Trustworthy IoT Traditional Network Security to Authentication and Access Control Model for Heterogeneous Devices

Ms.Shilpa B.Sarvaiya[1], Dr.D.N.Satange[2]
[1]*Department of Computer Science, Vidyabharati Mahavidyalaya, Amravati*
[2]*Director, Students' Development, S.G.B.A. University, Amravati*

***Abstract*-Security is the basic requirement of any user for Internet of Things (IoT) traditional network. An internet user will not share his confidential and important data on the network unless the traditional network is trusted. IoT is considered as a collection of heterogeneous devices, such as, radio frequency identification, sensors and actuators, which form a huge traditional network, enabling not connected to computer in the network to produce a trustworthy world of services. Security and privacy are the two most important aspects of the IoT network, which includes authentication, authorization, data protection, network security, and access control. Additionally, traditional network security cannot be directly used in IoT traditional networks due to its limitations on computational capabilities and heterogeneous devices storage capacities. Authentication and Access control is the mainstay of the IoT traditional network, as all components undergo an authentication process before establishing communications between heterogeneous devices therefore, securing authentication and access control is essential to ensure that resources are only granted to the authorized users. With authentication and access control information, it sets the access rights of the subject to the object and protects heterogeneous devices from unauthorized access to ensure confidentiality and integrity of the system resources in the send and receive data signal is one of the basic security services. Current access control technology can be divided into Role-based Access Control (RBAC) and Resource Role Hierarchy Based Access Control (RRBAC). The first kind of access control model is RBAC, which is widely used in traditional networks and second is suitable for multiple security domains with different applications. In this paper focused on IoT security particularly on their authentication and access control model. Also, studies on existing evaluation schemes of IoT authentication and access control.**

Keywords- Access Control, Authentication, Attribute-Based Access Control (ABAC), Role-Based Control (RBAC), Resource Role Hierarchy Based Access Control (RRBAC).

1. INTRODUCTION

The fundamental question that needs to be answered is how we can trust the validity of the data being generated in the first place. IoT therefore needs to improve its trustworthiness before it can be used to solve challenging economic and environmental problems tied to our social lives.

Due to huge number of IoT devices and machine to machine communication feature of IoT, legacy authentication and authorization techniques are not viable for it. Devices must authenticate each other before exchanging any information between them (M2M communication) which is a challenge for researcher due to massive number of heterogeneous devices. IoT is focusing on Machine to Machine (M2M) mode of communication. For such communication nodes authentication is very important for insuring security and privacy. When two or more nodes are communicating with each other for a common objective they should authenticate each other first in order to block fake node attack. However, there is no efficient authentication mechanism for massive number of IoT devices. Authentication and access control mechanisms are capable of preventing unauthorized users from accessing the data of sensor nodes on the IoT perception layer and guaranteeing the data security effectively. User authentication is to allow legitimate user to access resources as well as to decline malicious person or attacker [1]. After authentication, access control is to restrict authenticated user to access the only data that have the privileges. However, due to the characteristics of

wireless sensor network, secure access is faced with more severe challenges. The trustworthiness to heterogeneous device authentication and access control model in IoT traditional network are discussed here. In this paper, authors focus various evaluation techniques with their parameters and supporting equations. This paper presents an overview of the existing work on trust authentication, access control models in IoT. The first access control model is role-based access control (RBAC), which is widely used in traditional networks. Adopt ABAC-based authorization method in order to access various resources and data in this type of model, users require certain certificate information that falls into ABAC. If a user has some special attributes in ABAC, it is possible to access a particular resource or piece of data. ABAC is a more flexible and scalable that abstract identity, role, and resources information of the traditional access control into entity attributes. Additionally, ABAC can support either fine-grained access control in the complex system or dynamic extension of large-scale users. The second access control model RRBAC is suitable for multiple security domains with different applications [2, 3].

The paper focuses on building an access control model and system based on trust computing, which is a new field of access control techniques that includes Access Control, Trust Computing, Internet of Things, network attacks, and cheating detection technologies. Because target access control systems can be very complex to manage, there has been substantial research in this domain, most of which has been related to attacks like self-promotion and ballot stuffing where a node falsely promotes its importance and boosts the reputation of a malicious node (by providing good recommendations) to engage in a collusion-style attack. The traditional trust computation model is inefficient in differentiating a participant object in IoT, which is designed to win trust by cheating. There is an urgent need to put forward more suitable and effective methods to ensure the security of IoT

This paper is organized as follows. Section II describes the authentication model for IoT security. Section III presents Access control model for IoT security. In section IV Authentication Evaluation Techniques for IoT security, Section V presents Access Control Evaluation Techniques for IoT security finally, section VI concludes the paper and future research.

