Volume 8, No. 5, May-June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Survey on Applications, Privacy and Security Issues in Internet of Things

Chethan. C.
Asst. Professor, Dept of ISE
Sri Venkateshwara College of Engineering
Bengaluru, India

Tejaswini N. P.
Asst. Professor, Dept of ISE
Sri Venkateshwara College of Engineering
Bengaluru, India

Guruprasad Y. K.
Asst. Professor, Dept of ISE
Sri Venkateshwara College of Engineering
Bengaluru, India

Abstract: Growing interactions and technological advancements among various electronic devices has led to the concept of Internet of things (IoT). Any thoughtful impact to the advancement of the Internet of Things must necessarily be the result of sensors and internet as a whole. This paper introduces the concept of Internet of Things, its basic architecture and applications in various fields. Concerns are also raised over the misuse and misinterpretation of personal information pertaining to device and individual privacy. This survey tries to summarize the concerns of privacy and security threats of IoT.

Keywords: Internet of Things, architecture, sensors, security, privacy.

1. INTRODUCTION

With the advent of modern wireless telecommunications, especially with the explosive development in wireless networks over the last few years the one technology that is gaining popular ground in the recent times is The Internet of Things (IoT). IoT deals with the basic idea of having the ubiquitous occurrence of variety of things or objects – such as Radio-Frequency IDentification (RFID), tags, sensors, actuators, mobile phones, etc are able to interact with each other and cooperate with their neighbors to reach common goals[1]. The most obvious benefits of the IoT will be visible in both working and domestic fields. Smart cities, Smart homes also known as domotics, assisted living, e-health, enhanced learning are only a few examples of possible applicationIoT can bring with it along with assistances in business/process management, logistics, automation and industrial manufacturing and intelligent transportation of people and goods. The National Intelligence Council (NIC) foresees that ‘‘by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more”[2].But with great opportunities comes, great challenges. IoT poses several security and privacy concerns at different layers viz; Frontend, Backend and Network.

2. OVERVIEW

‘Internet of Things” semantically means ‘‘a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols” [3]. The IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service.The fig.1 signifies the evolution of internet. In the late 1960s, communication between two computers was made possible through a computer network. In the early 1980s, the TCP/IP stack was introduced. Then came the internet with its commercial use in the late 1980s. The more popular World Wide Web (WWW) became available in 1991 and stimulated the rapid growth. The mobile phones got popular among the people with their portability and efficient communications and soon got connected to the Internet and formed the mobile-Internet. The start of the century brought in social networking where users started to become connected together over the Internet.

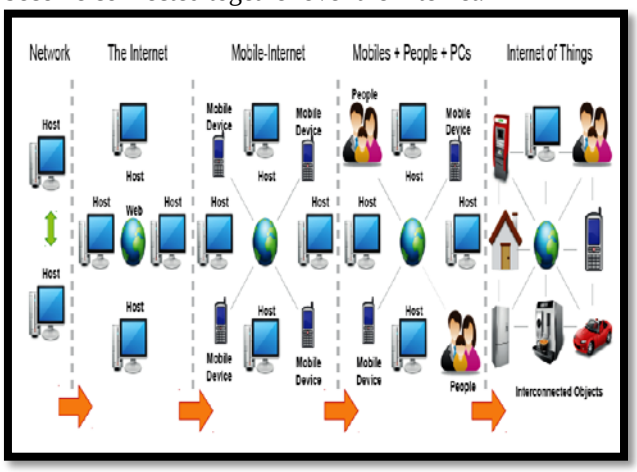

Fig 1: Evolution of Internet

3. ARCHITECTURE

The architecture of IoT can be broadly classified into 3 layers based on the usage. Because IoT employs internet and physical devices, the connection between the internet and devices forms an important layer. So the three layers: recognition, Network and Application as shown in Fig.2 are interdependent and inter important.

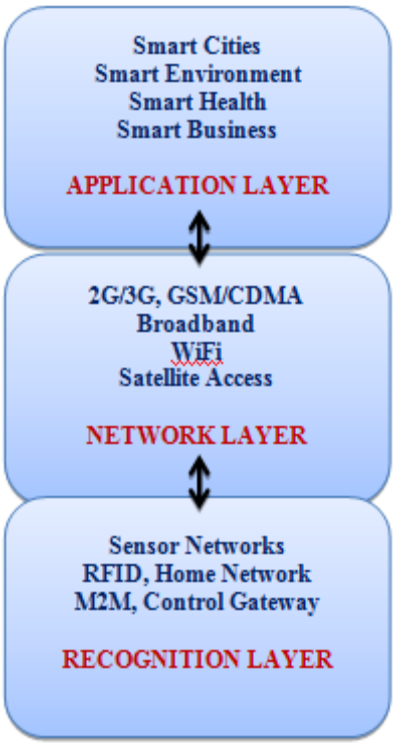

Fig.2: IoT Architecture

Recognition layer, also known as the Perception layer garners the relevant data/information using various sensors and RFIDs and identifies the physical world. The middle one, Network layer is responsible for the initial processing of data, broadcasting of data, assortment and polymerization. This is done using various mobile and land based communication connections like the 2G/3G, GSM, Broadband, Wifi services.This layer is also known as the "Central Nervous System" that takes care of global services in the IoTs, since it acts the part of aggregating with upward application layer and makes the link downward of perceptual layer. The topmost application layer puts in all the services that an IoT application can offer [4].

4. APPLICATIONS OF IoT:

An early study in IoT identified the many of the potential areas of applications[5].
It can be classified into various domains like Smart Homes, Smart Cities, Retail, Transportation, Lifestyle, Agriculture, Healthcare, Smart Factories, Supply chain, Emergency, User interaction, Culture and tourism, Environment and Energy.
But the most lucrative and interesting areas of IoT application should have to be in the domain of smart cities, smart homes, transportation and Healthcare.

A. IoT in Healthcare:

Due to population growth, population aging, shortage in medical staffs and institutional facilities especially in rural areas healthcare system needs to have a major upliftment in India. IoT can bring in the solution in doing so. Smart wearable devices like Fit bits, Pill cameras and RFIDs can help to bring in more and more patients under the supervision of doctors even if the patient is in remote location and can keep a track of their medical history with the help of cloud technologies.

Whenever there is an abnormal value, users and their close relatives are notified to take early treatment. This enables the early detection and prevention. Through real-time monitoring, when user is in emergency agencies or relevant authorities, which improve medical emergency treatment and response capacity. Furthermore, it is also efficient to establish national health management records, to provide prevention and decision-making basis for lifestyle diseases, epidemic and regional disease through monitoring, comparing analyzing and processing healthcare information of associated group. In this way, capabilities of disease prevention, early detection and early treatment are improved enormously.

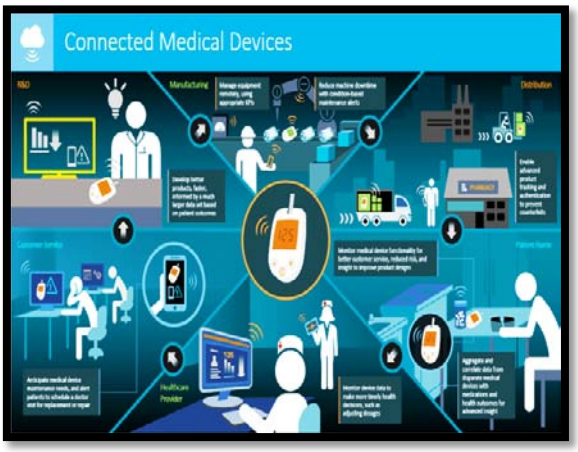

Fig.3: IoT in Healthcare

B. IoT in designing smart homes:

Fig 4: Iot in designing smart homes

Smart homes filled with connected products are loaded with possibilities to make our lives easier, more convenient, and more comfortable. Reading of remote meters can be attained through these smart home systems. The data related with home power, telecommunications, gas and water can be sent automatically to their corresponding utility company to enhance the efficiency of the work. If people are driving home on a hot summer day, nothing makes them happier than just using their smartphone to tell their smart thermostat to lower the temperature. BI Intelligence, Business Insider's premium research service, expects the number of smart home devices shipped will grow from 83

million in 2015 to 193 million in 2020. This includes all smart appliances (washers, dryers, refrigerators, etc.), smart home safety and security systems (sensors, monitors, cameras, and alarm systems), and smart home energy equipment, like smart thermostats and smart lighting.

C. IoT in Agriculture:

Offering high-precision crop control, useful data collection and automated farming techniques, smart farming technique is quickly catching on in the agricultural business. A recent Beecham's report[6] predicts that food production must increase by 70 percent in the year 2050 in order to meet our estimated world population of 9.6 billion people. It also describes growing concerns about farming in the future: climate change, limited arable land, and costs/availability of fossil fuels. IoT brings in innovation in the landscape of current farming methods. IoT sensors capable of providing farmers with information about crop yields, rainfall, pest infestation, and soil nutrition are invaluable to production and offer precise data which can be used to improve farming techniques over time.

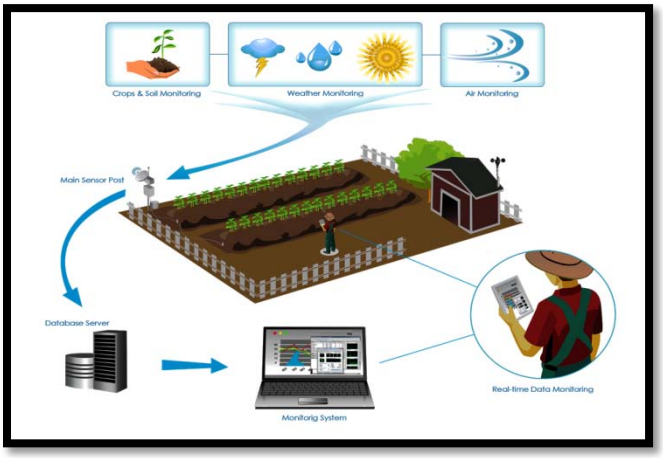

Fig 5: Iot in Agriculture

IoT in agriculture has the potential to conserve 50 billion gallons of fresh water in a year. The Agricultural IoT, integrated with Web Map Service (WMS) and Sensor Observation Service (SOS) provides a solution to managing water requirements or supply for crop irrigation. It also smartly analyzes crop water requirements and uses water supply resources available to reduce waste. In areas of drought, the crop water management function of Agricultural IoT can be of great value, as it intelligently manages the limited water supply by calculating the valve operation timing and building optimum irrigation strategy, resulting in better practices to preserve water resources.
Weather forecasting accuracy and other dynamic data inputs can affect crop productivity to a great extent. It ensures accurate and efficient communication to farmers of real time data related to dynamic agricultural processes (like weather forecasts, planting, harvesting, etc.), weather forecasts, soil quality, and availability and cost of labor. Farmers who have access to such important real-time information available to them can better plan their course of activities beforehand and take corrective or preventive measures in advance for the future. Agricultural IoT has a system to monitor and scan the environmental parameters and plant growth. There is also data available from pest control sensors which are capable of predicting pest behavior. This information can be used by farmers to reduce damage done by pests on a large scale. It also aims to ensure food safety at different levels, like storage, transportation, etc. To do so, it has a monitoring system over various factors like shipping time, storage temperature, and cloud-based record keeping. Supporting livestock health fortified with monitoring tools like as ear tags for cattle, capable of detecting respiratory diseases. If a disease is detected, it sends an alert so the animal can be separated from the herd, preventing the disease from spreading.

5. SECURITY AND PRIVACY CONCERNS

Each device which is connected increases privacy and security concerns surrounding the IoT. These concerns range from hackers stealing our data and even threatening our lives to how corporations can easily uncover private data. The fundamental security weakness of the Internet of Things is that it increases the number of devices behind your network's firewall. Ten years ago, most of us had to only worry about protecting our computers.Five years ago, we had to worry about protecting our smartphones as well. Now we have to worry about protecting our car, our home appliances, our wearables, and many other IoT devices.

A. Sensors & Devices

Front-end sensors and equipment receives data via the built-in sensors. Machine or perception nodes are mostly distributed in the absence of monitoring scenarios. An intruder can easily access these devices which imply damage or illegal actions on these nodes can be done. Possible threats are analyzed and are categorized to unauthorized access to data, threats to the Internet and denial of service attack.

B. Internet Services

Internet services plays an important role in the interconnection of the devices that make up the core of the IoT. Effective interconnection provides comprehensive interconnectivity, effectualness and thriftiness of connection, as well as authentic quality of service in IoTs. Since a large number of machines sending data to network congestion, large number of nodes and groups exist in lOTs may be resulted in denial of service attacks.

6. PRIVACY CONCERNS IN IOT

The Internet security glossary [7] defines privacy as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others".

A. Too Much Data

The sheer amount of data that IoT devices can generate is staggering. A Federal Trade Commission report entitled "Internet of Things: Privacy & Security in a Connected World" found that fewer than 10,000 households can generate 150 million data points every day. This creates more entry points for hackers and leaves sensitive information vulnerable.

B. Unwanted Public Profile

You've undoubtedly agreed to terms of service at some point, but have you ever actually read through an entire document? The aforementioned FTC report found that companies could use collected data that consumers willingly offer to make employment decisions. For example, an insurance company might gather information from you about your driving habits through a connected car when calculating your insurance rate. The same could occur for health or life insurance thanks to fitness trackers.

C. Eavesdropping

Manufacturers or hackers could actually use a connected device to virtually invade a person's home. German researchers accomplished this by intercepting unencrypted data from a smart meter device to determine what television show someone was watching at that moment.

D. Consumer Confidence

Each of these problems could put a dent in consumers' desire to purchase connected products, which would prevent the IoT from fulfilling its true potential.

7. CONCLUSION

The IoT technology draws huge changes in everyone's everyday life. IoT is an emerging technology that has attracted a considerable number of researchers from all around the world. There have been major contributions making this technology adapted into our daily life. However, there are lots of key issues addressing security concerns of IoT and they need more research effort to be solved.

In this survey, we presented Internet of Things with architecture and design goals. We surveyed security and privacy in IoTs. In addition, we identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. We also discussed applications of IoTs in real life. In the coming days, research on the IoTs will remain a hot issue. Lot of tricky problems arewaiting for the reserachers to deal with.

REFERENCES

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.

[2] National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, <http://www.dni.gov/ nic/NIC_home.html>.

[3] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro &Nanosystems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.

[4] G. Gang, L. Zeyong, and J. Jun, "Internet of Things Security Analysis," 2011 International Conference on Internet Technology and Applications (iTAP), 2011, pp. 1-4.

[5] O. Vermesan, P. Friess,and A. Furness, The Internet of Things 2012, By New Horizons, 2012. [Online]. Available: http://www.internet-of-things-research.eu/pdf/ IERC_Cluster_ Book_2012_WEB.pdf

[6] Towards Smart Farming: Agriculture Embracing the IoT Vision.

[7] RFC 2828, "Internet Security Glossary," May 2000, [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt.