Internet of Things (IoT)

Sachee Nene[1] Rushika Ghadge[2]
[1,2]Department of Computer Engineering
[1,2]VESIT, India

Abstract— The Internet of Things is a trending and evolving topic of technical, social, and economic significance. This concept has made progress in almost every field of human life. Right from durable goods, consumer products, vehicles, industries, sensors, and other objects are being combined with the Internet to connect the human life with technology There are number of applications of IoT that has made human life more simpler and only a few of these applications are discussed in this paper. This paper along with the applications will explore the vulnerabilities and threats in IoT environment and how the protection methods can be implemented to make IoT a promising technology that can be beneficial to the world.

Key words: Internet of Things, IoT

I. Introduction

Internet of Things (IoT) is a platform for connecting multiple objects via internet. The 'thing' in IoT could be any person with a heart monitor or a vehicle with built-in-sensors, i.e. each connected object is assigned an IP address and thus it can transfer and collect data without any physical or manual connections or human interventions over the internet. The objects have a technology embedded which helps them interact with the inside and outside environment, thus affecting the decisions taken or made.

Internet of Things helps connect devices in various systems through internet. Digitally connected objects can be controlled from anywhere. This connectivity then helps us collect more data from multiple places thus increasing the efficiency and improving security.

IoT is gradually becoming a driving force in companies which helps them improve performance via IoT analytics and security to yield better results. With the corporate world IoT also plays a major role in fields like oil & gas, insurance, manufacturing, transportation, infrastructure and retail sectors. Thus making these sectors reap the benefits of IoT by making more informed decisions and leading to increase in their revenues.

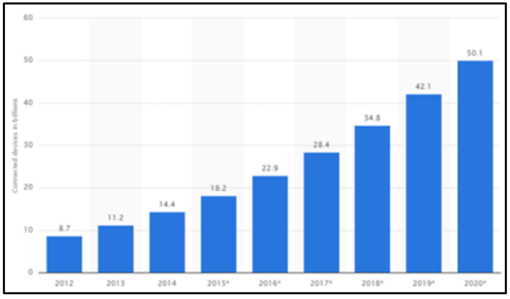

Fig. 1: No of connected devices worldwide from 2012 to 2020 (in billions) through IoT

Factors like process efficiency, asset utilization and productivity which are obtained from IoT platform helps organizations reduce their costs. Along with this, the improvements in tracking of devices using sensors has helped organizations make smarter decisions. The growth and convergence of data, processes and things on the internet helps create more opportunities for people, businesses and industries.

The figure below shows the survey and estimation of billions of connected devices via.

II. Working principle of IoT environment

IoT uses machine to machine communication (M2M), and acts on information which is received from another machine. Humans can interact with gadgets, access the data or give them instructions. These devices do most of the work on their own without human intervention.

The following are the building blocks of IoT:

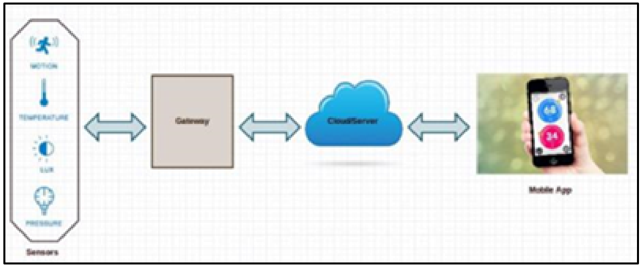

Fig. 2: Working of IoT

A. Sensors & Sensor Technology

They will collect a wide variety of information which includes Location, Weather/Environment conditions, Grid parameters, Jet engine maintenance data to Health essentials of a patient, etc.

B. IoT Gateways

IoT Gateways are the gateways that helps to interact with other network objects Gateways connects the internal sensor nodes network with the outside Internet. This is done by collecting the data from the nodes and transferring it to the Internet.

C. Cloud/Server Infrastructure & Big Data

The data transmitted through gateway is stored and processed securely within the cloud infrastructure using Big Data analytics engine. This processed data is then used to perform intelligent actions thus making devices 'Smart'.

D. End-user mobile apps

The user friendly mobile apps helps the end users to control & monitor their devices from anywhere and anytime. These apps are used to send commands to the IoT devices.

E. IPv6

IP addresses are the backbone to the entire IoT. All the devices/things are connected to the internet using an IP address.

III. Applications of IoT

A. Net Smart Thermostat

One of the most popular application of IoT is the Nest, a smart thermostat that's connected to the internet. It adopts family’s routine, adjusts the temperature based on how hot or cold the climate is, whether you are home or outside, awake or asleep and helps on saving on heating and cooling bills. /The mobile app allows one to configure the settings and even receive alerts when something goes wrong with the system.