2. AUTHENTICATION MODEL FOR IOT SECURITY

Authentication allows communicating entities to convince the identity of each other and exchange session keys. In wireless sensor network, user and terminal nodes in the communication process require mutual authentication to ensure network security, while terminal nodes require authentication mutually to prevent malicious nodes attacks. Encryption mechanism ensures confidentiality to prevent data from being stolen during communication process via encoding the data. Usually, the authentication is divided into two parts [4, 5].

(1) Authentication: authentication between user and terminal nodes ensures only the legitimate User can access the network.

(2) Key establishment: session keys should be created between the user and nodes for secure Communication.

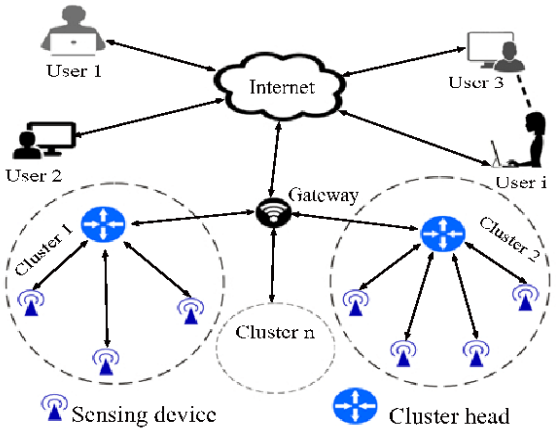

Figure 1: Authentication Model for IoT security

3. ACCESS CONTROL MODEL FOR IOT SECURITY

As discussed in Section 3, access control is the most fundamental component in trustworthy security. Many access control models have been developed in the past three decades and among all these models, Role-Based Access Control (RBAC) models [6] are most widely used in enterprises and other organizations. Role-based models can greatly cut down the cost for policy specification. Also, Role hierarchy in RBAC provides a natural representation (role hierarchy) of the structure of the users in an organization. Role faithfully describes the responsibility and authority of

the user in the position represented by the role. The RBAC model focuses on building a hierarchy of the subjects to reduce the overhead in access right specification and management but does not consider the same for the objects (i.e., the resources to be accessed). In IoT security, there are an enormous number of resources. If permissions have to be assigned for individual IoT resources to roles, permission assignment and management can have a very high complexity, likely to be infeasible [7].RBAC model also has limitations in highly open environment where no role hierarchy can be formulated [8] In RBAC, the only alignment required for interoperation is to map the roles from one domain to another and role mapping techniques has been well explored [9]. For interoperation in ABAC, need to align the attributes as well as the values for the attributes. If two systems do not have equivalent attributes, it is impossible to align them. Extended the RBAC model and created the RRBAC (Resource and Role hierarchy Based Access Control) model [10] to circumvent the problems in RBAC and ABAC discussed above. Similar to role hierarchy, IoT resources can be organized in a hierarchy and permissions can be assigned based on the resource hierarchy. By providing resource hierarchy as a part of the access control model, we can greatly simplify access rights assignments using the resource groups and privilege inheritance concept on the resource hierarchy. The high level RRBAC model is formally specified in Section 3.1. For the dynamic and open IoT systems develop a "resource role hierarchy" based access control model to support easy policy specification. An entity in the system can build a resource role hierarchy to specify its view of the other entities in the system without knowing the specific entities. Integrate the RBAC model with RRBAC so that access control policies can be specified based on the relative role hierarchy and resource hierarchy [11]. When a dynamic IoT network is formed, the other entities are mapped to the relative role hierarchy of entity based on their attributes. The attribute values are obtained by mining the societal databases and social networks. The resource role hierarchy concept is presented in Section 3.2.

3.1 Role-Based Access Control Model (RBAC)

Role-Based Access Control approach (RBAC), a policy mechanism defined roles and privileges. This approach scales better than other models. However, when talking about a huge amount of devices, managing roles for individual entities the possibility of grouping sensors and assigning roles to those that have the same rights is a good solution for this problem. For providing access rights to user, it is important to know the user's responsibilities assigned by the organization. RBAC try to reduce the gap by combining the forced organizational constraints with flexibility of explicit authorizations [12]. RBAC mostly used for controlling the access to computer resources. RBAC is very useful method for controlling what type of information users can utilize on the computer, the programs that the users execute, and the changes that the users can make. In RBAC roles for users are assigned statically, which is not used in dynamic environment. It is more difficult to change the access rights of the user without changing the specified roles of the user. RBAC is mostly preferable access control model for the local domain. Due to the static role assignment, it does not have complexity. Therefore, it needs the low attention for maintenance [13, 14]. Role is nothing but the abstractions of the user behaviour and their assigned duties [15].

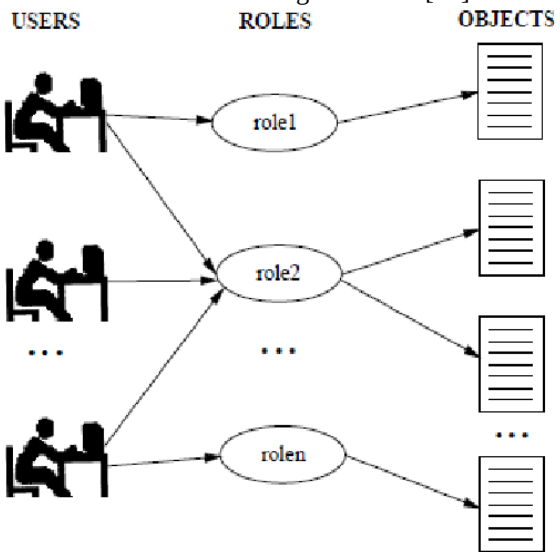

Figure 2: Role-Based Access Control Model

Essentially, in role-based access control policies need to identify the roles in the system, a role can be defined as a set of responsibilities and actions associated with a particular working activity. In an Access control security model, a role is considered as a job-related access right which can be given to the authorized users within an organization. It allows authorized user to achieve its associated responsibilities [14, 15].

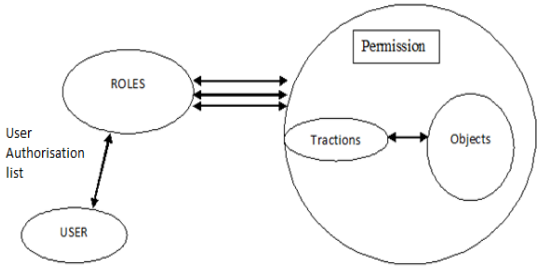

Figure 3: User-Role-Permission Mapping

A permission p is a pair < trans, objset >, where trans represents the transaction that executes on the set of objects that is objset. Consider P indicate the universal set of permissions, Trans indicate the universal set of transactions, and Obj indicates the set of objects.

3.2 Resource and Role Hierarchy Based Access Control (RRBAC)

The big difference between RRBAC and (ABAC). RRBAC is suitable for multiple security domains with different applications. Figure 4 is the structure graph of RRBAC model. From Figure 4, the users are distributed anywhere, in a school, in a company etc. In every security domain, the administrator is charge of managing the sessions and roles. Usually, the session IDs are randomly generated as a procedure for a user to perform actions. The roles are man-made according to the registration of the resources. The resources are also distributed. After a resource registers and passes the examination, it can become a legitimate resource. Surely, a valid resource is treated as a part of the domain [16].

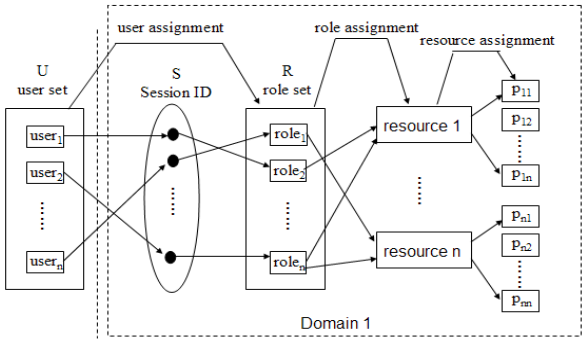

Figure 4: The structure graph of RRBAC Model [16]

4. IOT AUTHENTICATION EVALUATION TECHNIQUES

As the new and challenging authentication techniques are necessary to protect the IoT environment from various emerging attacks, evaluation of those proposed schemes are equally important to check their potency. In this section, discuss several evaluation techniques with their parameters and supporting equations [17].

A. Average Response Time

Response time is assumed to be the time taken by the server to result in the response of a request to the client. This can be affected by few factors, such as, number of users, number of request, type of requests, think time, network bandwidth, and server configuration. First response time can be executed by the time of client request and the time of first response, which is defined in equation 1.

$$T_{res} = t_{res} - t_{req} \quad (1)$$

Here T_{res}, t_{res}, t_{req} are response time, time of client request and time of first response respectively. Average response time is calculated by the mean of all response time, which is determined in equation 2.

$$T_{avg\_res} = (n/r) - T_{think} \quad (2)$$

Where T_{avg_res} is the average response time, n is the number of concurrent users. *r* is the number of requests per second the server receives. T_{think} is the average think time (in seconds).However, to obtain an accurate response time result, a user should always include think time in the equation.

B. Impact on Throughput

Throughput (TP) can be described as the amount of data passes through a system in a unit of time. In the traditional network of IoT, find out the total number of transmitted data preserved in a second. The TP can be defined in equation 3.

$$TP = \sum (Q^r_i * l_i) / T_w \quad (3)$$

Here, TP denotes throughput, while Q^r_i is the Quantity and l_i is the length of the i^{th} kind, and T_w denotes as the whole time of the simulation.

C. Packet Delivery Ratio

Packet Delivery Ratio is calculated based on the number of packets sent by the sender and the number of packets successfully received at the receiver end. However, it depends on several factors like network configuration, device capabilities, and bandwidth; therefore, it is difficult to test the network performance. Equation 4 can be used to calculate the packet delivery ratio.

$$PDR = N_{rp} / N_{sp} \quad (4)$$

Where *PDR* is Packet Delivery Ratio; N_{sp} is the total

number of sent packets, and N_{rp} is the total number of received packets. It has been identified that throughput falls when the number of nodes increases in a network. In the wireless sensor network, packet-sending circumstances are defined in the energy model, like that; energy is consumed when a packet is sent over the network. Therefore, more packet transfer cost core energy consumption. Ultimately, the packet can be discarded due to less energy or long-distance travel [17].

D. Handshake Duration

Handshaking is the process of negotiation between two network parties in the IoT network. These parties can be user, sensor, actuator, server or other nodes. As shown in Figure 5, handshaking takes place by completing the two-roundtrip message, whereas, client's discovery offers by the server and again the client's request acknowledges by the server. Duration to a handshake T_{hs} is computed at the client-end using equation 5.

$$T_{hs} = T_s + T_{res} + T_p \quad (5)$$

Where T_s is the time taken by whole session request, T_{res} is client response time and T_p denotes as processing time at the server. However, to calculate the handshake duration, a user must perform several random numbers of handshakes between the client and the server.

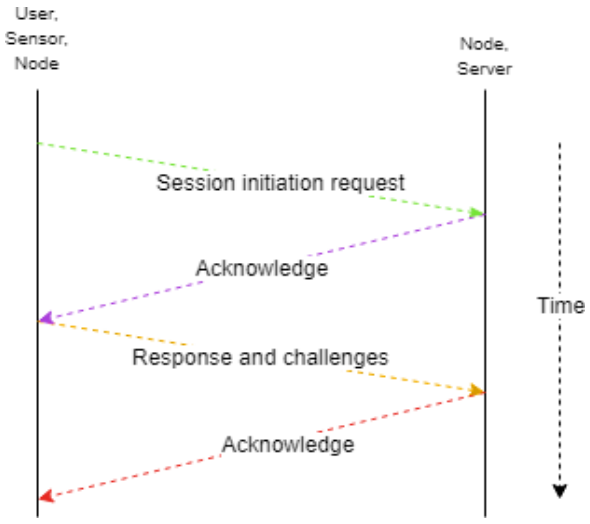

Figure 5: Four Way Authentication Handshaking.

E. End-To-End Delay

End-to-End Delay or E2ED denotes the average time to deliver packets from sender to receiver.E2ED can be calculated by using equation 6.

$$E2ED = \sum (T^r_i - T^s_{i)} / n \quad (6)$$

Here, i is the number of packets and n is the number of received packets, while T^r_i is the received and T^s_i denotes the sent timestamp for **i**th packet. E2ED is proportional to the number of sensors in the IoT network. Therefore, an increased number of nodes put up the congestion in the network.

5. IOT ACCESS CONTROL EVALUATION TECHNIQUES

Access Control technologies are known as the main elements to address the security and privacy issues in the Internet of Things. Any effective access control system should satisfy the main security properties of confidentiality (preventing unauthorized divulgation of resources), integrity (preventing resource to be modified without authorization resources), and availability (assuring access to resource by legitimate users when needed).In addition, the classification of IoT heterogeneous devices by assigning them a particular class according to their evaluation techniques. These evaluation techniques will help in building an adequate access control framework to achieve the required security level for each domain application.

A. Quantitative and Qualitative Evaluation techniques

In this section, we evaluate in both quantitative and qualitative way towards access control in IoT and their versatility for preserving security and privacy by referring to the above Role-Based Access Control Model (RBAC) and Resource Role Hierarchy Based Access Control (RRBAC) Model based on the described legend below this evaluation is highlighted as follow [18].

Legend: VH= Very High=> 5, H= High =>4, M=Medium =>3, L= Low => 2, VL= Very Low =>1, No= Null => 0

Each quality criteria is assigned a value ranging from 0 to 5, where 0 signifies not defined, 1 signifies a very low quality sufficiency,2 signifies a low quality sufficiency,3 signifies a medium quality sufficiency,4 signifies a high quality sufficiency while 5 signifies a very high quality sufficiency. These values are then used to indicate the sufficiency of each access control model's interoperability between heterogeneous devices for each security and privacy preserving analysis for IoT.

B. Evaluation of Access Control based on RBAC and RRBAC Model

The web service technology is known to provide great interoperability between heterogeneous devices. For this reason, we classify all the devices that adopt the web of think approach (based on web service) as high-quality sufficiencies in term of interoperability based on RBAC model have the following issues [18].

(1) Interoperability: the difficulty to approve a real consensus regarding the meaning of role to be shared with different applications, platforms, domains and enterprises.

(2)Role explosion: The role explosion issue justifies the critical dynamicity aspect of RBAC. Actually, RBAC defines access permissions in a static and fixed manner without taking the context of the access into consideration. As a result, a pure RBAC solution may be inappropriate for defining fine-grained access permissions based on context, and dynamics of IoT environment.

(3) Critical scalability: policies cannot evolve easily. In fact, the creation of new roles can lead to rebuilding the entire model.

(4) Nonsupport of delegation: a subject cannot grant access rights to another subject, as well as grant the right to further delegate all or part of the granted rights.

6. ANALYSIS AND DISCUSSION

The current concept of network and connectivity is going to be changed in the next few years. As it is predicted that the number of connected heterogeneous devices in the world will take over the headcount of human beings soon, this can be possible because of the expansion of the authentication and access control evaluation techniques in Internet of Things. However, security on IoT is still searching for its way to improve so that it can provide reliability and protection against threats. Again, suitable selection of authentication and access control model is one of the main important parts in security, because it is the gateway of a user or device to introduce in a network. In addition, a proper selection of authenticate devices to protect the network from attacks. Due those issues, basic RBAC model is not really a suitable solution to perform authorization functions in IoT domain applications requiring high level of interoperability/scalability, such as smart grids and smart cities. Authentication and access control is the process for giving the authority to access the specific resources, applications and system. Access control defines a set of criteria to access the heterogeneous devices of the IoT system and its resources. In Role Based model creates different authorities permissions by assigning access rights to specific roles or jobs within the IoT system then role based access control assigns these roles to users, It is effectively implemented in an environment because command and resources are assigned according to the roles.

7. CONCLUSION

The data can be perceived from any device at any moment. The powerful IoT heterogeneous devices authentication and Access Control is needed to make sure connected devices on the IoT can be trusted and access to the device resources to be what they intend to be. Accordingly, each IoT device needs a distinctive identity that can be authenticated when the device connected to the traditional network, it can track every device communicate securely with it, and inhibit it from executing detrimental processes. If a device shows unforeseen behaviour can simply revoke its privileges and compulsory to verify that the data do not change during transit. Then the network checks if this information is correct or not and ensures that the device is connected to the right network or not. It can be done using authentication and access control mechanism.

This paper is to propose a flexible Resource and Role Hierarchy Based Access Control (RRBAC) model for the dynamic IoT environment. Working from the RBAC access control model, the RRBAC access control model is more extendable, flexible and trustworthy. The main contribution of this paper is to understand the trust models enable the owners and roles to determine the trustworthiness of individual roles and users in the RBAC system respectively. RRBAC allow the data owners to use the trust evaluation techniques to decide to save their data in the IoT environment. RRBAC model provides a flexible approach for many security domains. Authentication and Access Control models supports different types of resources sharing to reduce the impact of any wrong data signal on the IoT traditional network. As a consequence, the RRBAC model provides a self-adaptive framework which is reliable enough too attached to any heterogeneous devices in the IoT environments.

REFERENCE

[1] Ms.S.B.Sarvaiya, Dr.S.S.Sherekar, Dr.V.M .Thakare," Taxonomy of Authentication Techniques in Security Attacks of Internet of Things", NCETS "Research Journey" International E- Research journal, Impact Factor 6.261 ISSN: 2348-7143,February-2019.

[2] Inayant 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.

[3] Sowmya Ravidas, et al. " Access Control in Internet-of-Things: A Survey", ResearchGate March 29, 2019.

[4] Antonio L.Maia Neto et al., " AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle" November 2016.

[5] Yungpeng Zhang,Xuqing Wu, " Access Control in Internet of Things: A Survey", Asia-Pacific Engineering and Technology Conference, ISBN: 978-1-60595-443-1, 02 October 2018.

[6] R. Sandhu, E. Coyne, H. Feinstein and C. Youman, "Role- based access control models," IEEE Computer, vol. 29, no. 2, pp. 38-47, 1996.

[7] E. Yuan and J. Tong, "Attribute based access control (ABAC) for web services," in IEEE International Conference on Web Services, 2005.

[8] C. Hu, D. Ferraiolo, D. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone, "Guide to attribute-based access control (abac) definition and considerations," in NIST Special Publication 800-162, 2014.

[9] B. Shafiq, J. Joshi, E. Bertino and A. Ghafoor, "Secure interoperation in a multidomain environment employing RBAC policies," IEEE TKDE, vol. 17, no. 11, pp. 1557- 1577.

[10] N. Solanki, Y. Huang, I.-L. Yen, F. Bastani and Y. Zhang, "Resource and role hierarchy-based access control for resourceful systems," in CompSAC, 2018.

[11] Xingdong Li, Zhengping Jin "Resource and Role Based Access Control Model", 3rd International Conference on Mechatronics and Industrial Informatics (ICMII 2015).

[12] Bokefode Jayant.D., Ubale Swapnaja A,Apte Sulbha S,Modani Dattatray G," Analysis of DAC MAC RBAC Access Control based Model for Security", International Journal of Computer Applications (0975-8887) Volume 104-No.5,October 2014.

[13] Zhuo Tang, Juan Wei, Ahmed Sallam, Kenli Li, and Ruixuan Li," A New RBAC Based Access Control Model for Cloud Computing Springer-Verlag Berlin Heidelberg 2012.

[14] Yizhu Zhao, Yanhua Zhao, Hongwei Lu," A flexible role-and resource-based access control model", International Colloquium on Computing, Communication, Control, and Management 2018 ISECS

[15] H.L.F.Ravi Sandhu, Edward J.Coyne, C.E. Youman. Role-based Access Control Models. IEEE Computer, 29 February 1996.

[16] Nidhiben Solanki,Yongtao Huang,I-Ling Yen,Farokh Bastani,Yuqun Zhang,"Resource and Role Hierarchy Based Access Control for Resourceful Systems, International Conference on Computer Software and Applications 2018 42nd IEEE.

[17] Tarak Nandy,Rafidah MD Noor,et al. " Review on Security of Internet of Things Authentication Mechanism ",IEEE,vol.7, August 26,2019.

[18] Aafaf Ouaddah, et al.," Access control in The Internet of Things: Big challenges and new opportunities", ScienceDirect, ISSN:1389-1286 17 January 2018.