ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Study of Architecture and Security Issues of IOT

L.V.Satyanarayana
Assistant Professor,
Aditya Institute of Technology and Management, Tekkali.

V.Ashok Gajapathi Raju
Assistant Professor
Aditya Institute of Technology and Management, Tekkali.

INTRODUCTION:

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home", offering more security and energyefficiency. Other personal IoT devices like wearable fitness and health monitoring devices and networkenabled medical devices are transforming the way healthcare services are delivered.

This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost.1 IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities", which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized

ARCHITECTURE OF INTERNET OF THINGS:

Implementation of IoT is based on an architecture consisting of several layers:from the field data acquisition layer at the bottom to the application layer at the top. The layered architecture is to be designed in a way that can meet the requirements of various industries, enterprises, socities, institutes, governments etc. Fig. 2 presents a generic layered architecture for IoT [2]. The layered architecture has two distinct divisions with an Internet layer in between to serve the purpose of a common media for communication. The two lower layers contribute to data capturing while the two layers at the top is responsible for data utilization in applications. The functionalities of the various layers are discussed briefly in the following:

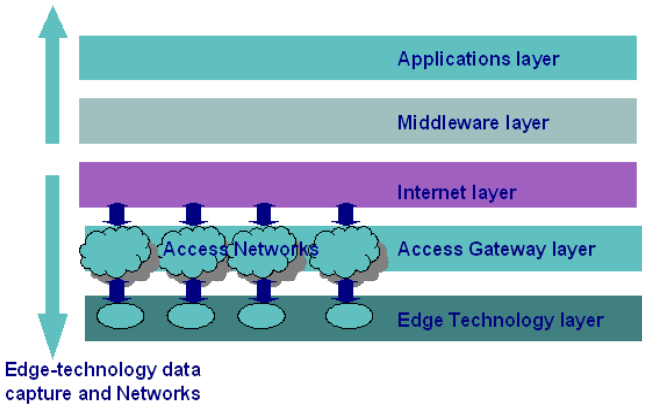

Fig: Layered architecture of Internet of Things

* Edge layer: this hardware layer consists of sensor networks, embedded systems, RFID tags and readers or other soft sensors in different forms. These entities are the primary data sensors deployed in the field. Many of these hardware elements provide identification and information storage (e.g. RFID tags), information collection (e.g. sensor networks), information processing (e.g. embedded edge processors), communication, control and actuation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

* Access gateway layer: the first stage of data handling happens at this layer. It takes care of message routing, publishing and subscribing and also performs cross platform communication, if required.
* Middleware layer: this is one of the most critical layers that operates in bidirectional mode. It acts as an interface between the hardware layer at the bottom and the application layer at the top. It is responsible for critical functions such as device management and information management and also takes care of issues like data filtering, data aggregation, semantic analysis, access control, information discovery such as EPC (Electronic Product Code) information service and ONS (Object Naming Service).
* Application layer: this layer at the top of the stack is responsible for delivery of various applications to different users in IoT. The applications can be from different industry verticals such as: manufacturing, logistics, retail, environment, public safety, healthcare, food and drug etc. With the increasing maturity of RFID technology, numerous applications are evolving which will be under the umbrella of IoT.

IOT PLATFORMS:

At this stage we divide our IoT development into two parallel technologies: Wearable and Embedded. Developers can build apps for custom wearable devices like Peeble, Samsung Gear or can opt to create their own platform using Embedded solution and then can develop app for that platform.

1. Wearable Platform:

Tizen is fast becoming one of the most popular platform for Mobile and wearable devices. Tizen SDK comes ported with wearable emulator which makes it easier to develop wearable solutions for Tizen platform. . Smart watches are getting popular by every day. Android Wear apps can be developed and tested in Eclipse. This Android Developer Guide helps you in setting up Android Wear development environment in Eclipse. Salesforce is another platform which is coming up with awesome development environment, APIs in wearable technologies. Their solution is extended from Peeble to Google glass. Salesforce is really worth a try if you are planning to have a serious go at wearable technology as a career option. Checkout Salesforce Wear page.

2. Embedded Platforms:

Arduino is probably the best starting point for embedded based IoT. Basic Android boards don't come with Ethernet shield and for Arduino to be able to work as IoT device, you need to select Android with Ethernet shield. Android Yun on the other hand is a board that comes ported with ethernet shield. You can actually order a basic board of Arduino like Arduino Decimilia or Dueminolova and learn the hardware basics like connecting sensors, working with actuators, serial communication and then you can go for Ethernet shield and look for more web based application for Arduino.Raspberry Pi is probably one of the best things to happen in DIY IoT. A wide range of Data driven applications like Home Automation Server toHome Multimedia server, File Server can be developed withPi. PI like Arduino has general purpose IO pins. But seamless working with sensors is bit tedious in Pi.Another efficient IoT board is Intel Edision which has integrated BLE, WiFi among host of other features. It supports wide range of Industry standard hardware (over 30) through 70-pin interface. What is important is it supports wide range of platforms including Arduino and Node.jsIntel Galileo is another good offering by Intel which supports the same shielding that of Arduino Uno. So it can be said to be first Intel powered divice which is Arduino compatible. It has among other thing a USB host controller like Raspberry Pi which makes this an attractive hardware. Galelio also has ethernet shield in built.There was a time when Microsoft used to dictate echnologies and trends. Industries used to follow. That is no more the story. With several companies gunning for a space in wearable sector, microsoft seems to be doing all the catching up and does not look too impressive at this moment. None the less Netduino is a .Net Micro Framework based plstform where hardware is simillar to Arduino. But Netduino has 12 bit ADC as against 10 bit Arduino ADC channels and uses 32 bit Controller. There are few more differences. But the reason why Arduino is a better bet for me than Netduino is that I get an Arduino Dueminolova for under $10 where as Netduino is about $60. Though Netduino really has better multitasking, cost is a big factor for DIY guy.

3. Cloud Platform for IoT:

Let's rediscuss the possibilities to beverage vending maching once more in terms of sheer possibilities. In the conventional vending machine you need to press a button or put a coin to trigger the process of liquid flow, which

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

stops after certain quantity.Now how about integrating paypal or Google money with the vending machine? How about a customer discovering the vending machine as "website" along with it's location and then pays online for a glass ofbeverage. Once payment is successfull he gets an access token. He can pass the token to the machine through NFC and bingo he gets his drink. Now this logical possibility is very important for understanding IoT and IoT really can bring several services (like online payment gateway), several hardware platform (like embedded board of the vending machine) and smart objects and data like NFC, GPS into a seamless environment.Now if you can integrate online payment into beverage vending machine, why not in for a community washing machine? If you are using location service for beverage machine, then whey not utilize the location and payment service for the toll gate? Why not get the data of a medical diagnesis like ECG (acquired through another embedded board partaining to medical electronics) into cloud such that several doctors can view it and form a comprehenssive opinion about the patient's state?

Well, infact all of them are possible. A little understanding of web and software design would take your mind towards cloud. Just like Web of Machines, in a Machine to Macine (M2M) or Machine to Objects (M2O) or any simimlar communication several modules will be common and several modules demands data to be available for sharing. Cloud APIs comes in handy in this regrad.For instance when you have to make a device discoverable in web, you have to assign a fixed IP address, maintain a router and follow several networking skills. You might not have the knowledge and infrastructure needed for maintaining a commercial sophisticated network for IoT. Yaler is a great example of what services and cloud can bring to table. This provides connection as a service such that your device is easily discoverable and communicable over the web without much hassle and take care of underneath security.

Axeda Provides infrastructure for M2M architecture. OpenIoT is an open source IoT platform that provides out of other services a unique Sensing as a Service. Google has already integrated location services with it's cloud. Location extracted from your devices are silently put in your status updates in facebook and twitter and are also used for more personalized searches. So cloud APIs has a great potential in IoT in all levels of architecture starting from firmware to hardware to more top level architecture.

SECURITY ISSUES

The IoT Security Challenge

As we note in the principles that guide our work, ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting trust and use of the Internet.56 As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don't believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector.As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction.

Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the Internet of Things as they are for the computers that have traditionally been the endpoints of Internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts.Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally, not just locally. For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyperconnected world. In fact, it is increasingly difficult to purchase some devices that are not Internet-connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber attack, but we can't so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behavior. This is why security of IoT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact.

References:

[1] K. Ashton, That ―Internet of Things‖ Thing, RFiD Journal. (2009).
[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things - CERP IoT, 2010.
[3] J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.
[4] M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Systems Journal. (1999).
[5] Y. Rogers, Moving on from weiser's vision of calm computing: Engaging ubicomp experiences, UbiComp 2006: Ubiquitous Computing. (2006).
[6] R. Caceres, A. Friday, Ubicomp Systems at 20: Progress, Opportunities, and Challenges, IEEE Pervasive Computing 11 (2012) 14–21.