IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 12-17
www.iosrjournals.org

A Review: the Risks And weakness Security on the IoT

Mohammed Tawfik [1,]Ali M. Almadni[2],Alhasan A. Alharbi[3]
[1, 2, 3](Department of Computer Science, MGM Dr. G.Y.Pathrikar College of Computer Science & Information Technology, Aurangabad Maharashtra India

Abstract:*Internet of things is the technique which is provided by the unique identifiers that can automatically transfer the data over the wide network without the help of human being. The devices uses are vulnerable to hack. The purpose of hacking the devices of Internet of things may not be accessing data only, but it could be harming the users of those devices. In other words, it might affect them economically, endanger their health or put their lives at risk since this technology is directly connected to their daily lives, and this is considered a violation of users' privacy. The devices of Internet of Things are hacked and exploited in order to attack the internet infrastructure supplied by some major companies.*
In this paper we have token an overview about the security of internet of things, the detailed architecture is also represented, Risks and attacks are also discussed here.
Keywords: *Architecture, Attack, Risk, identities, DDOS.*

I. Introduction

The Internet of things is a technique which is provided by the unique identifiers that can automatically transfer the data over the wide network without the help of human being. Why is the Internet of Things one of the biggest threats to internet infrastructure?

It is hazardous because of the large number of IoT devices that are connected to the Internet, which is currently at No. 20 billion devices. In 2020 the number will exceed 50 billion devices according to some previous studies. It is possible to control the devices of the internet of things and/or use it as widely for electronic attack due to weakness of security. Internet is a network of the interlinked computer networking worldwide, which is accessible to the general public. The internet has changed the face of the lives of people, turning them completely into the modern and latest lifestyle with its developments. Today, instead of the newspapers, the people use the internet to access the e-news which provides with not only the newspapers completely but also various different news channels from all over the world. Even the live video news from the news channels can be accessed through the net, overpowering the other media, even including the television. The internet came into exist in MIT on September 2, 1969 when the first piece of networking equipment (a packet switch) first communicated with an operational piece of the outside world[1][2]. The other key step was to make the computers talk to each other exploring this idea in 1965 while working with Thomas Merrill, Roberts connected the TX-2 computer in Massachusetts to the Q-32 in California. Through a low-speed dial-up telephone line [3], creating the first-ever (though small) wide-area computer network. On the basis of Licklider packet switching theory, Robert develops a network and made a plan for the ARPANET, publishing it in 1967 [4]. The first public demonstration of the ARPANET took place In October 1972. In the same year electronic mail, the initial "hot" application was introduced. In March, Ray Tomlinson of BBN wrote the basic email message send-and-read software, motivated by ARPANET developers' need for an easy coordination mechanism. From there, email took off. As the most popular network application and as a forerunner of the kind of people-to-people communication activity we see on the World-Wide Web today.

The paper organizes as nine section after the introduction the section II give the literature survey of IoT, in section III cover the Internet of things Architecture, in the section IV IoT , in the section V cloud computing and internet of things, in the sections VI and VII attacks and risks in IoT Respectively , the section VIII and IX give the types and possible solution to reduce risk respectively finally the conclusion given in section X.

II. Literature Review

In the perspective of supply chain management Kevin Ashton firstly invented the internet of things in 1999[6]. According to Atzori internet of things can be understood by three models -internet-oriented, things-oriented and semantic oriented [5]. Mark Weiser forefather of the ubiquitous computing define that Internet of things is nothing but a smart environment in which the physical world that is richly & invisibly connected with sensor, actuators, displays and computational elements, embedded seamlessly in the every objects of our lives and connected through a continuous network[6]. Also by studied the progress, opportunities and challenges of

ubiquitous computing Caceres and Friday got the idea of cloud computing and internet of things [7]. [8] define internet of things in terms of smart environment in which we uses the information and communication to provide services for administration, education, healthcare, public safety, real estate, transportation and utilities. Although the definition of Things has changed as technology evolved, the main goal of making computer sense information without the aid of human intervention remains the same. A radical evolution of the current Internet into a Network of interconnected objects that not only harvests information from the environment (sensing) and interacts with the physical world (actuation/command/control), but also uses existing Internet standards to provide services for information transfer, analytics, applications, and communications. Fuelled by the prevalence of devices enabled by open wireless technology such as Bluetooth, radio frequency identification (RFID), Wi-Fi, and telephonic data services as well as embedded sensor and actuator nodes, IoT has stepped out of its infancy and is on the verge of transforming the current static Internet into a fully integrated Future Internet . The Internet revolution led to the interconnection between people at an unprecedented scale and pace. The next revolution will be the interconnection between objects to create a smart environment. Only in 2011, the number of interconnected devices on the planet overtook the actual number of people. Currently there are 9 billion interconnected devices and it is expected to reach 24 billion devices by 2020[9]. A schematic of the interconnection of objects is depicted in Figure 1, where the application domains are chosen based on the scale of the impact of the data generated.

Figure 1: Application of Internet of Things Smart Home [9].

III. Internet of things Architecture

There are three basic components of the Internet of things:

A. Things : objects (Devices) that are connected wirelessly to the wide network.

B. Network : Router, network or gateway that connects multiple things to the cloud.

C. Cloud : Remote servers in a data center that store data safely and securely [10] .

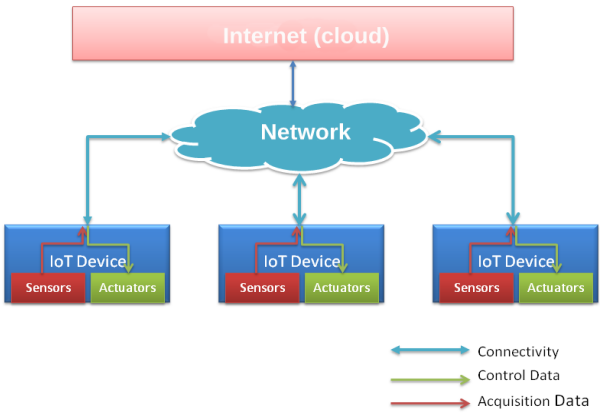

Figure 2: IoT Architecture

The IOT devices generate data that differs from one device to another by sensitive devices which determine the temperature, humidity, positioning (GPS) [12]. The sensors study of the nature of the environment of the these devices where data is transferred from the device to the network and then to the cloud that takes some time until they are analyses and returned back to the devices [13].

IV. Internet of Things (IoT) Protocols and Technologies

Communication technologies such as Wi-Fi, Bluetooth, ZigBee and, 3G, 4G cellular,NFC,Neul, RFID

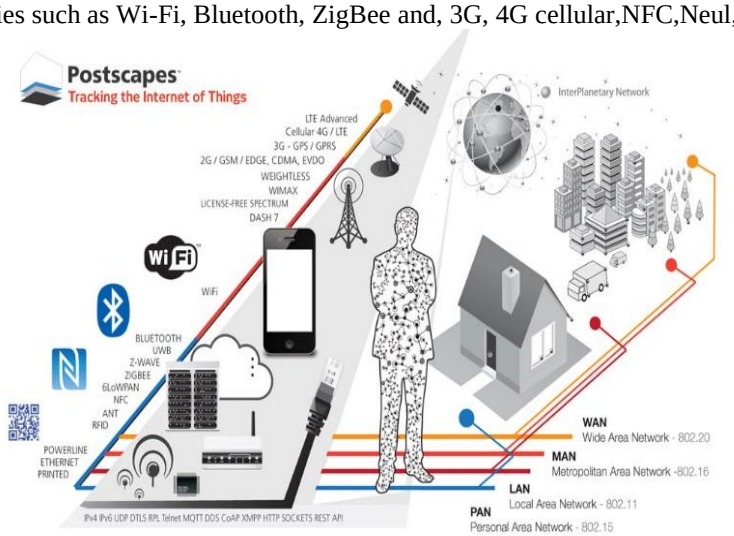

Figure 3**:** protocol and technique of IOT

- **RFID** is the key technology for making the objects uniquely identifiable.It's reduced size and cost makes it inferable into any object [14].
- **NFS**: stands for Near Field Communication. The specification details of NFC can be found in ISO [15]. The main characteristic of NFC is that it is a wireless communication interface with a working distance limited used in payment transactions transfer data
- **Bluetooth:** IOT may use Bluetooth for communicate in short distance Telecom is Radio which technology within shortwave designed to transmit data over short distances from one meter to meter percent and consumption of small amounts of energy.
- **ZigBee:** New web protocol is based on the IEEE 802.15.4 standard and this protocol is used automatic homes, which has enabled the construction of a network of wireless sensors and the change to automate laboratories are wireless. Today it is used in smart home automation Featuring consumes little power, where the battery is sufficient for two years and also characterized by a low rate of transfer of data from 50 kilobits / sec to 250 kilobits
- **Z-Wave:** Z- Wave wireless communication technology is low power designed primarily for home automation products such as lamp control devices and sensors and Gerald data up to 100 kbit / sec transfer [16].

