iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

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 5 Issue XI November 2017- Available at www.ijraset.com

Security Issues with Iot and Survey of Protecting System for Authentication at Gateway

Dr.Mamatha.T[1]
[1]*Maulana Azad College of Ennginering & Technology*

Abstract: ***Now a day's people want comfort and automation in their day-to-day life with one click. For that Internet of Things (IoTs) is the most emerging paradigm. This paper introduces IoTs, which offers capabilities to identify and connect worldwide physical objects into a unified system. As a part of IoTs, serious concerns are raised over access of personal information pertaining to device and individual privacy. This survey summarizes the security threats and privacy concerns of IoT.***

Keywords**: *Authentication, Challenges in Authentication, IoT, Security Challenges in IoT Network.***

I. INTRODUCTION

Recent advances in wireless technology for communication and computing leads to fully automated system in people's day-to-day life, and for this kind of automation system emerging technology is Internet of Things. Through IoT we can extend Information Technology (IT) for our lives. IoT transforming current isolated network and infrastructure into a global network of interconnected objects. IoT means the interconnecting deice with their unique identity in the Internet. IoT working on different protocols, standards and mediums with layering approach. IoT includes devices with various sensing, measuring and data capture ability with that achieve identification, location, monitoring and management of interconnected devices. This all features are done in various stages such as sensing, gathering of information and transform for further computation through any transmission network. But, these all stages are vulnerable to different. Security attack especially due to direct connectivity with the internet. This vulnerabilities leads to different security attacks as well as also leads to authentication, access control, data privacy
Kind of issues. So, if we combine and

II. INTERNET OF THINGS

IoT is a networking of cyber-physical system for information transfer without requiring human-to-human or human- to computer interaction. IoT is the digital view of the actual working of physical device as shown in Figure 1. IoT is embedded system of sensors, actuators and different computing devices. In IoT, wireless sensor network is one of the most important part, through which gathering the data of actual physical working or actual status of physical device[5]. IoT works with layered approach, consisting three layers named;

A. Perception layer
B. Transport layer
C. Application layer.

This layer consist of various Protocols and standards, through which layers done their own task like sensing, gathering of information, transmission of in-formation, making connection with the users through various kind of application, etc.

Figure 1: Internet of Things

D. All layers are working as following

1) Perception layer/Physical/MAC layer

This layer captures the data from the sensors and actuators which are connected with the wireless sensor network. This data captures with changes in status of that devices and forward to the higher layer for further computing.

2) Transport/Network layer: This layer takes data from perception layer and do control of processing data and transferring data. This layer is also responsible for routing of data or information.

3) Application layer: This layer mainly considered with the end user. It is responsible for the logic and presentation of data.

E. Characteristics Of Iot

1) Inter-connectivity: In IoT, anything can be inter connected for communication globally.

2) Thing related services: IoT provides changes of physical world with the changes of associatively of virtual things with physical things.

3) Heterogeneity: IoT can interact with any devices or service platforms from different networks.

4) Enormous scale: IoT supports number of devices for the management and for the communication according to their magnitude limits.

*5) Safety:*IoT takes care of data privacy, endpoints security and security of networks.

6) Connectivity: In IoT, using this characteristic enables network accessibility and compatibility for consume and produced data on network.

F. Working Of Iot

In working of IoT there are mainly 4component plays major role i.e. sensor node, gateway, server or cloud storage and analytics.

Figure 2: Working of IoT

Step by step procedures for working of IoT are as following:

Step-1: With the help of end device sensors collect data of their physical status.

Step-2: Gathered information transfer through the physical medium towards the gateway.

Step-3: At gateway check the data packets whether it is from the authorized sensor node or not. If it comes from the authorized user then data will be encrypted.

Step-4: Encrypted data transfer through secure transmission medium towards the cloud data storage or data center.

Step-5: As per the need of information of user, user request to the cloud storage for required information for analytics purpose.

III. SECURITY ISSUES WITH IoT NETWORK

There are many security issues in concern of IoT in terms of authentication, access control, data privacy, securing a transmission network and various kinds of security issues. Some of the major issues are as following:

A. IoT devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.

B. IoT devices along with their cloud and mobile applications components failed to require passwords of a sufficient complexity and lengths.

C. IoT devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

D. IoT devices used unencrypted network service.

E. IoT device collected at least one piece of personal information via the device, thecloud or its mobile application.

F. Insufficient authentication and authorization.

G. Insecure web interface.

H. Lack of transport encryption.
I. Insecure software and firmware.
J. Information security and data privacy protection because of mobility, deployment and complexity.

IV. AUTHENTICATION ANDTHEIR RELATED ISSUES

Authentication is the process to check the personal user's credentials for authorized user. Though authentication user can get authorized access. In context of IoT, authentication checks the identity of the sensor node for the taking upthe information from that sensor node for further analytics process. In IoT infrastructure, at gateway this authentication process is done. Authentication is done through various protocols [10].These protocols are enlisted below.

1) PAP Password Authentication protocol
2) CHAP Challenge handshake authentication protocol
3) 3. EAP Extensible authentication protocol
4) Kerberos
5) RADIUS Remote authentication Dial In user service
6) RFID authentication protocol
7) Host identity protocol
8) Open ID protocol
9) X.509 Digital certificate, etc.

For authentication in IoT Auth 2.0 and Open ID connect 1.0 are two standardized framework.

A. Issues with Authentication in IoT

Authentication is most important aspect of any IoT device. If authentication is not proper then it leads the issues related to the privacy of sensitive and important data, it also harmful for the whole infrastructure of the IoT because any one can easily get authorized access through creating backdoor or with the breaking of authentication. Some issues with authentication are as follows:

B. Node deployment. There are two types of node deployment:

1) Static deployment,
2) Dynamic deployment

Static deployment is vulnerable for replay attack. If deployed node should be traceable then we can find replay attack and take counter act against it but, if node can't be traceable for authentication following issues should be faced:

3) Moving nodes re-authentication
4) Nodes movement that should be untraceable
5) Message integrity
6) Confidentiality
7) Node capture and compromise
8) Complex management of public key infrastructure
9) Computational bottleneck
10) Oath authentications have been bound with HTTP only

V. STUDY ABOUT EXISTINGSYSTEM FOR PRESERVINGAUTHENTICATIONSECURITY

In IoT, there are no standardized authentication mechanisms at gateway for authenticating sensor nodes. So, every IoT application vendors are used any of the authentication mechanism which is enlisted in above section 4.Those all authentication systems are patented and standard authentication as per the cryptographic view but, still they all having their own limitation in terms of security from the various kind of security attacks i.e. Does attack, Impersonation attack, data theft attack, Flooding attack, etc. So, for the preserving authentication system from these kind of issues implements some protection mechanisms which are either for identifying the attacks affected sensor node or protecting from the affection of the attacks from the sensor node side.

Some existing protection mechanisms are as follows:

Implements a lightweight mutual authentication scheme which validates the identities of the participating clients and server through single key which is nothing but the session key allocated by the server. But it implements only in CoAP based IoT environment[6].

Implements one reception kind of thing which validates message and resource of sensor node for protecting an authentication from DoS attack [9].

Implements Identity based authentication scheme for heterogeneous environment using virtual IPv6 address for authentication of device and gateways. It prevents from masquerade, man-in-the middle replay attacks [7].Implements ECC based Mutual authentication and capability based access control model to ensure secure authorization. It prevents from man-in-the-middle, Dose, Node capture attack and replay attack [2].Implements authentication system which provides mutual authentication between the users, sensors and gateways with fulfillment of security characteristics of IoT [3].Implements verifiable secret sharing cryptography through signature in6LowPAN environment [8].

Implements object authentication framework to exploit device specification information with normal change in fingerprints for preventing from the different security attack [4].Implements modification in MQTT frame-work's services for reducing the authorization delay, message overhead, etc. But, security is no concerning [1].

So, as per the detail study of those kind of protection system for authentication is not concerning about the all kind of security attacks which would be hap-pens in IoT network. Also no any single system is feasible with all IoT protocols. If any system feasible with all protocol then it is not protecting from all security attacks and vice versa.

VI. FUTURE WORK

For securing IoT authentication system proposes and implements a new protection preserving system with authentication, which will be secure from all kind of attacks and feasible with all IoT protocols.

VII. CONCLUSION

IoT is good paradigm for our day-to-day life comfort. But, Security issues also matter with IoT. In IoT there were various related security attacks. In this study the main concern about various authentication issues and existing solution for those kinds of issues. It will beneficial for removing and securing the authentication system at gateway.

REFERENCES

[1] AimaschanaNiruntasukrat, ChaveeIssariyapat,PanitaPongpaipool, KoonlachatMeesublak,PramrudeeAiumsupucgul, AnunPanya, 25 May,2016, " Authorization Mechanism for MQTTbasedInternet of Things," IEEE ICC2016- MQTTbasedInternet of Things," IEEE ICC2016-Workshops: W07-Workshop on ConvergentInternet of Things.

[2] ChristialGehrmann, Marco Tiloca, RikardHoglund, 2015, " SMACK: Short MessageAuthentication ChecK against BatteryExhaustion in the Internet of Things," '12thAnnual IEEE International Conference onSensing, Communication, and Networking(SECON)', pg. 274 – 82.

[3] Fan Wu, LiliXu, SaruKumari, Xiong Li, 2016,"A privacy-preserving and provable userauthentication scheme for wireless sensornetworks based on Internet of Things security,"'Springer' pg. 1-16.

[4] Hong Yu, Jingsha He, 2013 " Authentication andEn-route Data Filtering for Wireless SensorNetworks in the Internet of Things Scenario,",'International Journal of Grid and DistributedComputing', Vol. 6, No. 1, pg. 1 – 12.

[5] Keyur K. Patel, Sunil M. Patel, 2016 " Internet ofThings-IOT: Definition, Characteristics, Architecture, Enabling Technologies,Application & Future Challenges,", '. IJESC',Volume 6 Issue No. 5 pg. 6121 – 6133.

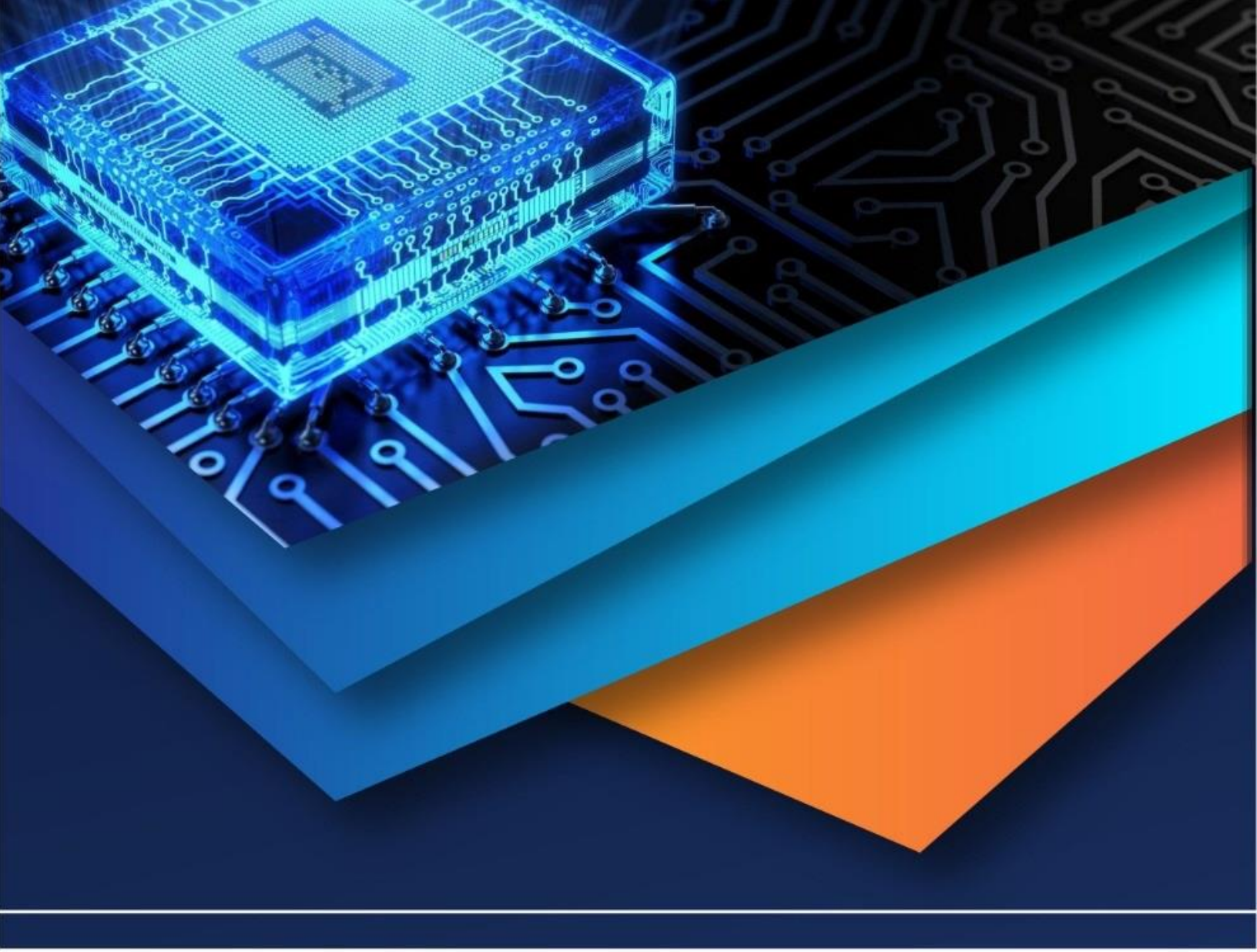
[6] Mian Ahmad Jan, Priyadarsi Nanda, XiaangjianHe, Ren Ping Liu, 2104 "A RobustAuthentication Scheme for Observing Resourcesin the Internet of Things Environment,", 'IEEE13th International Conference on Trust, Securityand Privacy in Computing and Communications'pg. 205 – 211.

[7] Ola Salman, Sarah Abdallah, Imad H Elhajj, AliChehab, AymannKayssi, 2016 "Identity-Based Authentication Scheme for the Internet ofThings," ' IEEE Symposium on Computers andCommunication (ISCC)' pg. 1-3

[8] Sudha Patel, Dhiren R. Patel, Ankit P. Navik,2016, "Energy Efficient IntegratedAuthentication and Access Control Mechanismsfor Internet of Things," 'International Conferenceon Internet of Things and Applications (IOTA)', pg. 304 – 309

[9] S. Raja Rajeswari, V. Seenivasagam, 2016,"Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," 'Scientific World Journal', pg. 1-16.

[10] YamanSharaf- Dabbagh, WalidSaad, 2016 "Onthe Authentication of Devices in the Internet ofThings," 'IEEE', pg. 1-3.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY