IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Access Control Approaches in Internet of Things

Meghana P.Lokhande[1*], Dipti Durgesh Patil[2]

[1]Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India
[2]Department of Information Technology, MKSSS Cummins College of Engineering for Women, Pune, India

**Corresponding author: meghna.ingole1983@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i5.11581161 | Available online at: www.ijcseonline.org

Accepted: 19/May/2019, Published: 31/May/2019

***Abstract* -** The Internet of Things is a rapidly growing concept in recent years. Safety and security have traditionally been distinct problems in engineering and computer science. With a massive amount of devices connected to the Internet and huge data associated in it, there is major concern of security of services. Many traditional security solutions including existing access control mechanisms may not be directly applicable in the IoT environment. Traditional access control approaches are not suitable to the decentralized and dynamic scenario in IoT as well. Various cryptographic algorithms developed which addresses security in Internet, but their use in IOT is questionable as the hardware devices used deal in IOT is not suitable for computationally expensive encryption algorithms. Particularly, the need arises for a dynamic and fine-grained access control algorithm on constrained resources. The paper summaries access control approaches that try to improve security in devices. Paper not only summarizes access control approaches, but also provides an understanding of the limitations and open issues of the existing work.

Keywords — Internet of Things (IoT), Access Control, Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), Capability-Based Access Control (CapBAC)

I. INTRODUCTION

Internet of Things where physical or logical objects connected over the Internet and provided with unique identifiers to enable self-identification to other devices and give the ability to sense and send data over remote locations to detect many events, and take relevant actions[1,2]. During the data aggregation and analysis, user privacy and information security become concerns for IoT services and applications. Hence, security of network, data and sensor devices is a paramount concern in the IoT network as it grows fast in exchanged data and connected sensor nodes. IoT network allows users, devices and applications in different physical locations to communicate with one another. In IoT comes in various computing devices which differ in size, operating systems [4]. The connectivity offered by IoT extends to machine-to-machine communications [2]. Likewise, authentication and access control is important and critical functionality in the context of IoT. With this amount of connected devices and to meet a satisfied level of security, one needs strong access control method applicable on the low resource devices such as IoT devices. A higher level of security is necessary for many critical IoT applications; however, it is a significant challenge to achieving security goals in IoT. Authentication and access control technologies are known as the central elements to discuss security and privacy problems in computer networks [3].

To do security and privacy, it should have more focus on access control methods. Even though these traditional approaches such as Role Base Access Control (RBAC) and Attribute-Base Access Control (ABAC) are possibly used, security between the end to end security devices and any Internet host is difficult to achieve. In this paper, aim is to present a comprehensive overview of traditional access control mechanisms and their applicability in IoT systems because access control mechanisms are essential to protect sensitive data and critical infrastructure, and to stop attacks like Denial-of-Service (DoS) attack, replay attack, etc. To solve the problems of security and controllability in IoT, system with a fine-grained and more secure access control model is needed.

The rest of this paper is organized as follows. Section II has discussion on threats and attacks majorly occurred in network. We present a comprehensive study of access control approaches in detail with its limitation in section III. In section IV we present conclusion and plan for future research.

II. THREATS AND ATTACKS

Firstly IoT is extremely open to attacks. Chance of physical and logical attack is possible as they stay unsupervised for long duration. Secondly due to the wireless communication, the eavesdropping is possible. Lastly IoT bear low competency in terms of computational capability and energy.

Computationally expensive security algorithms will result on performance of the energy constrained devices.

Man-in-the-Middle Attack: Man-in-the-middle attack is a type of eavesdropping. It is possible in the commissioning phase of devices to IoT [4]. The key establishment is vulnerable to man-in-the-middle attack .The attacker is trying to intercept the connection and spoof identity, key or security parameters and passive attacker, eavesdrop all the data transmitted between the owner and the devices .

Denial of Service Attack: DOS attack is responsible of making the system down; it makes the device out of service, so that the user can't access [4]. The attacker attacks on IoT devices that have constraints on resources and power. There may be more than one attacker, named as distributed denial of service DDoS.

Replay Attack: While exchanging identity related information or other credentials in IoT, information can be spoofed, altered or replayed to repel network traffic. This causes serious replay attack. The attacker inspects the session and gets the secrets of the owner or user.

III. ACCESS CONTROL APPROACHES

IoT connects many devices and entities with each other and shares information, services, and many other things that can be sensitive and private. Sufficient model and framework of access models were demanded. Some of the main approaches used in the field to secure devices, users, communication and data transmitted are as follows.
Access control authorization Models are:

1. Role Based Access Control (RBAC)

In a RBAC model, all grant authorizations deal with roles [5,6]. Users are made members of roles. User access to resources is controlled by roles. Each user is assigned with certain roles, and based on his own role; he/she can access the resources and operate them accordingly. Whenever a user needs a certain type of authority to perform an activity, he/she only has to be granted the authority of a proper role. When he/she changes his/her role inside the organization, he/she needs to revoke the permission function of the role. RBAC ensures that only authorized users are given access to certain data or resources. Role hierarchy in RBAC is a way of organizing roles to reflect the organization's lines of authority and responsibility. Junior roles appear at the bottom of the hierarchic role diagrams and senior roles at the top. The hierarchic diagrams are reflexive, transitive, and anti-symmetric.

RBAC Analysis

Due to the highly dynamic environment and the huge number of users of IoT, RBAC cannot assign permissions in advance. The reliability evaluation in the actual situation is not applicable. The new protocol includes the registration phase, login and authentication phase. In addition, the new protocol also incorporates password recovery and modification capabilities to help users manage passwords.
The analysis shows that the new method can meet the confidentiality, reliability, integrity and other key security requirements [2]. However, due to the huge number of nodes and dynamic environment of IoT and limited computing and storage capacity of an IoT node, the applicability of these types of methods will be greatly limited. It cannot be directly applied to IoT because of limitations of flexibility. Due to the highly dynamic environment and the huge number of users of IoT, RBAC cannot assign permissions in advance with traditional access control methods.

2. Attribute Based Access Control (ABAC)

ABAC is not only applied in different fields but also more flexible than other access control models. ABAC model contains subject, resource, operation and environment with attributes [7]. ABAC makes decision for access control based on one or more attributes and evaluates the value to judge whether the subject can access the resource or not. The subject can access the resource only through his or her attributes and protects the subject privacy. If the authorization cannot be revoked in time, it may have significant amount of security risks to the system. The problem of the policy repository explosion and policy conflict may occur if these authorizations are stored in the policy repository not revoked for a long time. ABAC is a logical access control model that controls access to resources by evaluating rules against the attributes of entities, operations, and the environment relevant to a request [10]. ABAC uses attributes as the basis for authorizations instead of directly defining permissions between subjects and resources. It focused on mutual authentication and secure key establishment based on ECC, which has much lower storage and communication overhead to solve constraints in resources of the IOT. ABAC model provide mutual authentication and defend attacks such as replay attack, denial of service (DoS) and ongoing dictionary attacks.

ABAC Analysis

The ABAC based authorization method has been adapted as access control policy but too heavy and complex to implement in constrained devices. This method has very low level of heterogeneity, usability and lightness. When the emergency situation happens, it is difficult to handle with the access control policy predefined. When some authorizations only used once or several times, ABAC cannot revoke them flexibly, which may lead to the problem of the policy repository explosion. Indeed, both RBAC and ABAC systems have been found to be inflexible, don't scale well, and are difficult to use and to upgrade. Moreover, the ABAC authorization process is complex, it does not apply to the highly dynamic, real-time environment of IoT and the number of rules rapidly increases with users, attributes and

growth.

3. Capability Based Access control (CAP-BAC)

In Cap-BAC, the user needs to show the service provider the authorization certificate prior to performing corresponding resource request operations. Authorization certificates are issued by the owner of a resource/service to desired users, in order to ensure that the users can request resources or services [8]. A capability based access control and rights delegation approach has, instead, the following advantages:

• Principle of Least Authority
• supports a more fine-grained access control;
• has less security issues
• does not need to manage issues related to complexity and dynamics of subject's identities.

Indeed, each capability directly identifies: the resource(s), the subject (grantee) to which the rights have been granted, the granted rights, as well as the authorization chain, while the grantee has to prove the ownership of the identity specified in the capability in order to have his/her/it access request accepted.

CAP-BAC Analysis

The main disadvantage of this solution is that it requires the ability to publish all the main certificates and to have the selection capability available when a certificate body submits a request [2]. The major limitation of model is its coarse granularity. CAPBAC model handles attacks like replay attack, man in middle, denial of service (DoS) attack.

5. UCON

UCON model includes subjects, objects and rights in combination with authorization (A) and obligation (B) and condition (C). The device (D) which control application service in IoT is subject(S) of UCON. The Att (Device) is attribute(S) contains honest and dishonest usage time of application services and some other properties also [9]. Service (S) request service information provided by services from wireless sensor network is subject (O) of UCON [12]. The attribute (O) is the Att (Service) contains the information about the services. The obligation (B) is decided according to the needs of network, depending on application services device has to perform. The condition(C) is according to the actual situation in sensor network. The Authorization (A) is decided by the device and the service and set according to needs of usage control. Authorization (A) is predicates that decide whether the device has rights to use the application service. Usage control is based on the trust threshold value of Device and Service. UCON model introduces sixteen models for secure usage control in the access control. In traditional access control models, the attributes of the subjects and objects are only changed after the access control whereas in UCON model subject's attributes and the value of object's attributes could be changed not only after access control, but also during the access control, changes in the attributes will affect the permission in the subject's next access. Concept of mutability is introduced in UCON model. UCON fundamentally improves the traditional access control models.

UCON Analysis

Access control designed for IoT should support lightweight solution and standards due to low capabilities of device, power and memory. It has low level of distribution, usability and lightness.

IV. CONCLUSION AND FUTURE SCOPE

With the increasing popularization of IoT in people's day to day lives, security of IoT is facing more and more challenges. Traditional cryptographic algorithms cannot suit to the open environment of IoT as it is too heavy for IoT devices. Lightweight and attack resistant solution is most favorable choice for IoT that gives challenges for authentication and access control of devices. Access control for IoT comprises Role Based Access Control which is widely used in traditional network. In order to access various resources and data in this type of model, user requires certain certification and authorities which comes under Attribute Based Access Control and Capability based Access Control. Existing literature survey says, there is need for dynamic and fine grained access control algorithms on constrained resources like limited memory and storage. Finally, this paper presents an overview of existing work on existing access control models with their advantages and limitations. In future, further study can be done on access control protocols and frameworks.

REFERENCES

[1] Guoping Zhang, Jiazheng Tian, "*An Extended Role Based Access Control Model for the Internet of Things*", 978-1-4244-8106-4 IEEE 2010 pp. VI-319-323.

[2] Yunpeng Zhang, Xuqing Wu, "*Access Control in Internet of Things: A Survey*", 2017 Asia-Pacific Engineering and Technology Conference (APETC 2017) ISBN: 978-1-60595-443-1

[3] Jing Liu and Yang Xiao, C. L. Philip Chen, "*Authentication and Access Control in the Internet of Things*", 2012 32nd International Conference on Distributed Computing Systems Workshops.

[4] Yahia Al-Halabi, Nisreen Raeq, Farah Abu-Dabaseh,"*Study on Access control approaches in the context of Internet of Things: A survey*", ICET2017, Antalya, Turkey.

[5] Jia Jindou, Qiu Xiaofeng, Cheng Cheng,"*Access Control Method for Web of Things based on Role and SNS*",2012 IEEE 12th International Conference on Computer and Information Technology.

[6] Guoping Zhang, Jiazheng Tian, "*An Extended Role Based Access Control Model for the Internet of Things*", 2010 International Conference on Information, Networking and Automation (ICINA)

[7] Ning YE, Yan Zhu, Ru-chuan WANG, Reza Malekian, Lin Qiao-min,"*An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things*",Appl. Math. Inf. Sci. 8, No. 4, 1-8 (2014)

[8] Sergio Gusmeroli, Salvatore Piccione, Domenico Rotondi,"*A capability-based security approach to manage access control in the Internet of Things*",Mathematical and Computer Modelling (2013),

http://dx.doi.org/10.1016/j.mcm.2013.02.006
[9] Zhang Guoping, Gong Wentao, "*The Research of Access Control Based on UCON*
in the Internet of Things", JOURNAL OF SOFTWARE, VOL. 6, NO. 4, APRIL 2011
[10] Marilyan Wolf, Dimitrios Serpanos, "*Safety and Security in Cyber Physical Systems and Internet of Things Systems*", Vol. 106, No. 1, January, IEEE 2018 pp. 9-20.
[11] Nikos Fotiou, Theodore Kotsonis, Giannis F. Marias, George C. Polyzos, " *Access Control for the Internet of Things*",2016 International Workshop on Secure Internet of Things IEEE DOI 10.1109/SioT.2016.10
[12] Inayat Ali, Sonia Sabir, Zahid Ullah, "*Internet of Things Security, Device Authentication and Access Control: A Review*", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016.
[13] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, Hongbin Zhao, " *A survey on Security and Privacy Issues in Internet of Things*", 2327-4662 IEEE 2017 pp. 1-10
[14] Parikshit N. Mahalle, Bayu Anggorojati, Neeli Rashmi Prasad, Ramjee Prasad, " *Identity Establishment and Capability Based access Control (IECAC) scheme for Internet of Things*", IEEE 2012 pp. 187-191.
[15] Mousa Alramadhan, Kewei Sha, "*An Overview of Access Control Mechanisms for Internet of Things*", 978-1-5090-2991-4/17 IEEE 2017.
[16] M. Dahiya, A.Sangwan, *and "A Review Paper on Various Attacks on Wireless Sensor Networks"* International Journal of Computer Sciences and Engineering Vol. 7(4), Apr 2019, E-ISSN: 2347-2693
[17] K.Amutha, V.Vallinayagi, "*E-security Through RFID*", International Journal of Computer Sciences and Engineering Vol. 7(8), Apr 2019, E-ISSN: 2347-2693
[18] Annie Singla, Kamal Jain, Ajay Gairola, "*Delving into Security of Networks – Time's Need*", Int. J.Sci. Res. in Network Security & Communication, Vol-2, Issue-3, PP(1-8) Oct 2014,E-ISSN: 2321-3256

Authors Profile

Meghana P. Lokhande is Assistant Professor in Computer Engineering Department at Pimpri Chinchwad College of Engineering, Pune. She earned her MTech degree from Bharati Vidyapeeth Deemed University College of Engineering, Pune. Now she is doing PhD in Computer engineering. She has published papers in International and National journals.

Dr. Dipti D. Patil is Associate Professor in Information Technology Department at MKSSS's Cummins College of Engineering for Women, Pune. She earned her doctorate in the year 2014 from Sant Gadgebaba Amravati University in Computer Science and Engineering. She pursued her UG and PG Computer Engineering from Thadomal Shahani Engineering College, Bandra of Mumbai University in 2002 and 2008 respectively. She has authored books in areas of Data Structures and Mobile healthcare. Dr. Dipti has published many research articles, which are published in various national and international Journals and conferences. She is involved in developing healthcare system prototypes and for which she has filed various national and international patents. She is contributing as editor, reviewer, Session Chair & committee member to various International conferences and Journals. Her areas of special interest include mobile healthcare, analytics, data science, artificial intelligence and Internet of Things.

