Indian Journal of Science and Technology, *Vol 8(26), IPL0507, October 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Mutual Authentication Scheme for IoT Application

G. Usha Devi*, E. Vishnu Balan, M. K. Priyan and C. Gokulnath

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore - 632014, Tamil Nadu, India; ushadevi.g@vit.ac.in, vishnubalan91@gmail.com, priyanit085@gmail.com, gokulkapoor@gmail.com

Abstract

Background: Internet of Things (IoT) is the next emerging technique in which each and every thing in the world is getting connected to the internet by means of various communication techniques. By using the technique of multicasting, these things communicate with each other to transfer the data. So there is a need of an authentication scheme in order to prevent the data form getting corrupted while transmitting. As we know trillions of devices are connected in IoT, a secure communication should be implemented for the same. So a light weight authentication should be provided for IoT. **Methods**: The IoT consist of many objects, the objects may me mobile phones, refrigerator, air cooler etc. along with sensors, actuators, base station. The objects are mainly connected with sensors in order to retrieve data from each of them. Since sensor network is adhoc networks and the computational power consumed of sensor networks are also very low. Hence in the Wireless Sensor Network (WSN) many sensors are connected with one or more base station. The base station in wireless sensor network manages all the sensor nodes with the help of processor and memory. Since we are transforming from wireless sensor networks to IoT, the objects are connected to internet by providing address to individual object. So, the base station not having the capable to provide a secure communication between the objects along with sensors and internet.In this paper, we propose a new authentication scheme by means of two different approaches. Since IoT contains many numbers of objects, we connect certain objects which are in same area and provide a database for that object. The data related to particular node is stored and updated frequently in the database and maintained by Data Base Management System (DBMS) and it is connected to internet. **Results**: Whenever a user wants to access the data, the authentication is provided by means of login id with hashing password or with the help of MAC passwords. These two authentication scheme provide better when compared to existing method which are shown in results. The metrics that measures the performance of the proposed approach are the resistance against node compromise,computation overhead,communication overhead, robustness to packet loss and message entropy. **Applications**: This main application of mutual authentication scheme for IoT is to provide a authentication between the end user and the sensor network data. This method is also suitable for smart house application where the user can securely access the data from anywhere in the world.

Keywords: Data Base Management System (DBMS), Internet of Things (IoT), Light Weight Authentication, Mutual authentication, Sensor Networks

1. Introduction

The internet is a growing instance and has been creating new standards through its development and added utilization. The internet also called as “internet of computers” and this statement has transformed into “internet of people” which paved the way for social networking sites such as Facebook, LinkedIn and counting. Now this technology has been used to find out a new concept called Internet of Things (IoT). The internet of things is internet-like structure by which objects becomes the integral part of internet are provided with a unique identity. By this identity the user can easily access the objects and find the status of the object. Internet of Things (IoT) was termed by Kevin Ashton in the year 2009.

IoT has evolved from the traits of wireless technologies, Micro-Electrochemical Systems (MEMS)

** Author for correspondence*

and the internet. It is evident that internet of things has creating revolution in recent years due to the development of IPV6[1]. It is so because IPV6 has huge address space where millions and millions of objects can be included and addressed. The Internet of Things is also called as "Future Internet". The "things" in IoT perspective includes different kinds of physical elements. The physical elements may be the gadgets that we use in our day to day life such as smart phones, tablets and digital cameras. This also includes the objects in the home which can also be brought under the concept of internet of things[2-4]. These elements are connected by a large database where the information is collected and processed. By the use IoT connectivity can be enhanced which involves the use of statement "any-time, any-place" for "any-one"[5-9].

We also use the concept of Database Management Systems (DBMS) to store the information of each object. DBMS is defined as a collection of programs that enables the user to store, modify and extract information from a database. There are different kinds of DBMSs, which bound from small system that works on personal computer to huge systems that run on mainframes. A separate database is maintained for all the objects, whenever the user requests for the status of object it responses by fetching the information on the database on which the information is stored. The data collection will help the user to modify if needed. Because of this information request from the user there is need to authenticate the accessing of physical objects. A combination of all these things will create Internet of Things[10].

The Internet of Things offers a great potential to the consumers, manufacturers and firms. However, there is a difficulty in commercialization because the idea has to be developed from certain object behavior. By this concept continuous monitoring can be employed without any human interventions. We present a technique to authenticate each of these physical elements which are connected to the internet and these techniques are explained in the methodology section.

