Internet of Everything and Secure Cloud for Real World Data Management

Ramya.P
Department of ECE
Gudlavalleru Engineering College

Priyadarshini.V
Department of ECE
Gudlavalleru Engineering College

Chandu.P
Department of CSE
Gudlavalleru Engineering College

ABSTRACT

Now-a-days the idea of Internet of Things (IoT) is not merely a dream, it is a reality. With the integration of Internet and wireless technologies, connecting number of devices to Internet is exponentially increasing. Now the current scenario of IoT is turning to Internet of Everything (IoE) i.e. smart cities are now real concept. With IoE people will be connected in more relevant ways with the help of sensors. Devices will connect data and stream through Internet to a server where the data is processed .IoE plays crucial role in many areas like water, waste, power managements, traffic control, healthcare etc. The concept of cloud in IoE plays a pivotal role as it is the efficient way to manage and process information.

Keywords

IoT, IoE, cloud, sensor

1. INTRODUCTION

Internet of Things which initially was considered as extension of Radio Frequency Identification (RFID) is now a vision for future advancements. IoT comprises of Internet, devices such as sensors, smart phones etc. Now-a- days sensors are being incorporated in many objects called smart objects. These objects form networks. With the extent of IPv6 in future which can support 2128 addresses provides IP address for almost everyone. Interfaces, microcontrollers, sensors, wireless technologies, actuators, cloud technologies contribute to the advancements in IoT. With the growing usage of WiFi, WiMAX wireless Internet connectivity the idea of smart connectivity using network resources plays a major role in IoT. The sharing of data across networks can be done using a storage cloud. In this paper we discuss about the challenges, architecture in IoE.

2. INTERNET OF ENVIRONMENT (IoE)

IoT can be considered as networks of networks. The major benefits of IoT include the following:

- Communication
- Control
- Cost conservation

However there are challenges to IoT. They are usage of IPv6 in order to provide IP addresses for sensors. These sensors can be RFID, Zigbee, WI-Fi, Bluetooth etc. They can also have 3G, 4G, GPRS, GSM connectivity. Sensors send, receive information and trigger actions w.r.t the information i.e. a sensor can send notifications about the status of the device (on or off). For example if a sensor is placed on a refrigerator it can send information to smart phone or other smart device about its status. Commands can be sent back to the device via smart phone. Also sensors need batteries. As IoE involves numerous sensors removal of batteries when they are out of charge is a risky process. Therefore the idea of sensors generating electricity through solar or wind energy is obvious choice. Also while developing IoT standards are to be followed for communication between sensors. Things in IoT include devices, sensors which are connected together and are connected to Internet. In IoE more sensors will be placed in homes and daily usage items like refrigerators, vehicles, TVs etc obviously leading to the concept of smart cities whose services include smart traffic control, smart lighting, smart power management, smart waste management etc.

Therefore the main concepts in IoE includes the following

A. Interconnectivity

As IoE will create a network of billions of wireless things (green related i.e. eco-friendly applications) communicating with each other, there should be proper interconnectivity between people, devices and sensors.

B. Storing and management of data

The data collected from devices, people, sensors should be stored and processed. The data processed should be sent to relevant users.

C. Security

While using wireless smart devices security threats may arise during sharing of data For example Proofpoint research discovered that 25 percent of malicious email came from things that are conventional computers but from home-networking devices like routers. Therefore security is a major concern in IoE and hence energy efficient encryption methods should be followed.

D. Architecture

In order to maximize interoperability between heterogeneous systems say between people, smart devices, software there is a need of open architecture which is well defined and follows a decentralized and distributed approach. IoT can be classified into three types. They are

- Consumer
- Machine to Machine (M2M)
- Industrial

1) Consumer IoT: It is characterized as a human interaction with a device. For example a human interacting with a smart phone say a user needs to stream a video using mobile. i.e. the communication is between the server and client streaming of large amounts of data.

2) Machine to Machine IoT: Typical examples of M2M are monitoring applications where an operator (not human, a controller) is involved for tracking. Tracking a vehicle is a most common example. This type of applications sends small amounts of data.

3) Industrial IoT: These are many to many applications wherein groups of nodes work together to accomplish a task. Data transfers between the nodes are quite often in order to convey the status. The nodes are not expensive and are usually wireless, twisted pair cables which have bandwidth compared to Ethernet. Loss of packets occurs due to noise, interference as these links are less reliable. Therefore the protocol stack must recover from the losses and hence the concept of packet retransmission is obvious and the failure should be confirmed through a message.

3. CLOUD COMPUTING IN IoE

As billions of smart devices are involved in IoE the data organization is a difficult aspect. Cloud computing is an efficient way of storing and managing data. The things in IoE form themselves into their own clouds. Each cloud can have its own operating system. Cloud integrates storage and computation. Cloud can handle the speed and volume of data that is received. Also it is accessible to any device anywhere. For example in smart cities cloud platform is intended to deliver services to people through mobile access, home based access etc. Smart devices with embedded sensors will feed data to cloud for analysis. Cloud providers have number of data centres for increasing data coverage. Central servers are maintained at backend which provide high computing performance. Public cloud providers have large infrastructure in order to offer pay-on services for millions of users. Systems in cloud convert data to insight and provide cost effective services.

However there are challenges for the cloud to connect to IoT. They are Quality of Service (QoS), reliability, security, energy efficiency, interoperability, portability etc.

Fig 1: IoT using Cloud

The hardware and maintenance of the servers and database in the cloud is again a challenge. If there is a need of high computational power the number of storage nodes in the cluster has to be increased. If the hardware is not required the nodes in the cluster can be reduced. In this way optimization can be provided with respect to both cost and computational power in the cloud.

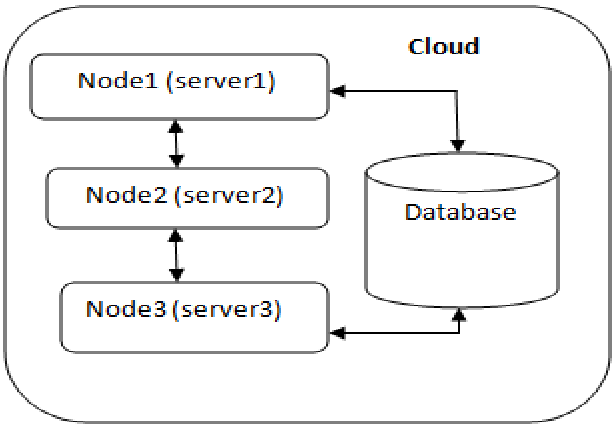

Fig 2: Cloud containing storage nodes

Cloud also provides virtual storage either through clusters or virtualized physical storage. The main task is real time processing of data i.e. receive data from sensors, process it and extract the information. Also a cloud needs a gateway which hosts the user to communicate with the devices in IoT. Gateways which can operate at network layer are routers or proxy servers which routes between networks.

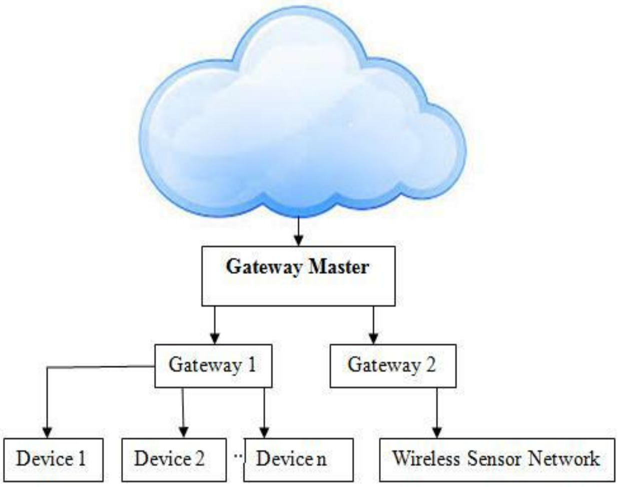

Fig 3: Architecture of cloud in IoT

In this paper we propose the concept of Gateway master which is used in the architecture to manage different gateways connected to the cloud. The applications which need to contact devices first contact gateway master to get the information. The master should be designed in such a way that it should handle all the gateway failures and send notifications. In this paper we also propose secure erasure cloud code based storage system with secure data forwarding. Design and implementation of a secure, reliable storage cloud system that supports multi-functionality is a challenging task. Therefore in this paper we propose integration of proxy re-encoding scheme [6] with erasure coding. This method supports both encoding, forwarding and decrypting data. In this scheme a proxy server transfers a cipher key under public key to another proxy server under another public key using re-encoding key. Messages are encoded by the client and are stored in storage server. When sharing is needed the client sends re-encoding key to the storage server which re-encodes the messages to the authorized client. To decode a message of

1000 blocks, they are encoded into n codeword symbols restricting each key server to partially decrypt only two codeword symbols. We also propose Key-private proxy re-encoding schemes. When a re-encoding key, a proxy server cannot identify the recipient. Thus this kind of proxy re-encoding schemes provides high privacy. The development side of the IoT cloud includes the software i.e. writing a sensor, client, library, repository, modules, configuration files etc. The sensor initializes the libraries in the cloud also the configuration files are used to set the required setting for networking between devices and cloud.

The figure Fig. 4 shows the home automation can be done using a smart phone. The air conditioners, televisions, refrigerators etc in the home can be controlled by simply using a smart phone. This can be done by using Application Programming Interfaces (APIs). The APIs can be at sensor side and client or user side.

3.1. Sensor API

Sensor APIs provide Interrupt Service Routines (ISRs) for controlling sensors like ON, OFF, STATUS etc i.e. to send and receive data and control messages to and from clients respectively.

3.2. Client API

Client API includes classes for providing subscription for the clients and sensors. When the registration for the client is successful they can obtain the information about the sensors in the network. If the sensor fails to respond in specific timeout it is assumed that the sensor failed or is no longer available. Also a client can unsubscribe to the cloud when he is no longer interested. The messages between sensor and client can be classified as data and control messages. Data messages are mostly sensor related data (status) and messages from the cloud. Control messages are sent by the clients to control the sensors in the network.

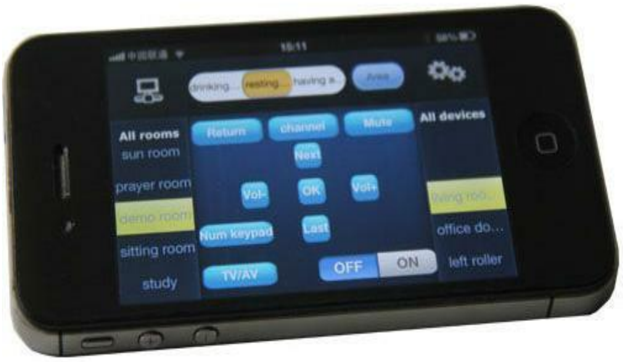

Fig 4: Home automation through smart phone

Fig. 4 shows a smart phone controlling the rooms in a home. Thus the benefits of IoT and cloud can be used to automate things and manage waste, traffic, power etc. Recently iPhone introduced its ability to support parenting through an application called "Parenthood" through IoT.

4. CONCLUSIONS

In the paper the benefits, challenges and different types of IoT are discussed. Also the importance of IoT in daily lives is highlighted. Next we discussed the concept of integration of cloud with IoT. The architecture of cloud in IoT and the importance of data storage with the help of cloud are discussed. Also the concept of introducing a gateway master in the cloud architecture is explained. Also the concept of secure cloud is introduced. In the next section we discussed about sensor and client APIs for providing communication between sensors and clients and thus provide automation. In the future the concept of IoT and cloud can be further extended to new applications. Also the cloud advancements can be included wherever necessary providing a great scope for new innovative ideas. However the future work can be concentrated on providing security and privacy at both sensor and router sides. Also for IoE, IPv6 should be implemented. IoE opens a door for advancements in different technologies like nano electronics, system integration, sensor networks, embedded systems, cloud computing, testing software tools etc.

5. ACKNOWLEDGMENT

We would like to thank the members of family, friends who assisted us.

6. REFERENCES

[1] Weiser, M., The Computer for the 21st-Century, Scientific American, 265, 94–104, 1995.

[2] York, J., and Pendharkar, P.C., "Human–computer interaction issues for mobile computing in a variable work context," International Journal of Human-Computer Studies,Vol. 60, No. 5–6, 2004, pp. 771–797.

[3] Khattak, A.M., Pervez, Z., Jehad Sarkar, A.M., and Lee, Y., "Service Level Semantic Interoperability," 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, saint, pp. 387–390, 2010

[4] Proofpoint Research: Internet of Things (IoT) Cyber Attack Security [Online].Available: http://www.proofpoint.com/

[5] World Wide Web Consortium, "W3C Semantic Sensor Network Incubator Group," [Online]. Available: http://www.w3.org/2005/Incubator/ssn.

[6] "Protected Data Forwarding By Erasure Coding To Cloud Storage System," International Journal Of Innovative Technologies, VOL. 02, ISSUE 01, pp. 36-41, JAN 2014.

[7] "Decentralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[8] "Key-Private Proxy Re-Encoding," Proc. Topics in Cryptology (CT-RSA), pp. 279-294, 2009.