devices. It does not addresses any device management and administration, but it provides feasibility of protocol in point-to-point communication.

Nehme et al [5] describes framework for data authentication in IoT environment. In this framework data are represented as streams with security punctuations. This paper does not solve the problem of security challenges and consisting of devices in IoT environment.

Seitz et al [6] propose a framework with authorization for IoT environment. This paper addresses the important security challenge by proposing set of security and performance requirements. This paper support generic authorization to a variety of devices. Moreover it does not resolve machine-to-machine trust but do user device security.

Jing et al [7] mainly focuses on security problem among all other problem in IoT environment. However IoT is built on an internet basis, problem in security of internet will be reflected to IoT. This paper survey focused on security architecture and security issues of IoT and IoT is divided into 3 layers: perception layer, transportation layer and application layer. RFID and WSNs technology is of great importance for perception layer so this paper analyzed both RFID and WSNs technology and their corresponding solutions. After analyzing this a new challenge was analyzed which is RSN, an integration of RFID and WSNs. This paper next analyzed one more layer that is transport layer security issue for 3G Network, WIFI and Ad Hoc. The application layer in IoT consists of application support layer and IoT application layer. This application layer was analyzed as its security is application related, security of IoT layers issues cannot be solved.

## III. PROBLEM DEFINITION

The IoT builds on an idea that a single device may not provide any significant and useful functionalities and therefore it corporates with multiple other devices in its neighborhood. An individual device needs to trust other devices in order to deliver any data for a user. The trust must be established not only among devices and but also between the user and the devices. Main issue in IoT environment is security, privacy challenges and device management also creation of confidential environment.

## IV. SECURITY FRAMEWORK PROPOSED

this paper proposes a framework with central identity store (Service provider) where user get registered. It automatically fetches users' Mac ID and User Name, based on these information of user central identity store (Service provider) authenticate user who has requested data.

Figure 1 shows the proposed security framework for IoT cloud. Main participants in proposed framework are: User, Service provider, cloud data server and IoT environment. Definitions of these participants are:

*A.* User - one who request a data from the Service provider.
*B.* Service provider - creates credentials for users by following some rules.
*C.* Cloud data center- a data acquisition system where all data is stored.
*D.* IoT environment - where data is collected.

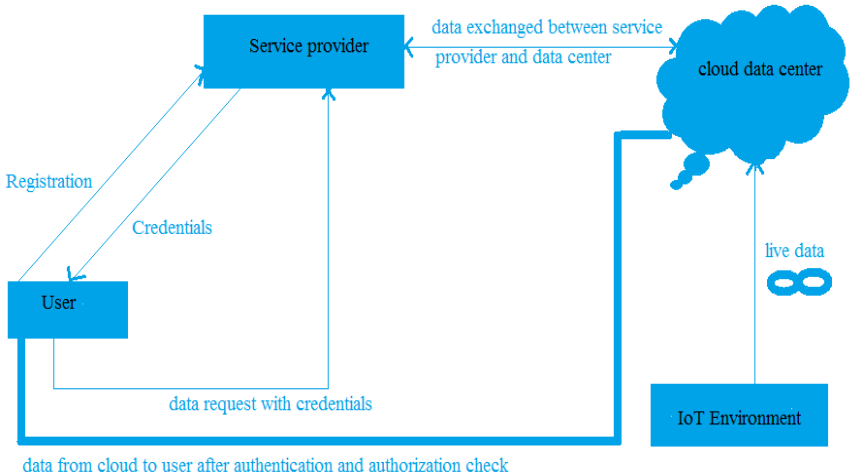



Fig 1: Proposed Architecture

Figure 1 demonstrate the workflow of users' authorization and authentication process. The steps for authorization and authentication process is as follows:

Step 1: User get registered to the Service Provider where Mac id and User Name is automatically fetched by Service provider.

Step 2: Service provider creates Credentials (Mac id, User Name) to the registered user and stores in cloud data center.

Step 3: After registration user request data from Service provider with Credentials which is created by Service provider.

Step 4: Service provider verifies user submitted credential with credential stored in cloud data server, if both matches then Service provider send requested data to the user where authorization and authentication is ensured.

In step 4 authentication is ensured by checking whether user is trying to access data from same User Name and same Mac id. Authorization is ensured by checking credential submitted by user whether he is having permission to access data or not.

## V. CONCLUSION

This paper addresses IoT security challenges with authorization and authentication of user in IoT environment for accessing data which ever they requested. The main component in proposed security framework is central identity store (Service provider). Service provider creates credentials for every user who got registered. Every user will have credentials for requesting data. This enables both authorization and authentication of user access to the data. In any security problem, the registered user can be removed by Service provider and he will not be able to get registered in future.

## REFERENCES

[1] L. Atzori, A. Iera, and G.Morabito, "The internet of things: A survey", Computer Networks, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[2] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D.Qiu,"Security of the internet of things: perspectives and challenges", Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11276-014-0761-S7

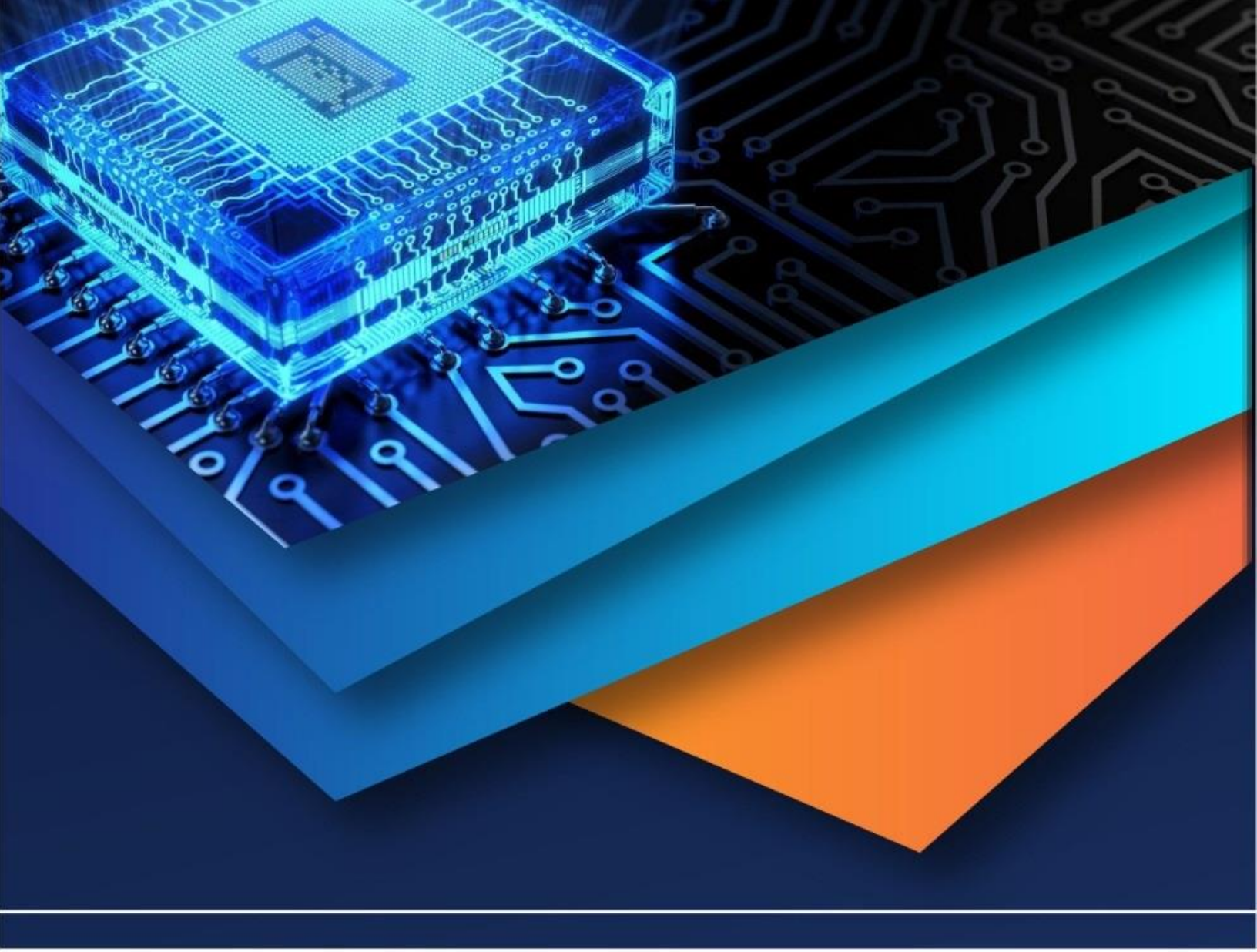
[3] R. Zhang, Y, Zhang, and K, Ren, "Distributed privacy-preserving access control in sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol, 23, no, 8, pp, 1427-1438, Aug 2012

[4] T. Kothmayr, C, Schmitt, W, H u, M, Bring, and G. Carle, "{DTLS} based security and two-way authentication for the internet of things", Ad Hoc Networks, vol, 11, no. 8,pp,2710-2723,2013. [Online]. Available:http://www.sciencedirect.com/science/article/ppii//S1570870513001029

[5] R. V. Netme, E. A. Rundersteiner, and E.Bretino, "A security punctuation framework for enforcing access control on streaming data," in 2008 IEEE 24th International Conference on Data Engineering, April 2008, pp, 406-415.

[6] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the internet-of-things," in World of Wireless, Mobile and Multimedia Networks( WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a, June 2013, pp, 1-6

[7] Q. Jing, A. V. Vasilokas, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp.2481-2501,2014. [Online]. Available: http://dx.doi.org/10.1007/s11276-014-0761-7.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY