CYBER SECURITY IN THE ERA OF IoT

[1]**Devapriya E D**, [2]**Arjun M P**
[1]Assistant Professor, [2]MCA Scholar
[1]Department of Computer Science
[2]School of Information Science and Technology
[1]Jamia Hamdard Kannur Campus, Kannur, India
[2]Kannur University, Kannur, India

Abstract : The internet of things(IoT) is a term which means, the collection of global physical objects ,a network of physical devices, vehicles, home appliances and other items which are accessed through the internet that can identify themselves to other device in the IoT is embedded with electronics ,software, sensors, actuators and connectivity .through a 'smart mode' anything can be connected and communicate in an IoT. The quality of life and new business models are getting empowered using IoT.IoT is actually connecting all our daily activities embedded with electronics, software and sensors to the internet. More personal information and business data will exist in the cloud and be passed back and forth through thousands of devices in the IoT system. We share and exchange data privacy in the IoT like application devices or systems in the cyberspace or in an iot space a user should always be cautious to secure their data. Attackers mean the hackers create opportunities to trespass in the secure space of IoT. According to infographic from cisco, it goes on to say that 30 billion devices are expected to connected by 2017 and 50 billion are stated to connected by 2020.nowadays in the cyberspace including IoT, the malicious attackers like computer viruses, attacks from black hat hackers and network outrages are on a rise.so in the present era of computing where the internet explosion is a high fly, cyber security of IoT become a major concern with growing sophistication of cyber-attacks, it is the responsibility of cyber persons to secure them.in this quickly evolving world, a recent study states that 75 percent of IoT devices contain serious vulnerabilities.it is time to take precaution to secure the environment of IoT by strengthening sensor network security, enables strong authentication and streamlines the management of identities.

IndexTerms – Cybersecurity, RFID, Hackers, Botnet Attack

I. Introduction

Cybersecurity, computer security or IT security means securing computer systems from unauthorized access and malicious attacks from the hackers. By cybersecurity, we can control the physical access to the system as well as the attack from the network access. Security of a cyber-area may be violated whether intentional or accidental. So there are various methods to secure the procedures which may cause malicious to our IoT. Cyber Security is a vast developing area due to the increasing reliance of computer systems and internet, Wi-Fi, smart devices, smart cars, smartphones televisions refrigerators and tiny many other devices which are the part of the internet of things.

IoT is a huge network where all devices are connected to each other and sharing and interacting information with each other. All the devices in the IoT will communicate with each other without any human intervention. In a presentation to Proctor & Gamble in 1999, Kevin Ashton coined the term "The Internet of Things". He pioneered RFID (used In bar code detector) for the supply chain management domain and he is a co-founder of MIT's Auto-ID Lab. As per the Gartner report, all connected devices will reach to 20.6 billion by 2020and as per the Cisco report IoT will generate $14.4 trillion in value across all industries in the next decade. He also started Zensi, a company that makes energy sensing and monitoring technology. The 'Thing' in IoT can be any scheme with any kind of built-in-sensors with the skill to gather and handover data over a network without physical interference.

II. Benefits of IoT

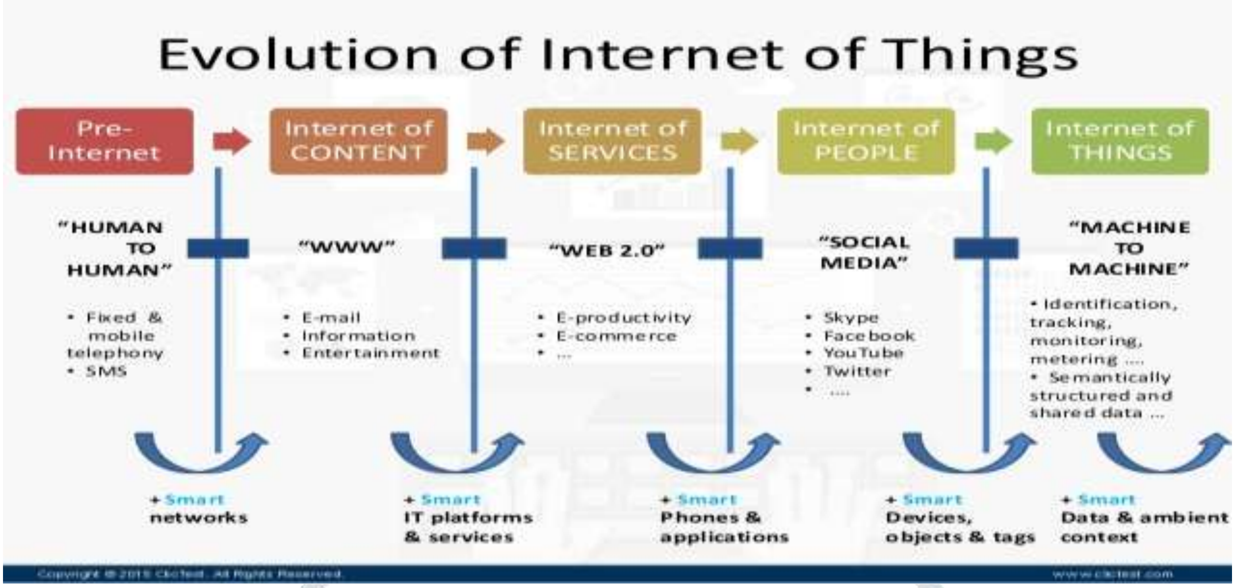
Using sensors and internet IoT allows devices to interact with each other in the physical world to the computer-based systems. IoT allows users to achieve deeper automation analysis and integration within a system. The most important features of IoT includes artificial intelligence, connectivity, sensors, active management and small device use. Multiple embedded devices are interconnected to make advanced applications. IoT technologies applied in smart grids, smart homes, intelligent transportation and smart cities. The major benefits of IoT are:

1. Behaviors of real-time marketing are tracked.
2. Increase situational awareness
3. Sensor oriented decision analytics
4. Optimization of process
5. Optimal resource utilization
6. Quick control and response of a complex automated system.

IoT devices are continuously emitting data and communicating through many remote devices.

III. IoT Hardware

The hardware used in IoT structures contains devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication, and detection to support specific goals and actions. The most significant hardware in IoT might be its sensors. These devices comprise of energy units, power management modules, RF modules and sensing modules. The common sensors are accelerometers, temperature sensors, magnetometers, proximity sensors, gyroscopes, image sensors, acoustic sensors, light sensors, pressure sensors, gas RFID sensors, humidity sensors & micro flow sensors. We also have many wearable devices like smart watches, shoes & 3D glasses which makes a smart solution. The most important device in IoT are the cell phones. Mobile apps make the world technologically revolutionized. Cell phones have Geo-location information, it can sense and trace light condition, the orientation of your device and a lot more information. Wi-Fi, Bluetooth, and cellular that assistance them to connect with other devices. Cell phones became the core of the IoT ecosystem. Today, Smartphone can interact with smart watch and fitness band to further ease and enhance the user experience. IoT uses multiple technologies and protocols to communicate with devices based on the requirements. The major technologies & protocols are Bluetooth, wireless, NFC, RFID, radio protocols and WiFi-Direct. IoT applications are booming across all industries & market. The IoT has a multitude of expansion over various industries. It spans over all groups of users, from those who are trying to reduce & conserve energy in their home to large organizations who want to improve their business operations.


Evolution of Internet of Things
Pre-Internet
Internet of CONTENT
Internet of SERVICES
Internet of PEOPLE
Internet of THINGS
"HUMAN TO HUMAN"
• Fixed & mobile telephony
• SMS
"WWW"
• E-mail
• Information
• Entertainment
"WEB 2.0"
• E-productivity
• E-commerce
• ...
"SOCIAL MEDIA"
• Skype
• Facebook
• YouTube
• Twitter
• ....
"MACHINE TO MACHINE"
• Identification, tracking, monitoring, metering ....
• Semantically structured and shared data ...
+ Smart networks
+ Smart IT platforms & services
+ Smart Phones & applications
+ Smart Devices, objects & tags
+ Smart Data & ambient context
Copyright © 2015 CkcTest. All Rights Reserved.
www.ckctest.com

evolution of internet of things

IV. Cybersecurity for the Internet of Things

Privacy is a major concern not only in IoT but also in all the applications, devices or systems where we share information. Users need to take precautions to secure their information. Hackers are always trying to hack the information in the IoT ecosystem. The Open Web Application Security Project's (OWASP) internet of things Top 10 Project aims to educate users on the main facets of IoT security and help vendors make common appliances and gadgets network- and Internet-accessible. The project walks through the top 10 security problems that are seen with IoT devices and discusses how to prevent them. Its list is as follows:

1. Insecure Web interface
2. Insufficient authentication or authorization
3. Insecure network services
4. Lack of transport encryption
5. Insecure cloud interface
6. Insecure mobile interface
7. Insufficient security configuration
8. Insecure software or firmware

These projects are for the future security standards for the users in the network of devices. Data is everywhere in the cyber environment and we need to secure from the hackers. Cybersecurity is adjusting to the new demands of the widespread network. Cybersecurity is growing as the digital revolution embeds itself in new parts of society every day. The three things need to know about cybersecurity in the world is increasingly dominated by mobile technology and the Internet of Things.

1. Mobile becomes the standard

Currently, mobile devices were secured onto a company's IT strategy because the devices themselves were what professionals used when they were traveling or between times when they were sitting at a computer. Mobile usage is rising in this technological world as Skyrocket. Each and every one treats mobile like a central component of its IT, data, and cybersecurity policies.

2. IoT complexity is increasing

IoT devices changed the IT security. IoT devises brings more complexity and risks to the corporate network and its growth is incredible. In this world, it is over 3 billion smartphones and 8 billion IoT devices. This number will reach 25 billion by 2020.

3. Cybersecurity provides public security

Here security is a major issue where the data loss and leakage of productivity and profitability is a bigger concern. IoT connects devices on the internet and it creates great attack surface for the black hat hackers.

Internet of Things devices no longer represent a niche market; rather they've become a mainstream part of our lives both inside and outside the workplace. Gartner predicts that nearly 20 billion IoT–connected devices will be online by 2020.The August 2016 Mirai botnet attack targeted Internet recording devices to create one of the largest DDoS attacks in history, and an August 2017 attack lead to the recall of 500,000 pacemakers over fears that security gaps could cause someone to manipulate the heartbeat-regulating device.

IoT devices improve our lives and businesses in many ways, so securing these devices become a major challenge in 2018.Identity management can help to reduce the risk the attack surface. Each device has an identity and multiple user credentials to manage. Three-way trust between a user device and the application drastically will reduce the attack surface. More people are adopting IoT as a reality of the modern life and workplace, companies need to ensure the security of these devices. For this Government has taken the initiative to secure the connected devices. Securing and supporting IoT was a priority set forth in the Commission on Enhancing National Cybersecurity's report in December 2016, and, last year, the U.S. Senate introduced the Internet of Things Cybersecurity Improvement Act of 2017 to establish guidelines for securing devices procured by the U.S. government. Companies adopt set of guidelines to secure development and deployment of IoT devices. Identity focused security solutions manage the relationships between these devices.

V. An Intelligent Cybersecurity System

In order to manage the safety of IoT, the systems must be brainy and able to work without human interference, knowing how to take defensive and proactive actions. The number of connected devices is huge so it is impossible for the people who own the internet of things to identify and stop risky activities. To recognize devices and behaviour of the patterns which represents a threat, the IoT system will be secure and intelligent which identify and spot all devices connected and the vulnerabilities they have IoT approve and deny the accession to the networks and learn the continuously evolving conditions to become more intelligent and effective over time. All intelligent products know the patterns of secure and insecure activities which look alike on connected devices. An intelligent system would always identify suspicious network traffic in the system. To secure the IoT system, an intelligent system can take action. An intelligent system can identify the malicious and suspicious activities in the network and stop the device from being used for malicious activities.

Cyber-attacks always hit businesses from all corners and through all channels, where IoT is a larger attack surface. As compared to any other field internet technologies are growing faster than any other field in this world. So it faces many security threats that are never seen before. As per the estimations from brands like Gartner and Cisco by 2020 more than a billion devices will be connected through networks to shape the advanced internet of things ecosystem. The security of IoT devices means protecting interconnecting devices and networks in the ecosystem of the internet of things. IoT applications are found to be in the sectors ranging from appliances to machine to machine to smart energy grids. It is relatively a new idea of connecting devices like appliances. Such devices are not designed with the security of data communication as a priority. This leaves the choice for cyber crooks to influence the safety loopholes in these IoT devices to hack the entire network which is secured otherwise. What makes these devices susceptible to hacks is their old unpatched entrenched OS and software. Further increasing the risk is the inability of buyers of these devices to change default passwords and even if they do change them, the new passwords are not strong enough. The risks are possibly incapacitating and new security attacks furthermore highpoint the security fears.

