Secured certificate based authentication protocol for Internet of Things

Shivakumar B[1],
Students, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Chinnaswamy C N[2],
Associate Professor, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Pooja T[3],
Students, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Chaitra M N[4],
Students, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Jayashree S[5]
Students, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Dr. T H Sreenivas [6]
Professor, Dept. of Information Science &Engineering
The National Institute of Engineering, Mysore, India

Abstract: Internet Of Things is the network of physical objects such as devices, vehicles, home appliances and network connectivity that enables these objects to connect data, process it and to exchange the data. It allows objects to be sensed and controlled remotely across existing network. The security and the privacy are the key issues for IOT application. The security challenges in IOT are the embedded devices which actively exchange information may have chance of control by an unauthorized person. There is currently no consensus on how to implement security in IOT on devices.

This paper is to design a new application for home devices and to implementation of new security protocol and to authenticate the end users by issuing secure certificate for controlling the home devices. The proposed protocol is with high security, high efficiency and low cost to meet the specific goals and applicable for Internet of Things applications.

Keywords: Security protocol, Internet of Things, Android App, Authentication, Smart home.

1. Introduction

The Internet of Things is a network of embedded devices with software, electronics, sensors, which enables monitoring and control of the physical environments by collecting, processing and analyzing the data generated by sensors. The IOT provides more advance services to person which connects a variety of devices such as in home area network which is controlled through an application by authorized persons.

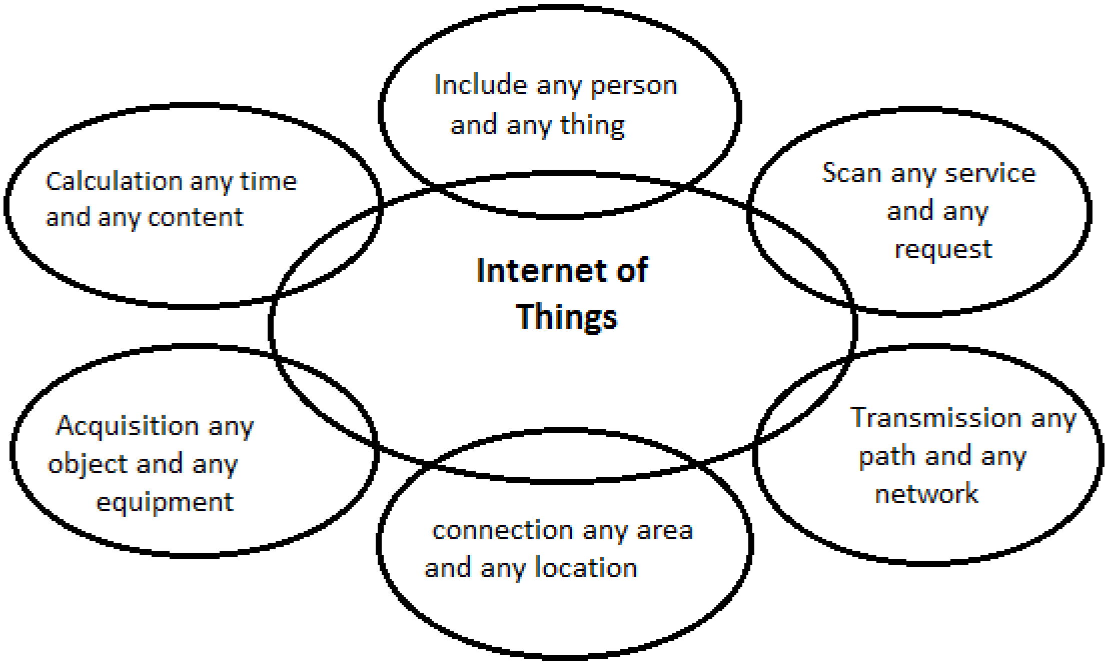
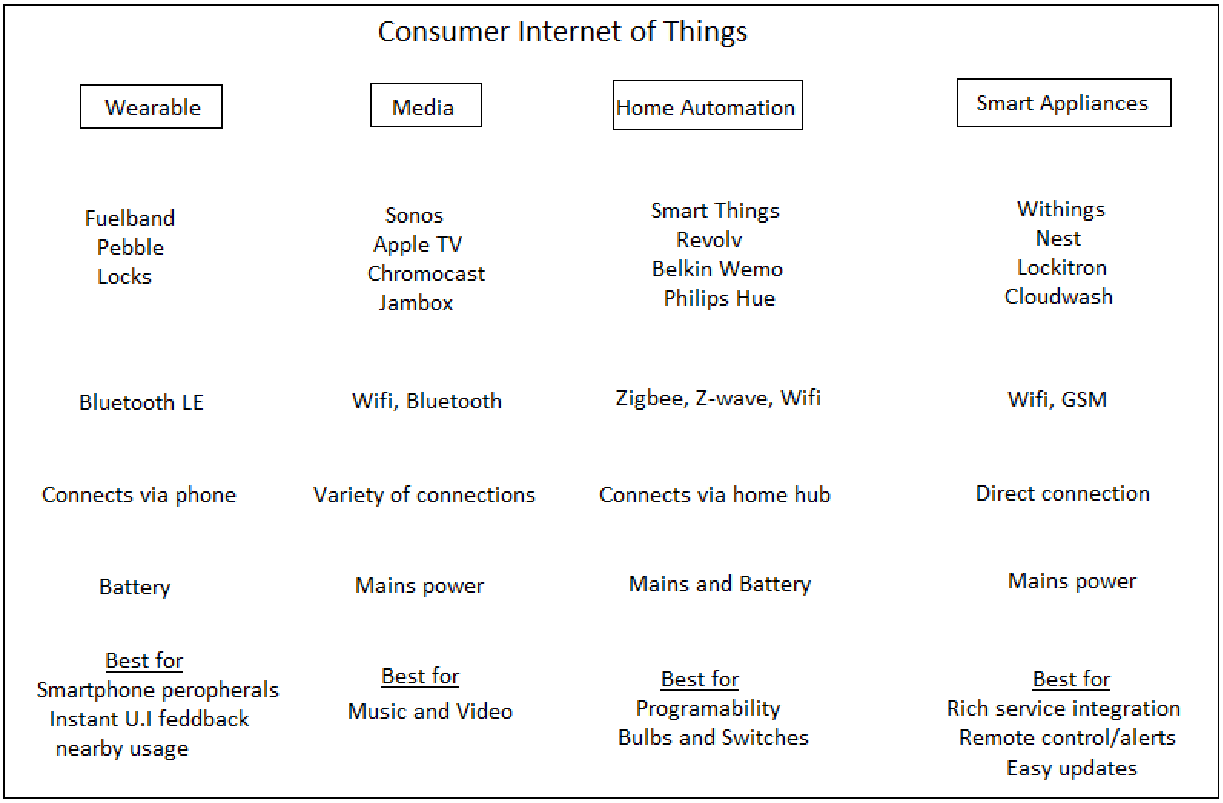

Include any person and any thing
Calculation any time and any content
Scan any service and any request
Internet of Things
Acquisition any object and any equipment
Transmission any path and any network
connection any area and any location

Fig 1: Structure of IOT

1.1 The main categories in IOT:



Consumer Internet of Things

Wearable	Media	Home Automation	Smart Appliances
Fuelband Pebble Locks	Sonos Apple TV Chromocast Jambox	Smart Things Revolv Belkin Wemo Philips Hue	Withings Nest Lockitron Cloudwash
Bluetooth LE	Wifi, Bluetooth	Zigbee, Z-wave, Wifi	Wifi, GSM
Connects via phone	Variety of connections	Connects via home hub	Direct connection
Battery	Mains power	Mains and Battery	Mains power
Best for Smartphone perophérals Instant U.I feddback nearby usage	Best for Music and Video	Best for Programability Bulbs and Switches	Best for Rich service integration Remote control/alerts Easy updates

These categories are driven by different things

- **Wearable** — battery-powered smartphone peripherals aligning around Bluetooth LE, but also devices that don't require their own connection to the web
- **Media** — music and movies
- **Home automation** — low latency interactions (sub 100ms) mean round-tripping to the web isn't possible; strong need for product interoperation.
- **Smart appliances** — products requiring their own direct network connection, with a tightly coupled service (this is where Berg is).

Smart Home is the integration of technology and services through home networking for a better quality of living.We live in an exciting time where more and more everyday items "things" are becoming smart! "Things" have sensors and can communicate to other "things" and can provide control to more "things". The price of microcontrollers with the ability to talk over a network keeps dropping and developers can now tinker and build things inexpensively.

1.2 Categories of smart home system

- Smart Outlets
- Smart Lighting
- Smart Sensors
- Smart gardener
- Smart Egg Tray

- Smart Surveillance

Although many protocols for Internet of Things have been put forward, it is still not enough to meet the complex requirements from applications. Many of them are not efficient enough to adapt the device diversity and timely communication environment. The powerful embedded devices such as smart phones and tablets will occupy the great part of the IOT. The different devices not only bring kinds of applications, but also many problems, especially in terms of privacy and security issues.

This paper is on design of a security protocol for Internet of Things through an Android App, and implementation of this corresponding security protocol on the embedded devices. This protocol will cover the integrity of messages and authentication of each client by providing an efficient authentication mechanism. By this paper secure communication is implemented on embedded devices.

1.3 Advantages of the system

With the internet and android app this application can be utilized more thoroughly.

- User-friendly: Smart phone with attractive GUI, User can perform action just with touch of the single button. Every action on the interface can be performed intuitively without costing extra learning time.
- Security: This approach is to incorporate strong security for home devices by authentication process.
- Accessible: This application can be accessed remotely through internet.

In this paper, we begin with introduction of preliminaries. The literature survey proposed in section II which describes about the related existing systems. The design procedure and architecture of the system is described in section III. The conclusion is given in section IV.

2. Literature survey

IOT is generally divided into three layers: perception layer, network layer and application layer. This hierarchy determines that the design of security mechanisms of things should base on technical Characteristics of each layer. Data encryption technology aims to protect the confidentiality and also PKI (Public Key Infrastructure) to achieve two-way public key certificate based strong authentication can resolve the physical authentication problem in IOT [1].

For this paper we conducted the thorough survey on the IOT by addressing almost every aspect of the IOT including different visions of paradigm. There are two major problems with regards to security, data integrity and authentication. It is difficult to ensure authentication especially against active attacks. Because it normally requires an authority center and appropriate infrastructures, working on exchanging appropriate messages with nodes. This is not available in some IOT scenarios. To ensure the data integrity, traditional cryptographic methodologies are preferred[2].

The analysis of various financial instruments is called security analysis. IOT which is a piece of small area with self-system obtain achievement. It can promote the development of IOT is some extent. But there are some serious hidden danger and potential crisis problems and analyzing the existed security risks of the IOT network transmission. Security requirements of sensor storage, processing, transmitting information and prevents unauthorized accessing even illegal operation called confidentiality [3].

As to the security, The IOT will be faced with the more severe challenges. They are the following reasons: 1. The IOT extends the internet through the traditional internet, mobile network and sensor network. 2. Everything will be connected to the internet, and 3. These things will be communicate with each other. Therefore, the new security and privacy problems will arise. Research issues for confidentiality, authenticity, and integrity of data in the IOT. Security and privacy are the key issues for IOT applications and still face some enormous challenges. In order to facilitate this emerging domain, the research progress of IOT, and pay attention to the security the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms. The other main research target in sensors is privacy and privacy is also a major problem. We should adopt the mechanisms to protect the privacy of humans and objects in the physical world. Most times people are often unaware of sensors in their life, so we need to set up regulations to preserve the privacy of people[4].

Tagging Mechanism for home network access control the devices that are given access to the networks should be assigned a particular tag by the centralized router. Authentication mechanism section that a hash is maintained at the centralized server. The tag will be maintained in the hash and determines the access level to the device or sensor into our private network along with device privileges [5].

Smart things is the easiest way to turn your home into a smart home like a monitor, control and secure your home from anywhere. To incorporate strong security in deploying IOT for smart home system, together with due to consideration given to user convenience in operating the system. The IOT smart home system runs on convection Wi-Fi network. A Wi-Fi gateway is to use as center node of the system to perform the system initial configuration.

It is responsible for authenticating the communication between the IOT devices as well as providing a mean for the user setup, access control the software through Android based mobile device. Security challenges in IOT include privacy, authentication and secure end to end connection. Security and convenience are the two major requirements for successful deployment of IOT in the smart home system based on Wi-Fi network. The proposed system uses a gateway to provide a better authentication process [6].

3. Design and architecture

A. **Architecture and General Approach refer fig. 3**

B. **IOT App:** IOT App is an android application to provide secured access and control devices connected in home area network. The application will present the user with an interface where he can login and then register to IOT server.IOT server will take login credential, IMEI, mobile number of user, to authenticate and their by giving unique certificate using hashing technique and hence declaring completion registration process. The command to control the device is manually given by the user using IOT app.Home devices which are connected to home PC is intern connected to IOT server. Home PC is installed with software which keeps checking for any new command by IOT server.

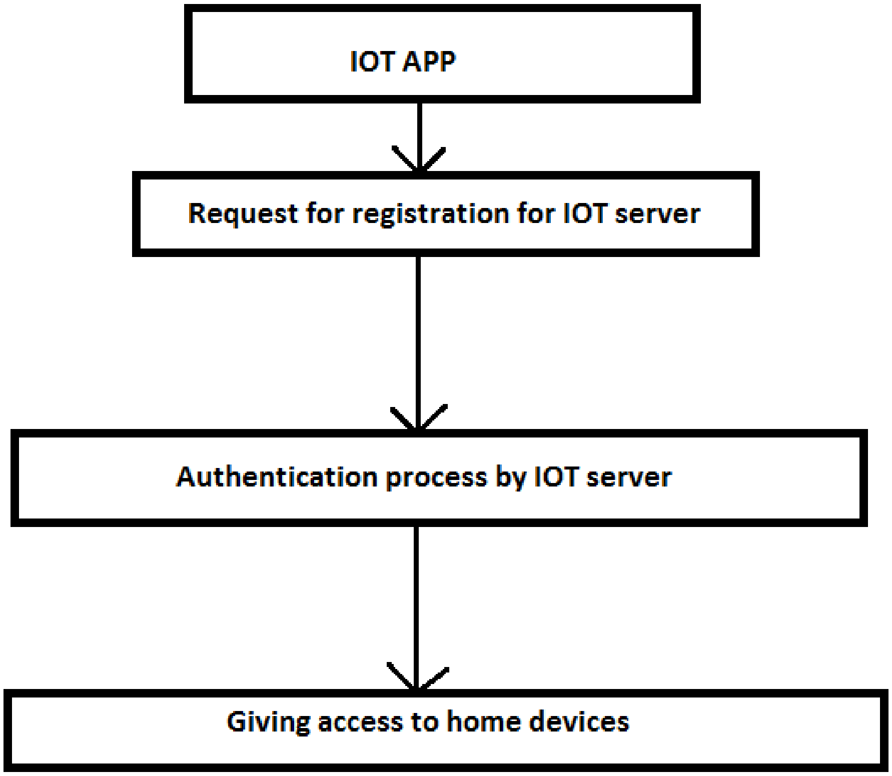

IOT APP
Request for registration for IOT server
Authentication process by IOT server
Giving access to home devices

Fig 3: General approach

3.1 Security protocol:

The core of the point to point security system for the Internet of Things is the security protocol. This protocol is the base of all system's communication and authentication. There are two main parts in this security protocol: Registration and Communication. The structure and design of this protocol mainly focus on high security, high efficiency and low cost. The registration process is carried out between recently joined user and server. The user will download the IOT App and enter details for registration like User name, password and mobile number. The user details will be sent to IOT server and the server will fetch IMEI number of user internally. Based on IMEI number, user name, password and mobile number along with the concept of SHA-1(Secure Hashing Algorithm) the certificate is generated and stored by IOT server. The requested user is approved by the server and the approved user will become the active user of the application and server will reply to the user with the acknowledgement of registered successfully.

The type of messages transmitted during first registration process.

(1) User to server: SSL connection request message.
(2) User to server: Registration request message
(3) Server to User: Registration reply message.

During the communication process, the user will login with user name and password with the IOT App. The server will check login user as registered/authorized user. For authorized users session will be created to control the device. By the use of random class IOT server will generate the token. This token is considered as session key. The session key is given to both user and home PC. By exchanging the session keys the user and home PC will communicate with each other. The user should communicate within the given session time. The secure message is transmitted within the session time.

3.2 Features of IOT App:

After downloading the IOT App,users will register himself to IOT server. Registration process was discussed in general approach (A).Certificate will be generated by IOT server for requested users. Certificate will be used internally by IOT server.

3.3Working of IOT server:

During signup process, The IOT server takes login credentials of user and maintains its database.

Username	Password

During registration process IOT server adds new row to its database.

The row contains are,

Username	Password	Mobile no	IMEI	Approved
Yes	Yes	Yes	Yes	Yes/No

Once the registration process completes, approved status will be updated, which means to give permission to authorized person and also storing corresponding digital certificate.

3.5 The digital certificate:

The digital certificate is generated by the combination of mobile IMEI, Cell phone number, user name and password. By taking these details the digital certificate is generated by the concept of SHA-1 (Securing Hashing Algorithm).

3.6 Home PC:

Home PC should be working continuously.Software installed in home PC contains list of IMEI member of home members. Command given by home members are accepted processed and actions are perform accordingly.

4. Conclusion and Future enhancement

This paper provides an efficient security protocol for the Internet of Things through IOT App. The protocol efficiency and security on embedded devices has been significantly improved. Security and authentication mechanism is improved in Internet of Things. Equipped with this protection, people's privacy could be well protected in the Internet of Things. This also promotes the development of the Internet of Things.

5. References

[1] Xu Xiaohui School of computer, Wuhan University School of economics and management, “Study on Security Problems and Key Technologies of The Internet of Things” Wuhan University Wuhan, China. 2013.
[2] Atzori, Luigi; Iera, Antonio; Morabito, Giacomo, “The Internet of Things: A survey” Computer Networks, 2010, Vol.54 (15), pp.2787- 2805 [Peer Reviewed Journal]
[3] Gan, Gang ; Lu, Zeyong ; Jiang, Jun, “Internet of Things Security Analysis” 2011 International Conference on Internet Technology and Applications, Aug. 2011, pp.1-4
[4] Suo, Hui ; Wan, Jiafu ; Zou, Caifeng ; Liu, Jianqi, “Security in the Internet of Things: A Review” 2012 International Conference on Computer Science and Electronics Engineering, March 2012, Vol.3, pp.648-651
[5] Zou, Caifeng, Lu, Zeyong, Morabito, Giacomo, “Access control for IOT devices home automation, of computer science and electronic engineering, jan 2014
[6] Freddy K Santoso, and Nicholas C H VunSchool, “Securing IOT for Smart Home System” of Computer Engineering, Nanyang Technological University, Singapore. 2015.
[7] Hao Zhang, Tingting Zhang “ A peer to peer security protocol for Internet of Things “Computer Science and Technology Donghua University, jan 2015.