Identity Management Framework for Cloud Based Internet of Things

Susmita Horrow
Department of Mathematics
IIT Roorkee
India
hsusmita4@gmail.com

Anjali Sardana
Department of Electronics and Computer Engineering
IIT Roorkee
India
dr.anjalisardana@gmail.com

Abstract— **Internet of Things is emerging as next generation technology with a vision of a connected world where everything is connected whether it is a person, a thing or a device. The connected things are able to exchange data including their identities, physical properties and information gathered from the environment. Hence they actively participate in decision making. The identification technologies like RFID have empowered the concept of Internet of Things by enabling the unique identification of things. The cloud computing technology has made the tasks of processing huge amount of data produced by the devices easier. But in order to make the system scalable, it must be able to handle the devices that are growing day by day. Hence there is a need of proper identity management. This paper discusses requirement of identity management and then presents a framework for identity management for Cloud based Internet of Things.**

Keywords- Identity Management, Internet of Things, Cloud Computing

I. INTRODUCTION

Internet of Things comes with a promise of smart world where intelligent devices form collaboration with each other to exchange information among them as well as gather information from the environment and take appropriate decision. Heer et al define Internet of Things as the interconnection of highly heterogeneous networked entities which include various kinds of communication such as Human to Human (H2H), Human to Thing (H2T), Thing to Thing (T2T) and Things to Things [4]. Internet of Things generally consist of five components such as (1) sensors to collect and transmit data, (2) Actuator to trigger a device for particular function, (3) Computing node to process information sent by the sensor, (4) Receiver to receiver message from other devices or computing nodes and (5) Communicator to pass messages form one component to another.

As an illustration, let us consider a scenario of smart home where a sensor gathers information regarding temperature and humidity. The sensor sends the gathered information to the computing node. The computing node processes all the information it has and accordingly appropriate decision is taken. Then the actuator is invoked and is given instruction to regulate the concerned device, for example air condition to tune appropriate temperature. Here the network works as a communicator. This is illustrated in figure 1.

The concept of Internet of Things has attracted both academics and industry. Hence this concept is maturing at a remarkable speed. But cloud computing has accelerated the development of IoT owing to its characteristics like provisioning of computing resources on demand. The job of computing node is handed over to cloud.

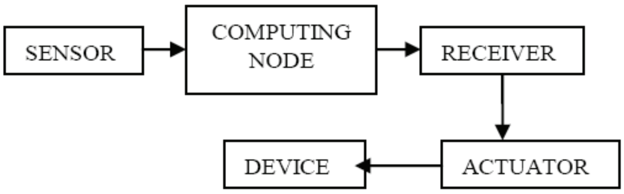

Figure 1.Simplified Working Principle of IoT

Though the concept of Internet of Things is very appealing, as long as security issues are not resolved, it cannot grow. Identity management is one of the key issues in the field of IoT. The goal of IoT is to connect the things around us so that they can communicate. In order to communicate, they must identify each other. At present, the identification, technology includes RFID, barcodes, 2D tags, biometry etc. But there must be unique agreed upon policy in terms of identification of things. In this work we have presented an Identity Management Framework for cloud based Internet of Things. By cloud based IoT, we mean, we have a number of sensors, receivers, actuators, devices and the task of processing information is given to cloud. In other words in cloud based internet of things, cloud computing is like the human brain and internet of things are as human facial features and limbs [5].

The rest of the paper is organized as follows. Section 2 discusses the issues of identity management in IoT. Section 3 illustrates the proposed framework. Section 4 concludes with discussion and implication to future work.

II. ISSUES OF IDENTITY MANAGEMENT IN CLOUD BASED INTERNET OF THINGS

The main idea behind cloud based internet of things is to have centralized control over the functioning of Internet of Things by leveraging the power of cloud for storage and processing of information. In internetwork of things, the devices may belong to more than one network. In this case, each time, any sensor device is triggered, it has to send the gathered information to the requesting computing node. Instead of issuing queries to the sensors, it is better to store the information in a centralized location where the

SecurIT'12, August 17-19, 2012, Kollam, Kerala, India
Copyright 2012 ACM 978-1-4503-1822-8/12/08... $15.00

information can be retrieved whenever required. In cloud based system, this information is stored in cloud. Now the cloud will be receiving huge amount of information from various different kinds of sensors. Hence the cloud must keep track of the identity of each sensors, it is going to getting information from.

Each network performs different kinds of operation on the information sent by the sensor node to produce processed information which can be used for further decision making. These operations are generally computation intensive which can be hosted over the cloud. The processed information is retrieved by the actuator/ receivers. Hence there is a need of managing the identity of the services hosted over the cloud. Figure 2 illustrates the traditional IoT and cloud based IoT.

The following section discusses certain issues of identity management.

Sensors must authenticate themselves as user of cloud. They must convince cloud that they are authenticated to store information in cloud.

The receiving nodes also need to authenticate themselves that they are eligible to get information from the cloud.

Again the cloud must also take care of sensors/receivers relationships. There are a number of network of things. One thing/device may be the part of more than one network. Hence an authorization mechanism must be enforced that receiver node can get information only from sensors, it is authorized to.

There may be devices/ things which dynamically change the membership of a network. The situation might arise that at certain point of time, a sensor belongs to a certain network. Hence only certain set of receivers are eligible to access the information produced by the sensor. When the sensor changes location, then some other set of receivers become eligible to access the information.

There may be issues of identity theft, issues like redirection of information to wrong receivers.

III. IDENTITY MANAGEMENT FRAMEWORK

In our proposed cloud based Internet of Things, we have identified mainly four components which interact with each other and with cloud. These are discussed below.

- Environment: This is the surrounding of sensors and receivers. Sensors are responsible to gather information regarding this entity. Receivers perform action on this entity directly or indirectly based on the results produced.
- Sensors: They do the job of information gathering.
- Receivers: They act on the results produced by the computing node.
- Network: A network is characterized by a type of sensors, receivers.
- Services: Services refer to the computational task that is hosted over the cloud.

The proposed identity management framework consists of two modules namely Identity Manager and Service Manager. Identity Manager is like an authentication module which authenticates the sensors, receivers and services. Service Manager acts as an authorization module which defines the accessibility of a service to the sensor information and the accessibility of receiver to the information provided by the particular service. Figure 3 shows the basic components of the framework and the work flow of the system.

The sensor needs to authenticate itself to the cloud. Once it gets authenticated, it can upload the information gathered from environment to the cloud. This is stored in the cloud storage denoted by “Database: Information sent by sensors “in the figure. The services also need to authenticate themselves to get access of the information sent by the sensors. They process information and store them in the database which is denoted by “Database: Processed Information”. In order to retrieve this information, the receivers need to subscribe to these services.

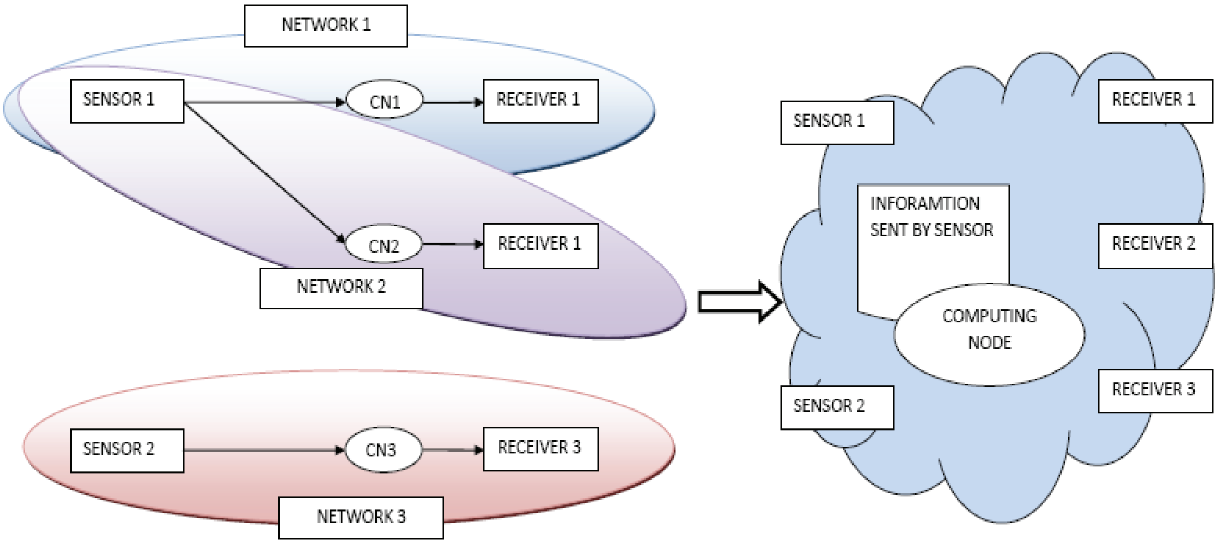

Figure 2. Difference between traditional IoT and Cloud Based IoT

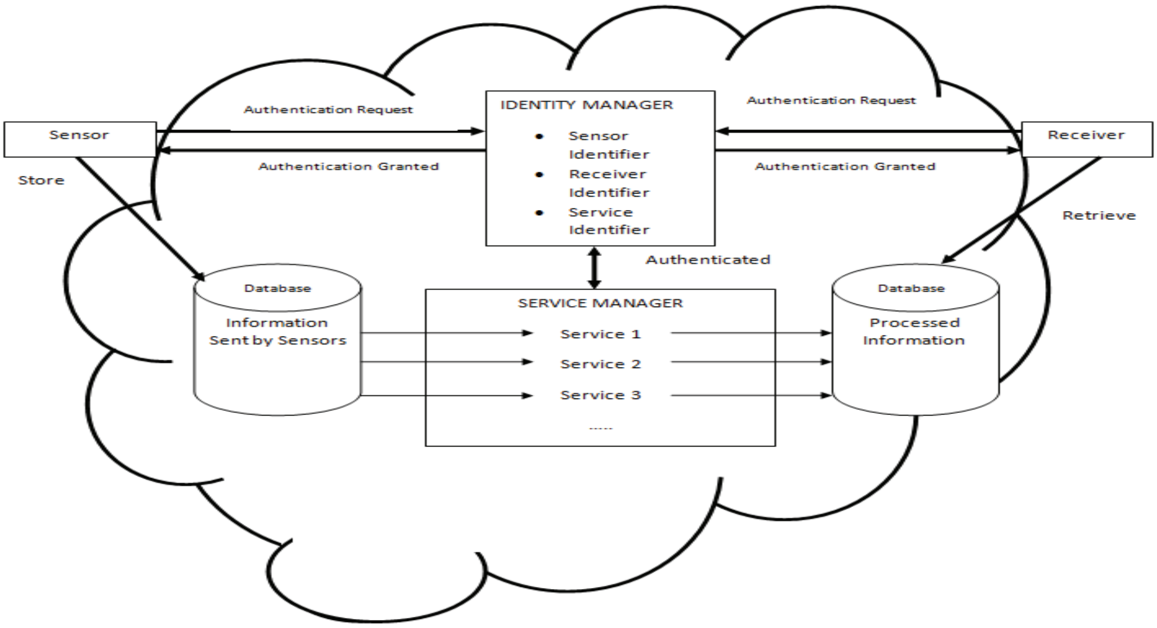

Figure 3. Identity Management Framework

A. *Basic Functions of the Framework*

The following are the basic functions of the framework.

- Registration of sensors and receiver device to the cloud
- Identification of hosted Services
- Authentication/ Login of sensors and receiver device
- Addition of new device
- Deletion of existing device
- Relocation of devices

*1) Registration:*In order to register the sensor and receiver devices, they need to provide their unique identification mark either in the form of RFID, biometry or barcode and the location of the device. There are different kinds of sensors and receivers. Hence each sensor registered in the cloud is identified as tuple <Sensor Type, Instance No>. Similarly the receiver is identified as the tuple <Receiver Type, Instance No>. Each sensor and receiver is associated with particular location. So for each sensor and receiver, the following information is maintained by the Identity Manager.

Sensor = {Sensor ID<Sensor Type, Instance No>, Location ID}

Receiver = {Receiver ID<Receiver Type, Instance No>, Location ID}

*2) Identification of services:*As discussed before, by service we mean the computation/ analysis task that have to be performed on the information provided by the sensor. Each service is characterized by the type of sensor data it is using and the type of receiver to which it is providing service. So each service must be uniquely identified. Like sensors and receivers, the service can also be identified by the tuple <Service Type, Instance No>. The identity manager must provide information regarding the sensors to which the services are subscribed to and the receivers which are subscribed to the service. The following information is maintained by the Identity Manager.

Service = {Service ID <Service Type, Instance No>, Sensor List, Receiver List}

*3) Authentication :*Once the devices have registered themselves, they are authenticated by the tuples <Device ID, Instance No>.

4) Additon of new device: When a device is registered for the system, it is provided with a unique ID and notification is sent regarding the new member.

*5) Deletion of devices:*When any device leaves the network, then this information must be reflected in the database containing the sensor registration and service registration information.

6) Relocation of devices: When device changes location, the sensor will gather information from another environment. Now the sensor will pass information to the service corresponding to the new environment. In this case, the Location ID associated with the device changes. Hence the service which is associated the device must invalidate the information provided. Then the device should be associated the service corresponding to the new location.

B. *Formation of Network*

According to the definition of IoT, the basic unit of IoT is the network of things. Each network is characterized by the type of sensors, receivers, actuators. Each network has different requirements and needs different kinds of services. When a new network has to be created, first its location has to be mentioned. Then it will be given the list of sensors and receivers which are available in that location. Accordingly, the network can subscribe to appropriate service. For easy management of the working of IoT, each network is assigned unique ID.

IV. Conclusion

In this work we have discusses the requirement of management in cloud based IoT and proposed a framework to address those issues. The framework follows a Publisher –Subscriber approach for proper functioning of Internet of Things. This work brings cloud into picture to be the central point of Publisher- Subscriber approach. The future work is directed to develop the protocols to implement the proposed architecture.

References

[1] P. Mahalle, S. Babar, N.R. Prasad, and R. Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges*,"* Communications in Computer and Information Science, vol. 89, 2010, pp. 430-439. DOI=http://dx.doi.org/10.1007/978-3-642-14478-3_43.

[2] A. Sarma, and J. Girao, "Identities in the Future Internet of Things". Wireless Personal Communication, vol. 49, May 2009, pp. 353-363. DOI= http://dx.doi.org/10.1007/s11277-009-9697-0.

[3] P. Parwakar, " From Internet of Things Towards Cloud of Things"*,* Second International Conference on Computers and Communication Technology, Allahabad, India, September 15-17, 2011, pp.329-333. DOI= http://dx.doi.org/10.1109/ICCCT.2011.6075156.

[4] T. Heer, O. Morchony, R. Hummen, S.L. Keoh, S.S Kumar, and K. Wehlre," Security Challenges in the IP-based Internet of Things", Wireless Personal Communications: An International Journal Archive.vol 61, Issue 3, Kluwer Academic Publishers Hingham, MA, USA ,Dec. 2011,pp. 527-542. DOI= http://dx.doi.org/10.1007/s11277-011-0385-5.

[5] H. Wang, P. Zhu, Y. Yu, and Q. Yuan."Cloud computing based on internet of things," Second International Conference on Mechanic Automation and Control Engineering ,Hohhot, China, July 15-17, 2011, pp. 1106-1108. DOI= http://dx.doi.org/10.1109/MACE.2011.5987128.

[6] G.C. Fox, and S. Kamburugamuve, "Architecture and Measured Characteristics of a Cloud Based Internet of Things API", International Conference on Collaboration Technologies and Systems, Denver, Colorado, USA, May 21-25, 2012.