International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr 2018 www.irjet.net p-ISSN: 2395-0072

AUTHENTICATION AND CONTEXT AWARENESS ACCESS CONTROL IN INTERNET OF THINGS

Bhramarambika R S , *Dept of CS Engineering,NIE College,Karnataka,India*

Navya V Hegde , *Dept of CS Engineering,NIE College,Karnataka,India*

Anjali S , *Dept of CS Engineering,NIE College,Karnataka,India*

Smt. Rashmi M R , *Assistant Professor,Dept of CS Engineering,NIE College,Karnataka,India*

Abstract - *For security in internet of things, access control is achieved by using another method as compare to the old way. The need for security and privacy for IoT devices is illuminated here. Moreover, assessment of various schemes related to access control in IoT over the latest years is discussed. Lastly, we provide guesses for upcoming research in the field of access control in IoT. On the basis of shortcomings observed in the existing model, the proposed model is designed to protect IoT networks with context-aware access control scheme. The proposed model covers the access control policy for IoT networks with context awareness. IoT is a very useful ecosystem that provides various services; however, at the same time, risk can be huge too. The main purpose of this paper is to survey the access control and authentication in IOT and analyzing three basic characteristics (i.e., heterogeneity, resource constraint, dynamic environment)of security requirements along six key elements of IoT (i.e., IoT network, cloud, user, attacker, service, Platform).*

Key Words: **Internet of Things (IoT), Access Control, Authentication, Security Requirements**

1. INTRODUCTION

The meaning of the internet is connecting the physical devices with each other. Physical devices are ingrained with sensors, electronics, software, actuators. Every aspect of actual life. IoT is used in all the fields like in clinics, in army, in cultivation, in rural areas for the luxury of the publics. IoT provides many services, however on the further hand threats 'as regards the security are also growing. For that, we talk over around the access control and authentication in the field of IoT Access control. Access control explains I formation possession issues and empowers new plans of action, Access control empowers organizations to share IoT gadget information.

The access control policy for IoT networks with context awareness approach which is included to describe the context and type of the IoT nodes In IoT network.it is used to determine the rate of data transfer among the network nodes. The nodes not following the policy as per their data transmission limit according to context, are not provided the access to the network resources under this access control model.

1.1 ANALYSIS OF CHARACTERISTICS IN INTERNET OF THINGS

This section analyzes security requirements based on 3 typical IoT characteristics that have been researched in other researches. These security requirements are commonly applied in IoT security.

Therefore, it is important to understand and advantage of it to design security mechanisms in IoT environment.

A. Heterogeneity

In IoT, heterogeneity means diversity of hardware performances(e.g., CPU computation, memory footprint),protocols,platforms,polices,etc. the biggest problem of heterogeneity is absence of common security service .heterogeneity weakens interoperability and causes extra fees about performance and money to interpret each other.besides, making security-related policies and updates are more complex.in order to solve these problems, we can use some technologies(e.g., meta data registry(MDR),middleware);however, it is not a fundamental solution. For providing common security service, unified IoT security standard has to be established.

B. Resource constraint

Most iot devices are lacking performance and battery capacity.therefore,legacy security services, such as TLS(transport layer security),AES(advanced encryption standard),cannot be applied to iot devices directly.therefore, these services or algorithms should be designed to be lightweight and straightforward to increase efficiency of CPU,memory and battery.in addition, scalability has to be considered.

C. Dynamic Environment

Due to mobility and bad connections, IoT has a dynamic network topology. In very demanding cases (e.g., smart city),numerous devices may send a large number of requests. Hence,nnot only flexibility, but also scalability is required in IoT communication protocols. Consequently, flexibility and scalability will be key security requirements of IoT.

1.2 SECURITY ISSUES AND REQUIREMENTS FOR IOT ENVIRONMENTS

Fig. 1 shows six key elements of IoT (i.e., IoT network, cloud, user, attacker, service, and platform). We consider reviewing security requirements from the elements to be the most effective way. A more detailed description is in the following subsections.

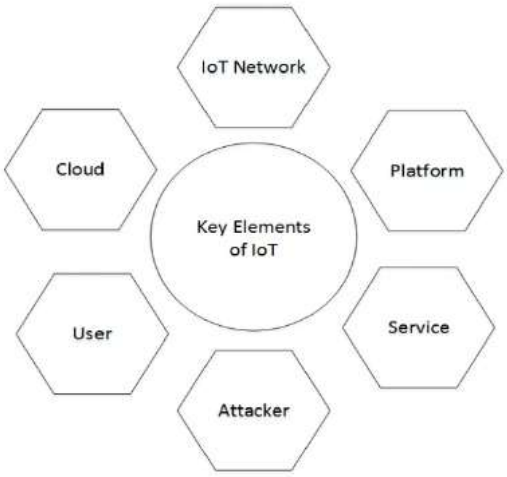

Fig 1: Six key elements of IoT

IoT network is a specialized form of conventional network .It has three features as described in Section 3. In IoT network, there are many Things (e.g., gateways, sensors), and they may communicate using lightweight communication protocols, such as MQTT and CoAP based on IEEE 802.15.4.

The most important fact is that IoT network is basically not different from conventional networks. Therefore, most existing problems (e.g., fragmentation, security attacks) could happen in IoT network. In this subsection, we focus on the following issues: privacy, security in multicasting and bootstrapping. Privacy. IoT is becoming more and more closer to human life like ubiquitous. It can be used anywhere, anytime with anything.

B. Cloud

Usually, IoT devices use cloud because they cannot save the data in their low memory capacity. In some cases, sensitive data (e.g., home CCTV video, personal location, health information) can be used for rescue people. However, if cloud out of order for some reasons, IoT devices cannot save the data. Then critical data that will be used for rescue can be missing. As a result, rescue service that require the data may be stopped. Therefore, in this case, availability is highly necessary, so that device should have back-up cloud to be replaced with original cloud. There are a lot of data sent from many devices in cloud. To protect the data from unauthorized user, cloud should use proper access control (i.e., authentication, authorization), encryption, data anonymity, etc. In addition, the data may not be fully needed to be encrypted based on the importance of data.

C. User

User is the most vulnerable element in IoT security. Even if information system is implemented securely, if a user, especially system engineer, is careless to manage, any security system will be useless. For example, in ID-password authentication model, if a user makes the password with a simple and guessable passphrase, attackers could crack the password easily using brute force attack or dictionary attack which is well known security attack. That is, the user has to follow strictly the security rules, and the user needs to be educated about social engineering.

D. Attacker

Security service can be compromised by attacker Although a user follows security rule. Due to IoT devices are connected to network, it can be victim anytime. most of IoT devices cannot apply strong security service because of its constrained resources. Besides, current IoT security services have not been fully validated. For these reasons, IoT is easy target to attack so that security attack will be increased and diversified. Thus, in this subsection, we analyze security requirements against security threats.

E. Service

In this subsection, we analyze security issues (i.e., trust, access control, middleware, storage) as illustrated in Fig. 2. Before we describe the security requirements based on security Issues To take advantage of a service, the user needs to trust the server, and the server needs to provide privacy to the user. If the user decides the server is trustworthy, the user will use service provided by the server or group of devices with smart phone, smart watch, or some kind of network devices. After that, the devices have to progress bootstrapping and access control (i.e., authentication and authorization). Thereby, devices obtain trust from server. Especially, automated, intelligent and context-aware devices in real IoT environment might be operated by itself without

human intervention. Finally, the attacker can compromise the server for malicious
intentions (e.g., collecting personal information).

F. Platform

AllSeen, oneM2M, OIC (open interconnect consortium) and other standards organizations have been established IoT platform standards. Open IoT platform (e.g., Mobius, OneM2M, AllJoyn, COMUS) provides multiple functions (e.g., distributed cooperation, execution control, interoperability between heterogeneous devices to share data). They are focusing on the functionality of platform mainly, however, security is considered only in common services (e.g., encryption, access control through authentication and authorization, signature). At this time, as mentioned earlier, because it is necessary to consider the performance of various IoT devices, all of security services should be lightweight.

2. LITERATURE REVIEW

S. Patelet al. [1] in this paper authors describe the mechanism for security, and privacy and access control. Different types of things are communicates with each other in IoT environment. So maintain the security and privacy of these is the man requirement when we implement a system. In this paper, the crucial methods to assure protected transmission among devices are access control and authentication. Aimed at this determination the author defines the Elliptic Curve Cryptography with mutual authentication and Capability based access control model to assure protect authorization. An AVISPA tool is used to check this protocol. AVISPA tool presents that the given protocol is secure enough for reply attack, node capture attack, DoS attack and manYin middle attack.

B. Chan et al. [2] define SYCBAC stands for SecureY Capability Based Access Control model. This model is used for IoT things in a distributed environment. This model is mainly used for group access in SYCBAC user access mutual service which is functioning at numerous devices by using a single token. In SYCBAC, IPsec channel technique is used to transfer all datagram packets with the Encapsulating Security Payload (ESP) header. This maintains the confidentiality of data. In this model a group of devices is created those produce a common service. A requestor who wants to access these services can access any device of the group by using a only one token.

H. Che et al. [3]tell that IoT is now used in number of areas such as clinic, family circle, towns and societies. Due to safety and confidentiality challenges, the use of Internet of Things is restricted. The IoT devices have a constrained storage capacity. The main target during the intention of IoT is on facility rather than safety and secrecy. In this paper, the author explains the role based access control in a hierarchy for the security of computer networks. Some authors describe cryptography key for security in IoT.

Q. Liu et al. [4]in the given paper authors discuss an access control model which aimed at source distribution established on the RoleYBased Access Control. Which are planned for multi area MIoT [Manufacturing Internet of Things] Furthermore, AROP and PGAOↄ procedures are planned. The suggested model and algorithms can support supervisors to

create a precise conclusion, reduce the loads, and support the access protection in source distribution.

M. Hemdi et al. [5] describe that by the expansion of the Internet of Things (IoT) and the habit of little powered strategies such as devices a huge amount of individuals are consuming IoT structures in their home environment and companies to have additional control above their equipment. But the security of data in IoT environment is a major threat, when the IoT devices are misplaced and robbed. In this paper author explains that how we can protect our data from illegal consumers.

S. Kinikaret al. [6] In IoT huge number of things (devices) are communicate with each other with the help of internet. These devices are constrained devices, so they have a limited storing ability and computing control. Due to these restrictions it is a challenge in IoT environment to offer robust authorization procedures.

Author,publisher and year	Technique proposed	Problem addressed	Brief review
Castellani,angelop,IEEE,2010[7]	This article presents the case study on the versatile architectures and protocols for IoT networks.	The new technique is designed to meet the requirements of IoT in the highly flexible and expandable environment	IPv6 based IoT architecture is analyzed for its ability to tackle the diverse and heterogeneous IoT network.
Debaty, philippe, IEEE Personal Communications 2001[8]	This paper discusses the correlation of people, places and things using the internet.	The context based approach is proposed, which utilizes the diversified network properties including location, identity and device capabilities.	This scheme focuses upon the web presence in the terms of people, places and things in the best interconnection ability.
Gornbaek, Inge,IEEE 2008[9]	This article discusses the IoT architecture and the needs of APIs for data exchange.	Diverse interconnection problems in the IoT are covered in this paper with QoS based IP networking in IoT.	This scheme involves the network architecture with multi-homing ability in mobile networks constructed with dynamic membership of network nodes in I Ot.
H weber, Rolf,Elsevier	This paper	The legislative	This article discusses

2010[10]	presents the various security as well as privacy challenges in the IoT.	and security related challenges are discussed in detailed for the management of IoT.	the upcoming internet based technical architecture facilities for the exchange of goods for supply chain management.

Table 1: Summary of Literature work

4. CONCLUSION AND FUTURE WORK

Now technology is increased day by day, and the internet is used all over the world, so the scope of iot is bright. iot makes our life smart, easier, faster and comfortable. But, still needs to confront hard difficulties identified with the use of security, furthermore access control structures. For further research block chain technology based access control model is used to fulfill the iot necessities. the utilization of capacity based messaging for decentralized access control is innovative and should be additionally researched, particularly with regards to iot. . the ontology analysis model will be designed, which will analyze the ontology of each node to determine the attacker nodes on the basis of their behavior. the context aware ontology approach will regularly monitor the node performance, which will help to find the anomaly (or attacking behavior) of the target node. we analysed three key characteristics of IoT ,such as heterogeneity, resource constraint, and dynamic environment to find out basic IoT security requirements. In addition, we analyzed overall IoT security requirements. We hope this paper can be a guide to design IoT system securely, and improve general understanding of IoT security issues and requirements.

REFERENCES

[1] Sudha Patel; Dhiren R. Patel; Ankit P. Navik Ienergy efficient intergrated authentication and access control mechanism for internet of things", 2016 International Conference on Internet of Things and Application (iOtA), Year: 2016

[2] BortingChen; YuYLun Huang; Mesut Gunes, IsYCBAC: A secure access control model supporting group access for internet of things´, 2015 IEEE International Symposiun on Software Reliability Engineering Workshops (ISSREW), Year: 2015

[3] HsingYChung Che; ChiaYHui Chang; FangYYie Leu, Iimplement of agent with roleYbased hierarchy access control for secure grouping iots", 2017 14th ieee Annual Consumers Communication & Networking Conference (CCNC); Year: 2017

[4] Qiang Liu; Hao Zhang; Jiafu Wan; Xin Chen, IAn Access Control Model for Resource

sharing Based on the RoleYBased Access Control intended for MultiYDomain Manufaturing internet of things", ieee Access, Year: 2017, Volume: 5

[5] Marwah Hemdi; Ralph Deters, Iusing Rest based protocol to enable ABAC within iot systems", 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (ieMCON), Year: 2016

[6] Swati Kinikar; sujatha terdal, Iimplementation of open authentication for ot application", 2016 International Conference on Inventive Computation application, year: 2016, Volume:

[7] Castellani, Angelo P., Nicola Bui, Paolo Casari, Michele Rossi, Zach shelby, and Michele Zorzi. 9Architecture and protocols for the internet of things: A case study.9 in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on, pp. 678Y683. ieee, 2010.

[8] Debaty, Philippe, and Deborah Caswell. 9uniform web presence architecture for people, places, and things.9 IEEE Personal Communications 8, no. 4 (2001): 46Y51.

[9] Gr0nbak, inge. 9Architecture for the internet of things (iot): APi and interconnect.9 in Sensor Technologies & Applications, 2008. SENSORCOMM 08. Second International Conference on, pp. 802Y807. ieee, 2008.

[10] Weber, Rolf H. 9internet of things-New security and privacy challenges.9 Computer law & security review 26, no. 1 (2010): 23Y30.