INTERNET OF THINGS: A RISING CONCERN OF SECURITY AND PRIVACY

Mohit Kumar

Abstract: In today's time IoT implies great significance in almost everybody's life. The common lifestyle has been largely affected by IoT devices. People are massively depended on these devices, whether it is for entertainment, study, research or communication purpose. Besides the facilities provided by these devices and applications, there is also a major concern and that is security and privacy of users. Rapidly usage of these devices without taking care of its bad affects may harm the users in many ways. In this paper the various concerns and threats which can affect the privacy, security and integrity of users are being discussed.

Index Terms**- Internet of Things, IoT, Security, Threats, Privacy.**

I. INTRODUCTION

IoT is a network of interconnected devices that collects and exchange information among each other with a aim to facilitate the user. These devices can be any electronic things we use like – TVs, air conditioners, cars, mobiles, health devices etc. The IoT market is set to rise from its valuation of $157B in 2016 to estimated $457B by 2020, accomplishing the CAGR of 28.5% [1]. And according to IOT analytics, Smart Cities (23%), Connected Industry (17%) and Connected Buildings (12%) are the top three IoT projects in progress [2]. With this data we can imagine that our future is going to depend on IoTs. This fast dependability on IoT raises some concerns about the data that is being collected by these devices. It is necessary to monitor and take care of every part of information that is accessed and transmitted among these devices. If this data captured by some unauthorized resources then it can be used for wrong purposes and this can lead to compromise of user's security and privacy. In Section II different applications of IoT are discussed, in Section III the various threats of IoT devices and its affects are discussed and Section IV concludes the paper.

II. APPLICATIONS OF IOT

As we know that the scope of IoT market is very large. But there are some key areas that are growing much faster than the others. Following are the some of the main applications of Internet of Things.

2.1 IoT in Smart Cities

IoT has good scope in smart cities as the technology has penetrated deep in lives of people. IoT is helping in solving major problems of cities like: traffic control, pollution, energy distribution, parking management etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied [3]. Smart traffics lights can also manage traffic with the help of real time traffic surveillance and can set the timing of lights accordingly. And with the help of sensors street lights can be turned on or off which helps in saving energy. As well as citizens can also get to know about traffic prone areas and free parking space available while sitting at their place.

2.2 IoT in Smart Cities

IoT automation solutions for industries from all big names like NEC, Siemens, Emerson and Honeywell are already in the market [4]. The IoT has a significant role in making the industry more fast and autonomous**.** Automation tools like PLC (Programmable Logic Control) and PAC (Programmable Automation Control) are used with smart sensor networks connected to a central cloud system which collect huge amount of data. Specially designed software and applications are used to analyse the data and its behaviour for improvements [5]. And this data needs to be handled with great care to prevent it from intruders.

2.3 IoT in Home Automation

There are number of home automation devices which help to make a smart home. Everything from light switches to air conditioner are connected together, which ease the user to control the lighting and temperature from anywhere in the world. There exist many prominent companies like Amazon Echo, Google Home, and Philips smart lights etc. which are doing significant research in home automation. So, every moment lots of data is being produced through these devices and any hacker can use data to monitor the day to day activities of users or can also damage physical or intellectual property.

2.4 IoT in Healthcare

IoT is undoubtedly transforming the healthcare industry by redefining the space of devices and people interaction in delivering healthcare solutions. IoT has applications in healthcare that benefit patients, families, physicians, hospitals and insurance companies [6]. With the help of Personal Medical Devices (PMD) that are very small electronic devices, patient's condition can be monitored by his doctor from anywhere. It helps the doctor make decision about patient's future treatment according to data collected by the PMD. IoT allow patients to receive care away from their hospital at home, elsewhere around the world. With wearable sensors and service solutions, doctors can reduce readmissions and enable proactive care [7].

III. SECURITY AND PRIVACY THREATS

3.1 Threats in IoT Smart Cities

IoT has big contribution in smart cities. These devices hold and transmit large amount of information and if the security of this flow of information is neglected then it can prove to be a serious threat for residents. No doubt smart cities provide the residents many facilities but the care should be taken over the use of IoT devices. Smart city intelligent applications rely on data harvested by ubiquitous sensors. These data is transmitted to the cloud by the integration layer that manages the heterogeneity of sensor devices and networks [8]. There are number of attacks and methods through which the privacy and security of users can be compromised. Let us discuss some of the major attacks:-

3.1.1 Botnets*:*

Botnets can be used to steal information and help the attacker to take over the control to multiple devices that are connected. In 2016 the Mirai attack turned millions of computers into remotely controlled botnets that can be used to access the sensitive information and manipulate the behavior of systems.

3.1.2 Spoofing:

Spoofing is when an attacker sends the messages to some computer by falsifying its own identity as the trusted partner of the receiver. Thus it can ask for any sensitive information from the receiver. This attack can be used to manipulate the flow of data and control signals.

3.1.3 Denial-of-service attacks:

By using the DoS attack any intruder can make the systems unavailable to its originals users. Denial-of-service attacks would disrupt the smart city such that the management, control and operation are either in a biased and incorrect way, or disabled [9].

3.1.4 Attacks on smart grids:

Smart grids play core part in a smart city regarding energy deployment and management. These are actually communicating instruments including sensors and communication networks that help in communicating data in real time [10].When the data is shared in real time scenario among power generator, distributed resources, the service provider and the users, any information that is prone to attacks that would take the system to failure. This will unfortunately lead to user's uncertainty and discontentment with the system [11].

3.2 Threats in IoT Industries

IoT in industries used in many ways such as RFIDs, GPS, WSNs and various mobile devices. The attacks on industrial IoT include:-

3.2.1 RFID Vulnerabilities

Radio Frequency Identification (RFID) used for the identification and tracking of products, packets, and pallets in supply chain scenarios, to smart devices, such as smart phones and wearable's (e.g., smart watches) with considerable computing capabilities and Internet connections [12]. It is possible because of the wireless characteristics of RFID system that helps the attacker to take out confidential information such as password or any other data which in turn makes the system vulnerable [13].

3.2.2 Stuxnet Worm

Stuxnet Worm was discovered in June 2010. It was designed to attack SCADA (industrial control) system. It targets industrial computer systems were responsible for causing substantial damage to Iran's nuclear program. It caused a major damage to Iran's nuclear program [14].

3.2.3 Sybil Attack:

Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy [15].

3.2.4 Ukraine power grid cyber-attack:

On 23 December, 2015 an Ukrainian electricity distribution company Kyivoblenergo, reported an attack on their systems. With this attack seven 110 kV and 23 35 kV substations were disconnected for three hours. It resulted in disruption of services to its customers.

3.3 Threats in IoT Home Automation

In a Smart home there is a network of smart switches, sensors and other devices. There are lots of opportunities for hackers and attackers to spy on anybody and take control of these devices. Attackers can also use home Wi-Fi network to take control on LED lights and other equipment. Some researchers show that attackers can infer whether the home is occupied with more than 90 per cent accuracy just by analyzing smoke and carbon dioxide sensors data. The power consumption recorded by the smart plug could also be used to analyze your operations on the computers [16]. Examples include attacks on home automation systems and taking control of heating systems, air conditioning, lighting and physical security systems. The information collected from sensors embedded in heating or lighting systems could inform the intruder when somebody is at home or out [17]. A smart fridge, which will have access to the personal information and, possibly, the payment details of the user. If it's authorizing payments on the user's behalf, hackers can exploit this device and steal the user's credit card information [18].

3.4 Threats on IoT Healthcare

Many healthcare devices require lot of interaction from user and saves lots of data every moment about the user. This data includes the activities, heart rate, calories intake, blood pressure in particular environment etc. This type of data can reveals serious personal information which can be life threatening. There are many types of attacks on medical devices that include eavesdropping in which privacy of the patient is leaked, integrity error in which the message is being altered, and availability issues which include battery draining attacks [19]. Most of the PMDs operate using battery power. If there is not any proper authorisation mechanism any intruder can drain the battery of PMD using Sleep Deprivation Attack or manipulate the working of the device.

IV. CONCLUSION

As we understood that IoT have made our life very easy, but there is much research work that needed to be carried out. Without required measurements of security and privacy these facilities may turned into bad dream. No one want the devices which compromise their privacy and let anybody spy on them. There are many other attacks and security flaws apart that of above discussed. Although much work had been carried out but major part of the problem is still unsolved. It should also be considered that users of these devices must know the possible consequences and effects on their security and privacy and they should be guided that how to use and how not to use the IoT devices. So the work needs to done on both sides e.g. on the side of developer as well as the end user.

REFERENCES

[1] Market pulse report, Internet of Things", by Growth Enabler. https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

[2] IoT Analytics, The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects. https://iot-analytics.com/top-10-iot-segments-2018 real-iot-projects/

[3] Analyticsvidhya, "10 Real World Applications of Internet of Things (IoT) – Explained in Videos ". https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

[4] internetofthingswiki.com," IoT Applications with examples". https://internetofthingswiki.com/iot-applications-examples/541/

[5] rfpage.com, "Applications of Industrial Internet of Things (IIoT)". https://www.rfpage.com/applications-of-industrial-internet-of-things/

[6] Wipro "What can IoT do for Healthcare", https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/

[7] Microsoft , "IoT for Healthcare"

[8] Talal Ashraf Butt and Muhammad Afzaal , "Security and Privacy in Smart Cities: Issues and Current Solutions".

[9] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen "Security and Privacy in Smart City Applications: Challenges and Solutions".

[10] C. Clastres, "Smart grids: Another step towards competition, energy security and climate change objectives," Energy Policy, vol. 39, no. 9, pp. 5399–5408, 2011

[11] Sidra Ijaz, Munam Ali Shah, Abid Khan and Mansoor Ahmed, "Smart Cities: A Survey on Security Concerns". IJACSA, Vol. 7, No. 2, 2016

[12] Ahmad-Reza Sadeghi, Christian Wachsmann, Michael Waidner," Security and Privacy Challenges in Industrial Internet of Things".

[13] Jaychand , Nishant Behar, "A Survey on IoT Security Threats and Solutions". International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017.

[14] Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security & Privacy 9.3(2011):49-51.

[15] John R. Douceur,"The Sybil Attack," in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260.

[16] Wei Zhou, Yuqing Zhang, and Peng Liu," The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved".

[17] Mohamed Abomhara and Geir M. Køien," Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks". Journal of Cyber Security, Vol. 4, 65–88.

[18] Diksha Sopori, Tanaya Pawar, Manjiri Patil, Roopkala Ravindran," Internet of Things: Security Threats". IJARCET Volume 6, Issue 3, March 2017, ISSN: 2278 – 1323.

[19] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah," Security Issues in the Internet of Things (IoT): A Comprehensive Study". IJACSA, Vol. 8, No. 6, 2017.