© 2018 IJSRST | Volume 4 | Issue6 |Print ISSN: 2395-6011 | Online ISSN: 2395-602X
National Conference on Smart Computation and Technology in Conjunction with The Smart City Convergence 2018

A Review on Security and Privacy in Application of IOT in Smart City

Megha Soni*, Krishna Kumar, Apurv Sharma
Department of Computer Engineering, Poornima Institute of Engineering & Technology, Jaipur, India

ABSTRACT

From Stone Age to Bronze Age to 21[1st] century, mankind has made a remarkable development. Whether it is a field of science & technology or literature they have achieved excellence. Today we are living in a "computer dependent" world and are on our way to enter a new era of technology known as "Internet of Things" commonly known as IoT. IoT is a system of interconnected devices over network embedded with electronic device and, sensors which enables the exchange of data between the devices. Use of wireless sensors has led to the gather of large amount of data in Smart City infrastructure and IoT may come handy in managing these data easily. Till now we have mostly seen human to human type of communication or human-machine type of communication but IoT provides machine to machine type of communication.

Keywords: Internet of Things, Smart City, Security & Privacy.

I. INTRODUCTION

The Internet of Things (IoT) is a coming-of-age technology which will bind together everyday's physical objects embedded with microcontroller, transmitter, receiver, sensor, and protocols which will enable them to share data and communicate with each other over internet. Thus it will provide us an easy access and interaction with devices such as home appliances, surveillance cameras, sensors, vehicles etc which stores enormous amount of data. In this way enormous amount of data will be on our fingertips.

There has been an increasing trend of people moving toward urban areas in recent years because of employment opportunities, lifestyle and more. Thus challenging the existing system to manage the services for the increasing population and in this way forming what is so called "Smart City". There is no formal or widely accepted definition of smart city.

Wikipedia defines smart city as-
"A smart city is an urban development vision to integrate multiple information and communication technology (ICT) and Internet of things (IoT) solutions in a secure fashion to manage a city's assets – the city's assets include, but are not limited to, local departments' information systems, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services.".[4]

Smart city is, basically a concept in which cities makes the use of technologies connected over intelligent network to address challenges. These challenges may be related to parking, street light, transportation,

traffic, safety, waste management, service quality, security, water management, education system, healthcare system and more.

Thus the smart city concept aims to make the efficient use of public resources, improving and increasing the quality of services provided to the citizen and on the same time reducing the operational cost of these services.

Since Internet of Things connects devices, infrastructure, vehicles, appliances and more. Thus make it possible to make cities so called "smart" and more efficient by improving infrastructure, generating more cost effective municipal services, enhancing public transport by providing ways to reduce traffic and keeping citizens more engaged and productive.

The combination of technology with that of the physical world and communication between them can simplify the lives of citizens. Since according to a report from Cisco System, 60% of the world population will reside in cities by the year 2050, so transforming city into smart city should be our first preference. [5]

According to Forbes top 10 smart cities in the world are – New York, London, Paris, San Francisco, Boston, Amsterdam, Chicago, Seoul, Geneva and Sydney.
Some of the companies which provide smart cities solution worldwide are IBM, Cisco, Intel, and Silver Spring Network etc.

There are various terms related to the Internet of Things:[6]

Internet Protocol Version 6(IPv6) -
As IPv6's huge increase in address space, it is an important factor in the development of the Internet if Things. According to Steve Leibson(occasional docent at the Computer History Museum), the expansion of address space means that "after assigning an IPV6 address to every atom on earth, still we will have enough addresses left to do same for another 100+ earths." In simple words, we can easily assign IP address for every "thing" on the planet. An increase in the number of smart nodes, as well as the amount of upstream data the nodes generate, is expected to raise new concerns about data privacy and data security.

6LoWPAN -
6LoWPAN is a acronym that combines of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (Low PAN). This concept allows for the smallest devices with limited processing ability to transmit information with a battery life that lasts for years.

General Packet Radio Service (GPRS) -
A wireless communications process 2G, 3G and 4G cellular networks which supports a number of bandwidths and provides data rates of 56-114 kbps. As cellular companies need more advanced and effective network, GPRS network may be more cost-effective for IoT networks on basis of privacy and security purpose

Machine to Machine (M2M)-
It is a vast term that describes technology that permit one connected device to communicate for exchanging information with another connected device, without any human efforts.

II. APPLICATION

A.Traffic light Control

Traffic light control systems are used to monitor and control the flow of automobiles running on roads. They aim to make smooth motion of vehicles in the transportation routes. However, multiple traffic light systems' synchronization at adjacent intersections creates a complicated problem. However a system based on PIC microcontroller that evaluates the traffic density using IR sensors and accomplishes dynamic timing slots with different levels can be helpful. Moreover, a portable controller device is designed to solve the problem of emergency vehicles stuck in the overcrowded roads.

B. Smart Education

Albert Einstein said," Education is not the learning of facts, but the training of mind to think". So by making the education system smart, we can actually make the thinking process smart.

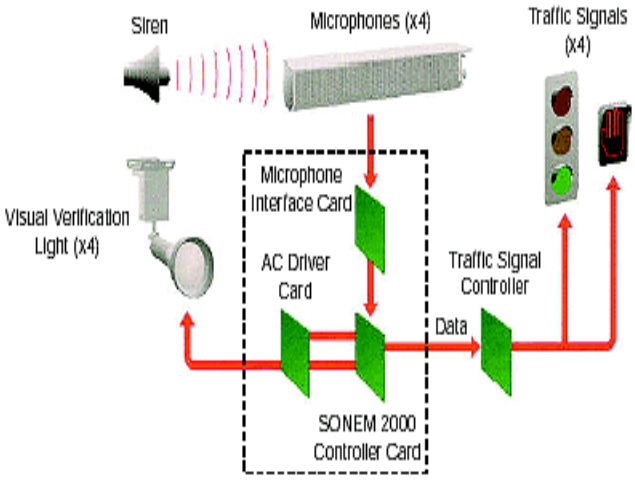

Figure 1. Traffic Light Control

Progress and enhancement of life and modern society demands the changes in today's educational infrastructure, which are traditionally very slow because of the existing education system.

Technology benefitted us in every way possible right form communication to education. Improving the quality and the enhancement of teaching and learning through the use and implementation of new trends of technology and IT enabled education is the primary target of higher education system.

Smart education, a concept that describes learning in digital age, has gained increased attention.

C. Intelligence Building

Building and home automation systems have usually been implemented only in high-level offices and buildings. The modern home entertainment systems could easily be combined with other sensors and actors within a building, thus forming a fully interconnected and smart environment. . Web- based smart energy metering and localization and mapping of energy consumption will be one of the IoT applications.

Figure 2. Intelligence Building

D. Waste Management

Municipal solid waste management (MSWM) is one of the major environmental problems in Indian. Improper management of municipal solid waste (MSW) causes hazards to inhabitants. Many studies have found that about 90% of MSW is not treated scientifically and then is dumped in open dumps and landfills, creating hazardous effects to public health and the environment. Various adopted treatment technologies for MSW are critically reviewed, along with their advantages and limitations. Recycling is a resource recovery practice that refers to the collection and reuse of waste materials such as empty beverage containers. Recycling is the process of making new objects from the material the item, which is being recycled, is made of. Kerbside collection process can be adopted to collect the material for recycling from general waste using dustbins and collection vehicles.

III. WORKING OF IoT [3]

The concept of Internet of Things lends to fabulous ideas. This concept provides internet based communication between physical objects, sensor and controllers. The connecting gadgets of the IoT such as computing hardware, including processors (with embedded programming telling what to do), sensors to gather various information (such as temperature, chemical levels, moisture, light, motion, heart rate and body movement) and communication hardware that can exchange signals.

Working of IoT mainly revolves around these components – sensors and devices, connectivity, data processing and user interface.

A. Sensors and devices

Devices with the help of sensors and other tech collect data from their environment. A device can be consists of one or more sensors to gather information. For example Phone is a device which is consists of many sensors like camera, GPS etc.

B. Connectivity

The data collected is then sent to cloud. A cloud is a data storage model in which data is maintained, managed and made available to the user. The sensors and devices can be connected to the cloud with the help of wifi, Bluetooth, satellite, internet.

C. Data processing

Now software performs some kind of operation on the data as per the requirement of the user, once data is uploaded on the cloud. It then resends the processed data to the devices or sensors at the user's end.

D. User interface

Here the processed data is made useful in some way to the user and may be communicated to the user through email, text, notification, alert etc. User can also proactively check the system for the result. User can also perform some action and affect the system. For example opening and closing the door, checking the temperature etc through an app or web browser.

User can also provide some predefined rule to automatically perform these actions.

IV. PRIVACY AND SECURITY [2]

a. Data Confidentiality

Confidentiality is somewhat equivalent to privacy. Confidentiality is done in order to prevent important and sensitive information from reaching the wrong

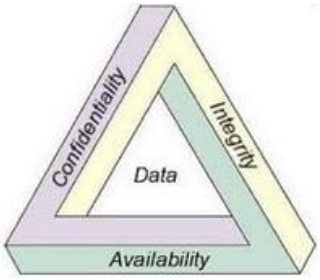

Figure 3. The CIA triad

people. On the same time making it sure that the right person gets the information thus restricting the access to the authorized person only. It is a process of providing confidence among the users about the privacy of their data. There are many methods to provide data confidentiality. Data encryption converts data into cipher text which makes it difficult to access for unauthorized persons. Two-step verification authenticates by testing two dependent component and allows the access only if both the components pass the authentication test. Biometric verification uniquely identifies each person.

b. Data Integrity

Data during its transition period may be changed by some unauthorized person, and the process is commonly referred as cybercrime, or it may get affected by some other factors such as crash of server or electromagnetic disturbance. Thus data integrity refers to the process of maintaining the accuracy of data and protecting it from being modified by some unauthorized person. Common method to provide data integrity is cryptography where hashing of received data is compared with the hashing of original data. Other methods includes user access control and file permission.

c. Data Availability

One of the main goal of IoT security is to make data available to the authorized persons whenever and wherever they need it. Any information has values if it can be accessed by authorized person at right time. To ensure availability there should be countermeasures for DoS attack which denies data availability to the users. Backup is the key to data availability.

A. Security And Privacy Concer And Their Measures [2]

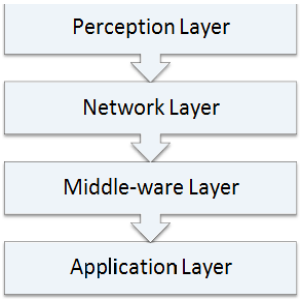

Figure 4. Generic architecture of IoT

Perception Layer

It consists of different types of sensors and other communication tools in order to communicate data between machines by uniquely identifying each object. Due to the lack of proper authentication mechanism in sensors data can be accessed by some unauthorized person and can be modified. Data cloning can also be easily done by any cybercriminal. System becomes vulnerable to spoofing in which attacker gain full control over system through broadcasting false information and making it appear as if it is coming from original source.

Security for this layer may include measures such as- authentication which means providing access only to the authorized person. Data privacy can be achieved through encryption, two step verification or biometric verification. Discovering new threats in advance can help in preventing security breaches. This process is called risk assessment.

Network Layer

This layer transmits the gathered information obtained from the previous layer to an information processing system over a connected network.

Challenges network layer faces are

Sybil attack: the attacker manipulates a node in a network such that that node acquires multiple identities.

Sinkhole attack: compromised node in a network attracts network traffic through its fake routing update. It can be used to launch DoS attack.

Sleep deprivation attack: maximizes the power consumption which eventually cause the node to shut down.

DoS: Network is flooded with useless of information and noises due to which network become unavailable to users.

Malicious code injection: attackers inject malicious code into the node which may cause complete shutdown of the network. Attacker may also get full control over network.

Measures that can be taken are-

Authentication: with a proper authentication process and proper encryption, unauthorized access to the sensor nodes can be prevented which in turn can prevent misuse of data.

Routing Security: routing algorithms can be implemented to ensure the privacy of data that is being exchanged between different devices connected over network.

Data privacy: encryption process, two step verification authentication, or biometric verification can be used to ensure data privacy.

C. Middle-ware Layer

This layer performs automated actions based on the results of the data processed and links the system with the database.

Challenges this layer faces are-

Unauthorized access: Middle-ware Layer provides different interfaces for the applications and data storage facilities. The attacker can easily damage the system by preventing the access to the related services of IoT or by deleting the existing data.

DoS Attack: This is similar to what we have discussed in the previous section.

Malicious Insider: This kind of attack occurs when someone from the inside tampers the data for personal benefits or the benefits of any 3rd party. The data can be easily extracted and then altered on purpose from the inside.

Measures that can be taken are-

Authentication: with a proper authentication process and proper encryption, unauthorized access to the sensor nodes can be prevented which in turn can prevent misuse of data.

Risk assessment: Discovering new threats in advance can help in preventing security breaches. This process is called risk assessment.

Data privacy: encryption process, two step verification authentication, or biometric verification can be used to ensure data privacy.

Intrusion Detection: it provides security solutions by generating alarm on generation of any suspicious

activity by continuously monitoring and keeping logs of intruder's activity which could help to trace the intruder.

D. Application Layer

This layer provides various application of IoT based on the needs of users. Some of the application includes smart city, smart home, smart hospitals, smart education etc.

Challenges this layer faces are-

Spear phishing attack: It is a type of email spoofing attack towards a specific individual, organization or business. The victim is attracted to open email through which the attacker may get control over the system and can also install malware on the targeted system.

DoS Attack: This is similar to what we have discussed in the previous section.

Malicious code injection: Some kind of malicious code is injected into the system in order to steal some kind of data from the user.

Sniffing attack: The attacker can introduce a sniffer application which can corrupt the entire system.

Measures that can be taken are-

Authentication: with a proper authentication process and proper encryption, unauthorized access to the sensor nodes can be prevented which in turn can prevent misuse of data.

Risk assessment: Discovering new threats in advance can help in preventing security breaches. This process is called risk assessment.

Data privacy: encryption process, two step verification authentication, or biometric verification can be used to ensure data privacy.

Intrusion Detection: it provides security solutions by generating alarm on generation of any suspicious activity by continuously monitoring and keeping logs of intruder's activity which could help to trace the intruder.

V. CONCLUSION

This review paer is significant in outlining general information about urban IoT, such as definition and status of IoT, which has become IT topic nowadays, and research institutes participating in related projects build a smart city as part of the future vision of local governments by reflecting the new information paradigm of IoT. A proof-of-concept implementation, deployed in the city of Padova, Italy, is a relevant example of application of the IoT paradigm to smart cities.

VI. REFERENCES

[1] J. Sathish Kumar and Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014

[2] M.U. Farooq, Muhammad Waseem, Anjum Khairi and Sadia Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015

[3] Calum McClelland, "How does an IoT system actually work?" [online]. Available: https://iot-for-all.com/how-does-an-iot-system-actually-work-7c27f366018f

[4] Wikipedia, [online]. Available: https://en.wikipedia.org/wiki/Smart_city

[5] Dr.P.B.Pathak, "Internet of Things: Understanding the Security Concerns", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5, Issue 3, March 2016

[6] Vandana Sharma and Ravi Tiwari, " A review paper on "IOT" & It‟s Smart Applications", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 2, February 2016