2. Light Weight Authentication Scheme

As we know trillions of devices are connected in IoT, a secure communication should be implemented for the same. So a light weight authentication should be provided for IoT[11]. The IoT consist of many objects, the objects may me mobile phones, refrigerator, air cooler etc. along with sensors, actuators, base station. The objects are mainly connected with sensors in order to retrieve data from each of them. Since sensor network is adhoc networks and the computational power consumed of sensor networks are also very low. Hence in the Wireless Sensor Network (WSN) many sensors are connected with one or more base station. The base station in wireless sensor network manages all the sensor nodes with the help of processor and memory. Since we are transforming from wireless sensor networks to IoT, the objects are connected to internet by providing address to individual object. So, the base station not having the capable to provide a secure communication between the objects along with sensors and internet.

The base station is integrated in three ways to the internet, they are front-end proxy solution, gateway solution and TCP/IP overlay solution[12]. In the first integration method the base stations simply acts as intermediate between the sensor networks and IoT. So the sensor networks connected to internet via base station and there is no direct connection between sensor networks and IoT. In the second integration method, the base station act as a gateway similarly as application layer, so it converts the lower data from sensor networks into higher data in internet and vice versa. In the third integration method, the sensor node use TCP/IP suite to communicate with the internet. So the base station forward or route the packet from sensor node to internet or vice versa. Here both are communicating directly.

Authentication scheme is not used by the above three methods, since there is no authentication in IoT, the data may get corrupted and many attacks are possible. So a light weight authentication scheme should be used in IoT. We proposed a new methodology in order to overcome the authentication issues[13]. The methodology is to provide an authentication for IoT and provide a secure communication between wireless sensor networks and the internet.

3. Proposed Methodology

The IoT consists of many nodes and each node is uniquely addressed. In the proposed approach, a certain number of nodes which are present in the same area are commonly connected with one data base. The data base is connected with Data Base Management System (DBMS) which acts as a server and manages an unauthorized access. The authentication is provided by means of two ways. In the first approach, the MAC address of system which has frequent access to the data base is stored in DBMS. So whenever the users access the data from a particular database and if the mac address of user is already stored in database, the user can easily access the data without login the page. The server obtains the mac address by using the ARP protocol from the IP address. Since the mac address is not changed, it provides a better security when compared to existing method.

In the second approach, whenever the users access the database from some other device, the user must login in order to get the data from the database. The username is provided to a particular user and the password is obtained by hashing technique. Whenever the user enters the username, the onetime password is generated in server and the server hashes the password by exponential function and sent to the users. The password is hashed by user by hashing function and the server also use the same hashing function to hash the onetime exponential password. The hashing function is shared only between the server and client. Finally if both the hashed passwords are same, the server allows the user to access the data.

4. Architecture

We proposed a new architecture in order to provide a better authentication. The basic structure is similar to wireless sensor networks with the some modification. The architecture of mutual authentication is shown in Figure 1. The base station in the wireless sensor network is replaced by database management system in Internet of Things which acts as a server for certain number of nodes that are present in the same small area.

Initially the nodes which are present in the same area are connected with the single database. For example if the things are in the single organisation, all are connected with single data base. Because of this, we can easily maintain the data of certain nodes easily. The sensors and actuators are connected with each node in order to obtain the data from the physical world. The data base maintains the information of every node, so all the data related to particular node is available in the data base.

The database of a particular node is connected with single Data Base management system which manages the database and also prevents unauthorised access. The main vision of IoT is every object in the world accessed from anywhere of the world. In order to achieve this vision the DBMS is connected with the internet and provided each node is addressed by using IPv4 addressing scheme. The end users access the data of any node via the internet. Here the nodes may be mobile phone, refrigerator, air cooler, television, etc.

5. Working Procedure

Each node should be tagged and the relevant location is also identified. The node has the data which is needed by user. This data may in any form and related to anything. If the data is not in a physical form, a sensor and actuators are used to retrieve the data. The sensor sense the information from the physical world and the actuators convert the physical world data into a user understandable form. Then this is stored in a data base along with DBMS. Whenever the user needs a particular data, it can easily access from that database after getting the authentication from DBMS.

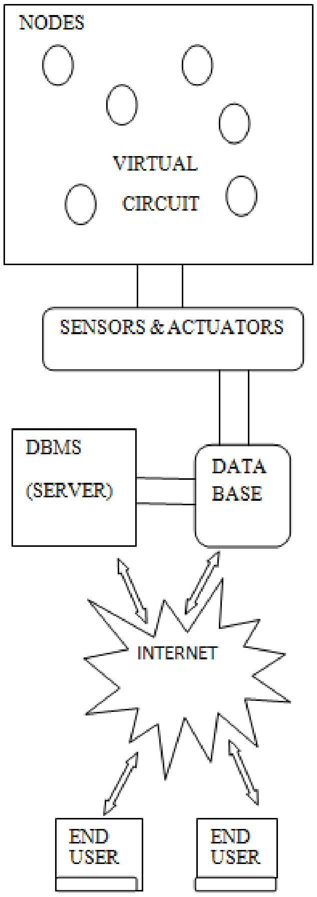

Figure 1. Proposed architecture.

6. Authentication Scheme

In this paper, the authentication scheme is established in two different approaches. In the first approach, the physical address of authorized system is stored in the Database Management System (DBMS). The DBMS consists of the list of physical addresses of all the system that can access the data directly. Whenever the user requests the data of a particular node from the database, the DBMS checks whether the particular address of a system is present or not. If the physical address is present in the server, then the server provides all the related data to that particular user. Normally, the physical address of a user is obtained from a ARP protocol by using the IP address. Since the physical address remains same for the particular system and this approach provides the authentication for certain level. The first approach takes less time to check the authentication of a particular user whereas in second approach takes more time.

In the second method, if a user access from some other system which physical address is not stored in the database, the DBMS provide the login page with one time hashing password technique. When the user request the data from the resources, then the server produce a random number in an exponential form and send the particular exponential number to the user.The key generated at the server side is a one time key (Qb) with any Random Number (Rb) and Hashing Function (S), it is given in Equation (1).

$$Qb = S^{2^{*}\,Rb} \qquad (1)$$

After receiving the one time key from the server the client also produce the key with another random number. The key Qa is generated at the client in an exponential form with another Random Number (Ra). Then the client send the one time key to server, after that a hashing function is used based on the both the random key, since both sender and receiver know the both the random number and using the same hashing function, they produce the same hashing data which is given by K_1 and K_2. This K ($K=K_1=K_2$) is used as a one-time hashing password by the user. The server checks the K value from client and K value generated at server, if the hashing password match with the server hashing password then the server allows the user to access the data from the data base.The key (Qa) produced at the user side by using another random number (Ra) is given in Equation (2).

$$Qa = S^{2^{*}Ra} \qquad (2)$$

After interchanging the value of Qa and Qb between the user and server, both the user and the server produce the hashing variable K. The hashing variable K is obtained by Qa and Qb in server and the user respectively. The hashing variable K at the server is given in Equation (3).

$$K_1 = \text{hash}\ (Qa^{2^{*}Rb}) \qquad (3)$$

Similarly the hashing variable at the user side is obtained by Qb and given in Equation (4).

$$K_2 = \text{hash}\ (Qb^{2^{*}Ra}) \qquad (4)$$

Then the hashing variable is again hashed by both the server and the client, so both are obtaining the same hashing value. The whole process is taken place whenever the user request the data base, so this second approach takes much time when compared to the first method. After obtaining the final hashing value by user is used as a one-time hashing password and the server also having the same hashing password. If both the hashing password is matched then the server allows the user to access the data. These are the two authentication schemes to increase the security level of IoT devices.

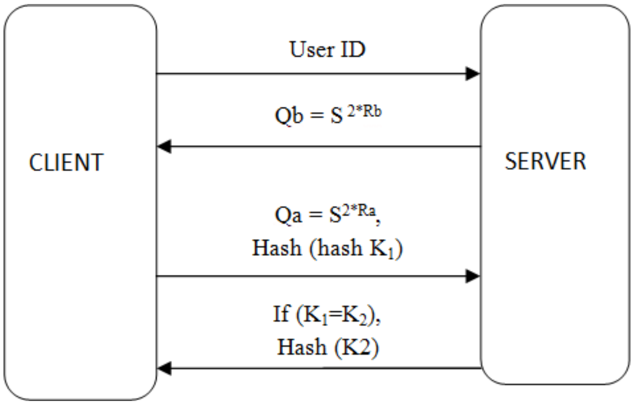

Figure 2. Authentication scheme.