B. *WeMo Switch Smart Plug*

It is one of the most useful devices for home purposes which is nothing but a smart plug. It plugs into any outlet, accepts the power cord from any device, and can be scheduled to turn the device on and off via a smartphone. Another model of smart plug, the Insight switch which monitors energy consumption of devices and makes one’s home more energy-efficient.

C. *Automatic Car Tracking Adapter*

The Automatic app tracks information about a car by using an in-car adapter. It keeps track of things like mileage, hours driven, fuel cost, fuel efficiency, location, and ignition status. It can be connected with other apps making it more useful. Dash is an alternative to this that gives similar information, and calculates an overall “Dash score” to help improve driving. Many vehicles are now getting IoT capabilities so they can be monitored and made more efficient.

D. *DHL's IoT Tracking & Monitoring*

The Internet of Things can also bring a positive change in logistics. For example, DHL provides shipping, warehousing, distribution, and supply chain management all over the world which requires a huge amount of communication. DHL used IoT technology which includes vehicle monitoring and maintenance, real-time tracking of packages, environmental sensors in shipping containers, information-gathering on employees and tools, and a number of safety-enhancing features for vehicles and people.

IV. SECURITY ASPECTS OF IOT

A. *Threats and the vulnerabilities*

Devices which are connected results in the generation of massive amount of Internet traffic which includes loads of data that can be used to make the devices useful. But this data can also be used for other purposes. All this new data, and the Internet-accessible nature of the devices, raises both privacy and security concerns.

– Some of the threats to IoT in [3] are,

1) *Ransomware*

It’s another type of malware that locks down access to files by encrypting them and later sells the decryption key that will give back the access to the files. IoT ransomware is more dangerous. Andrew Tierney and Ken Munro of PenTest Partners demonstrated about the smart thermostat ransomware at DEF CON. This particular IoT thermostat runs a modified version of Linux, has a large LCD screen which showed the ransom demand – and has an SD card.

2) *IoT Botnets*

An IoT botnet is a group of virus infected and hacked computers, Internet-connected devices that are used for malicious purposes. These devices are very cheap, easy to infect and are mostly used for DDoS attacks. One of the example of botnet attack, is a researcher at Proof point in December 2013, noticed that hundreds of thousands of malicious emails logged through a security gateway had originated from a botnet that included not only computers, but also other devices -- including smart TVs, a refrigerator and other household appliances.

3) *Distributed Denial of Service (DDoS)*

DoS attack happens when a service that would usually work is unavailable. In a Distributed Denial of Service attack, a large number of hacked systems attack one target system. This is done using a botnet, where many devices are programmed to request a service at the same time. DDoS attacks doesn’t try to steal information or results in data loss, but affects the company in terms of cost and time. An example of DDoS attack is on Dyn, a company that is a major provider of DNS services where huge amounts of traffic was directed on its servers. This attack is famous as 10/21 IoT DDoS attack.

4) *Insecure Web Interface*

Attackers exploit this vulnerability by using weak credentials or by capturing plain text credentials to access the web. This results in data loss, DoS etc. One of the example is about an insecure web interface which was exploited by hackers to compromise Asus routers in 2014 that were shipped with default admin username and password.

5) *Eavesdropping*

It is the unauthorized access of a private communication such as a phone call, instant message, video conference or fax transmission. Eavesdropping is easier to perform with IP-based calls than TDM-based calls. A protocol analyzer can pick and record the calls without being noticed by the callers. There are software packages for PCs that will convert digitized voice from standard CODECs into WAV files.

6) *Social Engineering*

It is the act of manipulating people so they give up confidential information. The individuals are targeted by the attackers who usually try to get information about one’s credential details or bank information or even try to get access to a computer to install install malicious software that will then give them access to personal information with control over the computer, All this is usually done in the form of phishing emails, which makes one disclose their information, or redirects to websites like banking or shopping sites that look legitimate, letting you to enter your details.

B. *Recent attacks due to IoT devices*

The DDoS attacks against dynamic domain name service provider Dyn on October 21st 2016 have caused unavailability of services across the Internet. According to Dale Drew, the attack resulted from a "botnet" of Internet-of-Things (IoT) devices The attack began creating problems for Internet users reaching multiple sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix. The botnet which was made up of devices like home Wi-Fi routers, IP video cameras was sending huge numbers of requests to Dyn's DNS service. Those requests looked legitimate, so it was difficult for Dyn's systems to identify them from normal domain name lookup requests. The attack involved Mirai, the malware which used IoT devices protected by default usernames and passwords, and then enlists the devices in attacks that created traffic at Dyn’s servers until it could not accommodate legitimate visitors or users.

Few more attacks happened like in December 2015, a malware which infected Ukraine’s power grid which brought down the power supply of hundreds of thousands of residents. In this attack, attackers used spear-phishing and social engineering to gain entry to power grid's network. The attackers found that the operational systems which controlled the power grid were connected to regular IT systems. The Black Energy malware which attacker used acted as a network sniffer which discovered sensitive data such as user credentials that allowed the attackers, access the industrial control system and endangering the electricity supply.

In general, in most of the attacks, the attackers used small, embedded, low-powered sensors which were connected to industrial networks along with social engineering or phishing etc.

V. SECURING IOT DEVICES

Embedded device security will never be easy. But, increasing the importance of security in the initial stages and using analytics to monitor the device and protect the network to which the devices are connected, will prevent attackers from exploiting the system.

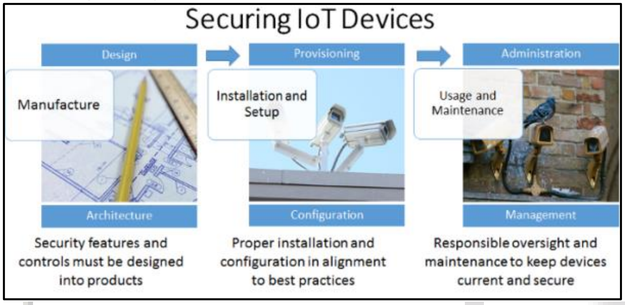
Securing IoT Devices
Design
Provisioning
Administration
Manufacture
Installation and Setup
Usage and Maintenance
Architecture
Configuration
Management
Security features and controls must be designed into products
Proper installation and configuration in alignment to best practices
Responsible oversight and maintenance to keep devices current and secure

Fig. 3: Securing IoT devices

These are the measures to protect the lifecycle of IoT devices in [9] are:

A. *Well Designed and Architecture Security*

Manufacturers of IoT devices must keep in mind to include security into the architecture, interfaces, and designs of their products. Separation of data and code, communication between trusted parties, data protection and authentication of users should be established and tested. The developed product must be updated on a regular basis in terms of security which includes build validation, software examining, and default configurations as per industrial guidelines. The hardware, firmware, operating systems, and software must be designed to go into a secured environment and survive.

B. *Security provisioning and configuration*

Most of the IoT devices need setup and provisioning upon installation. Authentication and identity of a device is very important. Rules must be placed to prevent use of default passwords upon installation, data to be encrypted, and only secure web connections must be allowed. Implementation of software security, such as anti-malware, intrusion prevention systems (IPS), and local firewalls will improve the device's security. Detection is necessary to know whether the systems are under attack. Policies must be established for privacy, data retention, remote access, key security.

C. *Administration and Management*

Managing devices is decided by the customers after the product is deployed. Manufacturers and online service providers play a role in provisioning but it is upto the owner to make decision about who will have access to system and who will be refrained from using the system. Owners have the authorization to turn on or off their products and choose which online services they can connect to. This requires proper end-user identification and authentication. IoT systems should be capable of authenticating its owner. A reset capability must be present in the event of an unrecoverable compromise or transfer of ownership. IoT devices should be simple to understand and easy to manage. Devices should be able to detect if something goes wrong and communicate such events to their owners, and provide ways to resolve the problems.

VI. CONCLUSION

The Internet of Things is a fascinating field, which connects everyday devices to the internet, bringing life more closely to the technology. With the technologies and applications mentioned earlier and ones still in the research phase, the world is reaching out to build more and more smart devices which leads to more efficient, intelligent machines. According to estimates, by means of this concept 50 billion devices will be connected by 2020 which places heavy demands and challenges in maintaining the required safety level of such an environment. This paper has analyzed various attacks caused due to IoT devices and the risks that might affect the security and the integrity of IoT devices, and also various security measures to be considered right from manufacturer of IoT devices to the end user.

ACKNOWLEDGMENT

We thank our mentor from Vivekanand Education Society's Institute Of Technology (VESIT), who provided insight and expertise that greatly assisted the research.

We would also like to show our gratitude to the Arthi C.I, V.E.S.I.T for sharing their pearls of wisdom with us during the course of this research.

REFERENCES

[1] (2016) Embitel website.[Online]. Available: https://www.embitel.com/blog/embedded-blog/how-iot-works-an-overview-of-the-technology-architecture-2/
[2] (2015) TechTarget website.[Online]. Available http://internetofthingsagenda.techtarget.com/definition/IoT-botnet-Internet-of-Things-botnet/
[3] (2016) CBR website.[Online]. Available http://www.cbronline.com/news/cybersecurity/breaches/top-five-biggest-threats-iot-security/#3/
[4] (2014) Gemalto website. [Online]. Available: https://safenet.gemalto.com/data-protection/securing-internet-of-things-iot/
[5] Cuno Pfister, "Getting Started with the Internet of Things", May 2011.
[6] (2016) Linkedin website.[Online]. Available:https://www.linkedin.com/pulse/how-secure-future-iot-matthew-rosenquist/
[7] Olivier Hersent, David Boswarthick, Omar Elloumi, "The Internet of Things: Key Applications and Protocols", 2015.