VI. Security Threat Types of an Internet of things

The attacks in the IoT is on the connected devices which is an entry point into the network. Without proper security, it causes privacy risk and increased security threat, if it is a new smart car or smart air condition device. Many conventional attacks capable to exploit the security loopholes in the internet of things ecosystem. Most common of these attacks are:

1. IoT Botnets

According to Wikipedia, “A botnet is a number of Internet-connected devices used by a botnet owner to perform various tasks. Botnets can be used to perform Distributed Denial of Service Attack, steal data, send spam, and allow the attacker access to the device and its connection. The holder can control the botnet by command and control (C&C) software.”

The botnets like. Mirai, Aidra, and Linux/IRC Telnet affected the internet of things. These botnets are known as thing bots.These thingbots consist of all devices including smartphones to laptops and smart devices like TV, refrigerator. When the IoT devices are infected by the botnets then it will become the part of the DDOS ecosystem.Then it will send requests to target server to crash it.This kind of attack would not be traced easily so it will attack the whole network.

2. Man-In-The-Middle Attack

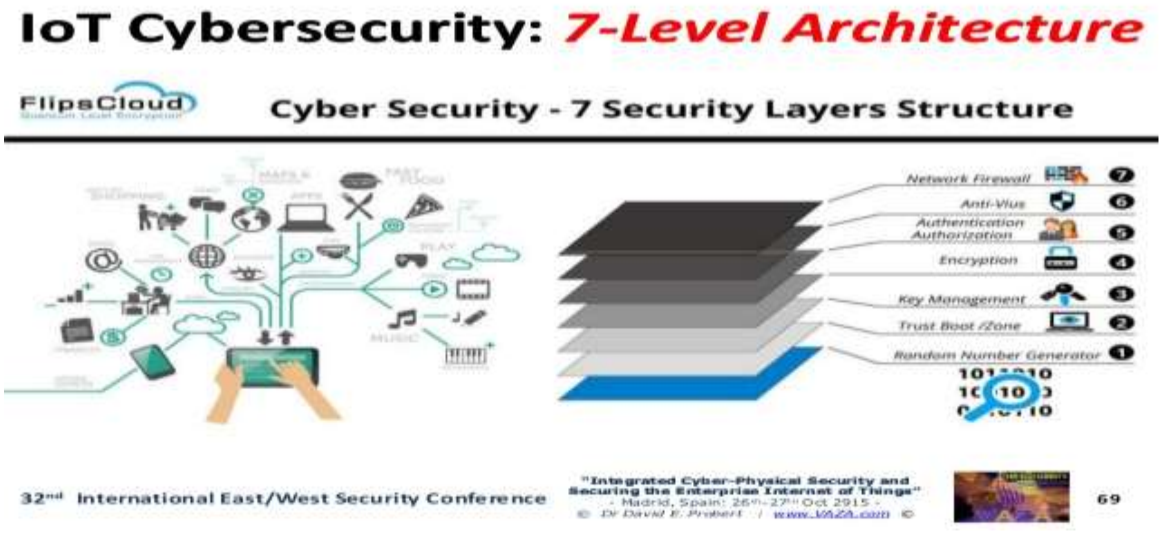
The committee will attack or disturb the communication between two systems. The invader can change the data without both parties knowing it. The receiver will get the deployed data without acknowledgment of any interruption by the invader in between. This risk can get very hazardous and such cases are already being stated.

3. Data & Identity Theft

As the internet is growing more and more than it has the higher risk to get stolen and to do identity theft. Hackers can easily access the private data from smart devices like smartphone, smart watch etc. With the IoT devices, it is very easy to hack the data about that and to perform the identity theft.

VII. IoT Security Concerns

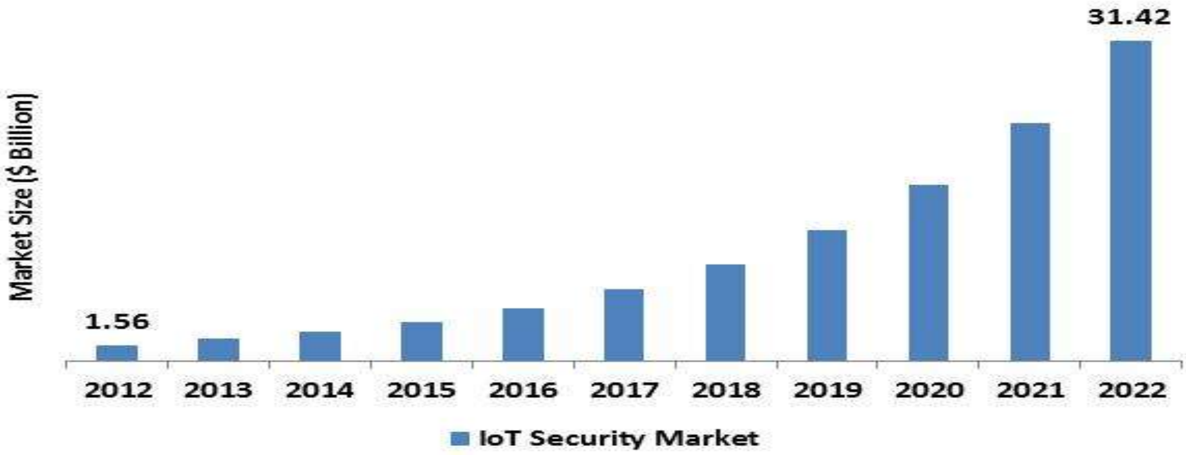
In IoT security threat to privacy is most concerning matter. Interconnected devices in the internet of things concerns about the data that will be collected and how it will be used. This is not only for individuals but also for businesses.


IoT Cybersecurity: 7-Level Architecture
FlipsCloud
Cyber Security - 7 Security Layers Structure
Network Firewall 7
Anti-Virus 6
Authentication Authorization 5
Encryption 4
Key Management 3
Trust Boot /Zone 2
Random Number Generator 1
32nd International East/West Security Conference
"Integrated Cyber-Physical Security and Securing the Enterprise Internet of Things"
- Madrid, Spain: 26th-27th Oct 2015 -
© Dr David E. Probert / www.VAZA.com ©
69

IoT cybersecurity: seven level architecture

VIII. IoT Security Companies and Start-ups

There is a lot of budding the internet of security arcade. According to M2M Magazine-The IoT security market is expected to grow from USD 6.89 billion in 2015 to USD 28.90 billion by 2020, at a Compound Annual Growth Rate (CAGR) of 33.2% from 2015 to 2020. Some of the key players in this market include Cisco, IBM, Infineon Technologies, Intel Corporation, and Symantec.



IoT security market

This is bringing in start-ups and tech giants on the same platform. Existing internet of things companies like Google, IBM and Cisco are improving their infrastructure to add security provisions where Mocana, Argus, and Rubicon like start-ups are offering smart solutions to issue security concerns for IoT devices and networks.

IX. Security Solutions of internet of things

The security experts suggest some security solutions to IoT. First thing is to direct access to the internet should be segmented into their own networks that have restricted access. Then it is easy to monitor a device's network segment for any anomalous traffic. Data security and privacy policies need to be improved by the Companies. To substantially decree see the security risk it is mandatory to provide training and guidance to common people and business staff on securing their IoT device .

X. Conclusion

The connected devices in the IoT demand security. To achieve protection from various types of threats and vulnerabilities cybersecurity is defined as a process to protect IoT devices against physical damage, unauthorized access, theft, loss by providing confidentiality and integrity of information. IoT belongs to increase in the automation of the Systems. Automated security monitor is essential in the IoT environment. In each level of your network security teams can manage devices and data. The cybersecurity area balances the threat detection and integrates all aspects of digital infrastructure connected via the IoT. To sustain the competitive advantage resulting from your innovations, you must be able to protect your valuable data. Cybersecurity's evolution will help you in working to protect the data that is critical to the success and growth of your business. Detecting and responding to threats isn't getting easier. A rising tide of known threats and the mainstreaming of cybercriminal activities have created an undercurrent of concern

REFERENCES

[1]. Omnar bajaras." How the iot is changing" https://securityintelligence.com/how-the-internet-of-things-iot-is-changing-the-cybersecurity-landscape/
[2]."Cyber risk in the internet of things".https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html
[3]. University System of Georgia "cybersecurity and internet of things "https://www.coursera.org/learn/iot-cyber-security
[4]. Lisa Froelings "Cybersecurity threats in the internet of things "https://www.cso.com.au/article/632981/cybersecurity-threats- age-iot/
[5]. Cybersecurity https://www.techopedia.com/definition/
[6]. computer-security https://www.techopedia.com/definition/27682/sandbox-computer-security
[7]. Shubham Singh "Introduction to internet of things"https://www.edureka.co/blog/iot-tutorial/
[8]. TechTarget. (June 2014). "Internet of Things (IoT)".
[9].Padraig scully "understanding IoT security"https://dzone.com/articles/understanding-iot-security-part-2-of-3-iot-cyber-security
[10]."Naresh Persuade" https://www.csoonline.com/article/3244467/internet-of-things/2018-