6LowPAN Standard: RFC6282,
is an IPv6-based design for home automation devices to communicate on a local wireless mesh network

- **WiFi**: Based on 802.11, Frequencies: 2.4GHz and 5GHz, used in homes and many businesses, mesh network most popular in many IoT applications
- **Cellular**: Standard GSM,GPRS,2G), UMTS/HSPA (3G), LTE (4G) Frequencies: 900/1800/1900/2100MHz ,it used for any application required for long distance 3G refers to the third generation of developments in wireless technology, telecommunications and private phones. The third generation, as the name suggests, follows the first generation (1G) and second-generation between two device.
- **Neul** : Specially designed for the Internet of things M2M apply coverage, battery life, and cost goals of unity and efficiency solutions GPRS, 3G, CDMA and LTE WAN access them away today is to give long battery life.
- **LoRaWAN**: Technology standards for the exchange of data between the base and thousands of machines around the station. These technologies allow developers to build low-power, wide area networks [17]. This table show the protocols of IoT technique :

Techniques Name	Frequency	Range	Examples	Date Rate
RFID	120–150 kHz	10cm to 200m	Road tolls, Building Access,	4 or 8 kbps
NFS (near field communication)	13.56 MHz	0.2 m	Smart Wallets/Cards, Action Tags	100–420kbps NFC is not suitable for many

Techniques Name	Frequency	Range	Examples	Date Rate
				types of data transfer
Bluetooth	2.4GHz	1-100m	Hands-free headsets, key dongles, devices IOT	1Mbps
Wi-Fi	2.4 GHz, 3.6 GHz and 4.9/5.0 GHz bands	-	-	600 Mbps maximum, ,150-200M as standard, latest 1Gbps
Cellular	900/1800/1900/2100MHz	35km, GSM; 200km for HSPA	Cell phones, M2M, smart meter	35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)
ZigBee	2.4GHz	10-100m	Smoke detectors and fire equipment	250kbps
6LowPAN	2.4GHz	N/A	----------	N/A
Neul	900MHz (ISM), 458MHz	10km	cloud	100kbps
LoRaWAN	Various	2-5km-15km	-	0.3-50 kbps

Table 1: protocol and technique of internet of things

V. Cloud computing and internet of things

Cloud computing is considered the third party for the Internet of things , the Internet of Things devices connected to the central server [18] . The idea of the Internet of Things depends on linking those devices target to the Internet via the cloud. The data of such devices is stored in the cloud and is digitally controlled such as smart cars and other smart electrical appliances [19]. Cloud computing is the basis of the infrastructure of Internet of things. The data is collected from the peripheral devices and sent to cloud computing then it is analyzed and it returns as requested information for peripheral devices to perform a certain task [20].

VI. Attacks

Attacks DDOS

The most true Assumptions of how the attack took place is The 10/21/2016 attacks were perpetrated by directing huge amounts of bogus traffic at targeted servers namely those belonging to Dyn , a company that is a major provider of DNS services to other companies and contain about 170000 company registered domain in this company this attack called " DDOS " [21]. Distributed Denial of Service (DDOS) attacks, the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled, a DOS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business , disrupting normal operations. Criminal perpetrators of DOS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks. The DDOS attack was using the infections devices possible by the use of default passwords on these devices. Because the default passwords have not yet changed, and they are known for hacker.

Figure 4: Dyn attack

The basic types of DDOS attack are:

A. The network-centric attack the attacker which using devices to overloads a service by using up bandwidth and an application-layer attack which overloads a service or database The inundation of packets to the target causes a denial of service .

B. The hacker have many hacked hundred or thousand or may be more than millions devices that group of computers is known as a "botnet" and " zombie " and make them working as soldiers for king , Under control to direct them to make big attack by one command the attack on the big servers or large institutions for denial of services to users like that happened in 21/10/2016 oct for DYN [22] .

VII. Risks in internet of things:

Any device connected to the Internet like a smart CAR, a camera surveillance and a smart lamp lighting has a title (IP) [23], which has its own system that performs a specific task . It is apt to hacking more than computers because their security system is extremely weak .The most significant problems are summarized as follows [24]:

i. Privacy problems that might put the user data at risk, however this data is considered too sensitive.

ii. Material damage that could be caused by tampering with instruments which can lead to harming the user, such as home appliances.

iii. Misusing this technology for purposes like monitoring users and violating their privacy.

iv. IV Possibility of exploiting location data of those devices for example determining the car site .

v. Exploiting those internet devices for hacking electronic governments and major companies that are associated with the Internet [25].

i. Types of security vulnerabilities of internet of things

ii. Vulnerabilities in communication interfaces between the user and internet of things is insecure, where the user can bypass , access and control the device .

iii. Weakness in the authentication process [26]

iv. There are not enough methods to identify the authorized users, and this allows unauthorized people to log in to those devices.

v. Insecure software occurs when programmers focus only on the speed of transfer data neglecting the security aspect.

vi. Using insecure protocols for data transfer.

vii. Easiness of scanning and knowing the devices connected to the internet[27].