The Figure 2 explains the authentication mechanism between the user and DBMS. The server issues certain user id to the regular user, whenever the user enters the user id in login page the server creates the hashing password. If the user is not authorized with the server, then the server ever creates the hashing password for that particular user. The second approach also has more advantage compared to the first approach but it takes more computational time to authenticate the user.

7. Results and Discussion

The proposed approach satisfies some of the basic parameters[14] as shown in Table 1. The first parameter is resistance against node compromise, which means the failure of particular node should not affect the other node. This property is satisfied by our approach since every node does not depend on other node. The second parameter is low computation overhead, which means the time taken to compute the key and authenticate should be minimum. This property is satisfied by our first approach, since it takes very less time for computation.

The third property is low communication overhead and this property is achieved since the less number of messages are exchanged between the server and the client. The fourth property is robustness to packet loss, which means the packet loss should not affect the efficiency of the network. If the packets are loss, we can retrieve the data from the database. Thus, satisfy the third property in our approach.

Table 1. Desired parameters

Desired Parameter	Proposed Method Achieved
Resistance against node compromise	High
Low computation overhead	Low
Low communication overhead	Low
Robustness to packet loss	High
Immediate authentication	High
Message entropy	High

The next property is immediate authentication, which also satisfied by our first approach and providing data to the user without login page by storing the physical address of the system in the database. The final property to discuss is high message entropy which is also satisfied by this approach.

8. Conclusion

The authentication mechanisms with two different approaches are described in the paper which satisfies all properties. In the first approach, the time taken to authenticate is very less when compared to the second method. But the second method provides the better results when compared to the first method. In this paper we attempted to provide a light weight authentication scheme for IoT application and provide a secure communication in transmission channels.

9. References

1. Savolainen T, Soinien J, Silverajan B. IPV6 addressing strategiesfor IoT. IEEE Sensors Journal. 2013; 13(10):3511–9.
2. Dlodo N. Adopting the internet of things technologies in environmental management in South Africa. Proceedings of International Conferenceon Environment Science and Engineering. 2012; 3:45–55.
3. Li J, Wu X, Chen H. Research on mobile digital health system based on internet of things. Electrical Power Systems and Computers (Lecture Notes in Electrical Engineering). Springer-Verlag. 2011; 99:495–502.
4. Shang X, Zhang R, Chen Y. Internet of Things (Iot) services: Architecture and its application in E-commerce. Journal of Electronics and Commerce in Organisations. 2012; 10(3):44–55.
5. Yao X, Han X. A light weight multicast authentication mechanism for small scale IoT applications. 2013; 13(10):3693–701.
6. Yasmin R, Ritter E, Wang G. An authentication framework for wireless sensor networksusing identity-based signatures. IEEE International Conference on Computer and Information Technology; 2010. p. 882–9.
7. Wang QA, Khorana H, Huang Y, Nahrstedt K. Time valid one-time signature for time-critical multicast data authentication. IEEE INFOCOM; 2009. p. 1233–41.
8. Li F, Xing P. Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal. 2013; 13(10):3677–84.
9. Suciu G, Vulpe A. Smart cities built on resilient cloud computing and secure internet of things. 19th International Conference on Control Systems and Computer Science; 2013. p. 513–8.
10. Ndibanje B, Lee HJ, Lee SG. Security analysis and improvements of authentication and access control in the internet of things. Sensors. 2014; 14:14786–805.
11. Raza Sl, Lithe: Lightweight secure CoAP for the internet of things. IEEE Sensors Journal. 2013; 13(10):3711–20.
12. Roman R, Lopez J. Integrating wireless sensor networks and the internet: A security analysis. Internet Research. 2009; 19(2):246–59.
13. Perrig A, Canetti R, Song D, Tygar JD. Efficient and secure source authentication for multicast. NDSS'01; 2001. p. 35–46.
14. Luke M, Perrig A, Whillock B. Seven cardinal properties of sensor network broadcast authentication. Proceedings of 4th ACM WorkshopSecurity Ad Hoc Sensor Network; 2006. p. 147–56.