I. Possible solutions to reduce risk

II. Default passwords and ideally default usernames to be changed during initial setup

III. Ensuring user accounts cannot be enumerated using functionality such as password reset mechanisms

IV. Ensuring account lockout after 3- 5 failed login attempts

V. Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF

VI. Ensuring credentials are not exposed over the internet

VII. Implement two factor authentication if possible.

VIII. Implemented Secure Sockets Layer (SSL and Transport Layer Security (TLS)

IX. automatic Update IoT devices with security patches when packages update become available

X. disable Universal Plug and Play(upnp) protocol for prohibit from discover hacker to know devices in your network

XI. most devices exploit by Mira virus must be updated firmware

XII. Conclusion

The Goal Of This Paper Shows What Has Happened And Maybe Happen In The Future As Well As The Work Of The Crisis Precautions To Reduce Risk . This Paper Refers To The Fact Of The Security Architecture Should Be Fit With The Lifecycle Of A Devices As Well As Its Capabilities And Includes Aspects Such As The Way A Security Domain Is Reated , The Need For The New Types Of Protocols For The In Conclusion, We Would Like To Suggest That More Effort On Development Of Secured Measures For The Existing Internet Of Things (IOT) Infrastructure Before Going For Further Development Of New Implementation Methods Of IOT In Daily Life Would Prove To Be A More Fruitful And Systematic Method.

References

[1]. Licklider, J.C.R., and Clark, W. On-Line Man-Computer Communication. Aug. 1962.

[2]. Leonard Kleinrock; “Breaking loos”, communication of the ACM, Vol.44-No.09, Sept-2001.

[3]. Roberts, L., and Merrill, T. Toward a Cooperative Network of Time-Shared Computers. In Proceedings of the Fall AFIPS Conference Oct. 1966.
[4]. Roberts, L. Multiple Computer Networks and Intercomputer Communication. In Proceedings of the ACM Gatlinburg Conference
[5]. Oct. 1967.
[6]. L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Computer Networks 54, 2787–2805, 2010.
[7]. M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Systems Journal,1999.
[8]. R. Caceres, A. Friday, Ubicomp Systems at 20: Progress, Opportunities, and Challenges, IEEE Pervasive Computing 11 (2012)14–21.
[9]. J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.
[10]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswamia "Internet of Things(IOT), A vision, Architectural elements, and feature directions" Department of Electrical and Electronic Engineering, The University of Melbourne, Vic - 3010, Australia.
[11]. www.infoq.com https://www.infoq.com/articles/internet-of-things-reference-architecture , A Reference Architecture for the Internet of Things , 25/12/2016
[12]. Cloud Standards Customer Council 2015, Cloud Customer Architecture for Big Data and Analytics, Version 1.1
[13]. uk.rs-online.com , http://uk.rs-online.com/web/generalDisplay.html?id=i/iot-internet-of-things
[14]. Jan Henrik Ziegeldorf1∗, Oscar Garcia Morchon2, and Klaus Wehrle1 Sundmaeker H, Guillemin P, Friess P, WoelffleS. Vision and challenges for realizing the Internet ofThings. Cluster of European Research Projects on theInternet of Things, European Commission 2010
[15]. Gokhan Tanyeri , Paul Beckett; Glenn Matthews ,' Short range wireless technologies BLE, Bluetooth and Wi-Fi are an essential part of any IoT effort' , ebadded world 2015
[16]. Karen Rose, Scott Eldridge, Lyman Chapin , Devices iot , October 2015
[17]. www.rs-online.com/designspark/ , https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about
[18]. www.postscapes.com , http://www.postscapes.com/internet-of-things-protocols/
[19]. Internet of Things (IoT) Dr. John Barrett explains the Internet of Things in his TED talk ,puplisher Margaret Rouse
[20]. Shagufta Rajguru1,Swati Kinhekar2,Sandhya Pati3 , Analysis of Internet of Things in a Smart Environment , International Journal of Enhanced Research in Management & Computer Applications , ISSN: 2319-7471 , Vol. 4Issue 4, April-2015, pp: (40-43).
[21]. DYN company , dyn.com , http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[22]. www.welivesecurity.com , http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/
[23]. Tobias Heer, Oscar Garcia-Morchony, Ren e Hummen,and other , Security Challengesin the IP-based Internet of Things , COMSYS Group, RWTH Aachen University, GermanyandyPhilips Research, the Netherlands
[24]. Tuhin Borgohain, Uday Kumar, Sugata Sanyal ,SurveyofSecurityandPrivacyIssusof Internet of Things
[25]. Chen Qiang1,*,Guang-Quan2, Bai Yu3andLiu Yang2,Researchon Security Issues of the Internet of Things , International Journal of Future Generation Communication and Networking , Vol.6, No.6(2013), pp.1-10
[26]. M.U. Farooq, Muhammad Waseem, Sadia Mazhar, A Review on Internet of Things (IoT), International Journal of Computer Applications (0975 8887)Volume 113 - No. 1, March 2015
[27]. SECURITY IN THE INTERNET OF THINGS Lessons from the Past for the Connected Future , iver Systems, Inc . Rev. 01/2015