International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Secure Integration of Cyber Security and Internet of Things in Addressing its Challenges

S.Malathy, C.N.Vanitha

Abstract*— *The main objective of this paper is to give details about the security problems related to IoT and ways to overcome it. Almost everyone are accessing to internet daily. Most crucial data are shared over internet among various persons. Things which are connected to internet are known to be Internet of Things. Even though Indians are facing the huge attack, they are the leading internet users around the world. The main type of attacks are Phishing, smart phone attacks etc. This the main reason for the raise of internet security which is termed as cyber security. Setting strong passwords, preventing illegal access using two factor authentications are most common ways for preventing the things from internet.

Keywords: Internet of things, IOT security, hacking.

I. INTRODUCTION

Now we are living in the 21ST century which is full of developing technologies with lots of production and few security issues. So, everyone must be safe and secure to survive this technology world [1]. Cyber security is used to protect the smart devices, the computer privacy and other digital systems in this world of digital environment. In this last two decades the risk in security has been increased rapidly. The Internet is been connected with all devices in this world [2]. Computers are providing the common platform to everyone in digital environment for accessing the devices connected to the internet. The resources are equal for everyone so that it means that terrorists are also has same technology, so that they can harm us. In this world, internet is connected with almost young age to old aged people. If there is no internet, no man can live in this world. Technology has developed rapidly in these past decades, it has more advantages [1] at the same time it has disadvantages such as online frauds. This paper will gives you the detailed view of cyber security.

II NEED OF CYBER SECURITY

Cyber security is needed for every individual person to browse their needs and protect us from online frauds. A person anyone can't live without internet because everyone fall under technology world and social media. Everyone use internet to top their needs for example, student may browse to obtain study material. So everyone need is different but they are in common internet platform [3]. There is risk of cybercrime to steal the data without the knowledge of the person; everyone needs a security in this platform. For this government has also undergone the threat in the internet but they can't able to manage it because less security in sever maintenance in government sector. So everyone needs security in this digital world.

In this world of advanced [7] technology, online stealing can be done easily so that the privacy is important to secure data and their safe browsing needs they need. Everyone needs security to safe their data.

III ANALYSIS OF INTERNET USERS

In India there are about 483 million of internet users before 3 years .India provides 1.5GB mobile data at a cost of 0.28$. India emerged as the second largest online market around the world [9]. The mobile phone users are the maximum users of internet.

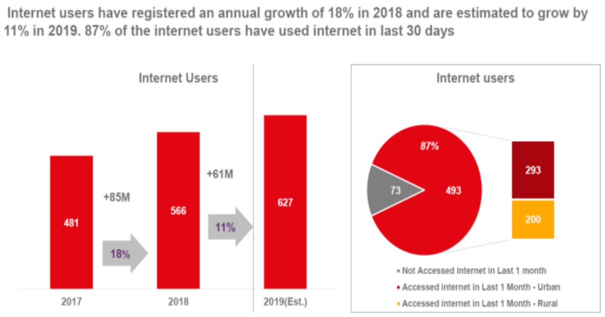


Fig 1. Analysis of internet users

They take merits of fewer alternatives to luxurious landline connections that require PCs and infrastructure. By 2016, India has 325.60 million mobile internet users and forecasts calculate approximately as 490.7 million Indian mobile internet users by 2022.

IV. CYBERCRIMES

More advanced tools are used to overcome the privacy of user by cybercriminals and obtaining the required results. 2 billion data records have been compromised by the year of 2017 [10], more over additional 4.5 billion records were breach in the first half of 2018 alone. The rising trends and the security issues are listed below.

Manuscript published on November 30, 2019.
* Correspondence Author

Malathy.S*, Department of CSE, Kongu Engineering College, Perundurai, Erode, Tamil Nadu India. (Email: ksmalathy@gmail.com).
Dr.C.N.Vanitha, Department of CSE, Kongu Engineering College, Perundurai, Erode, Tamil Nadu India. (Email: rushtovanitha@gmail.com.)

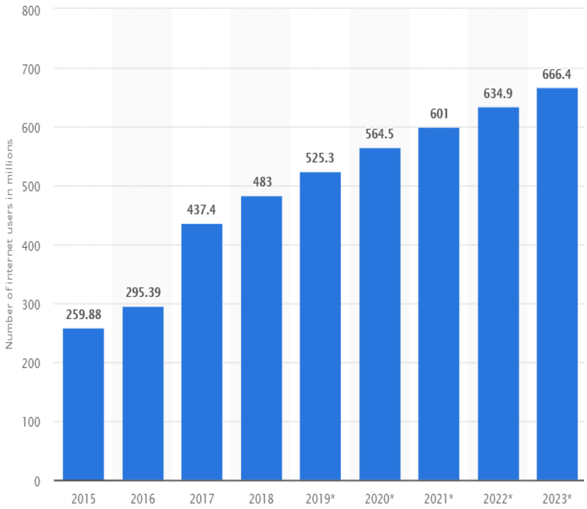


Fig 2. No of internet users in India from 2015 - 2023

Advanced phishing kits

For every four seconds a four different type of malware samples has been developed and the speed is the main reason for the success of phishing, as most phishing sites stay almost about four[8] to five hours online. 17% of phishing attack has been reported by the user, and it is considered as a low-risk activity type. And at last, only 63% of all URLs can be considered as trustworthy. This puts a pull on the consumer and the enterprise with an online company. By 2020 there will be more advanced phishing attacks, due to availability of large number of new phishing kits on the dark web[4].

Remote access attacks

Remote attacks are growing in number, and also becoming more and more complicated. Crypto jacking is the main types of remote access attack in 2018.This targets the owners of crypto currencies [2]. Perimeter devices have threatened is another type of attack. According to many reports of the intelligence available database, the attacks which are accessed from remote access are the most usual attack vectors in a internal connected home network. Crackers target smart phones, network attached storage device, cameras connected with internet and personal computers. These tools should have open ports and forwarded to internet which is external of the networks.

Attacks via smart phones

The attacks to the mobile phones are common nowadays. The mobile phones are the cause to insecure browsing leads to malware, phishing and spear [1]. Mobile phones are mainly skilled with platform are leads to online frauds about 70%. The main lead to mobile threats is only through mobile apps and web browsers. Usually the mobile users had done their mobile operations from their home network for financial and highly sensitive data. As most of them use their mobile phones to do their monetary transactions or wish to hold sensitive data trusting the security of their home network [4], this becomes a high up threat.

The fact is that most of the users hold most of their information on their phone, The two-step authentication is recently enabled to avoid frauds. It is one among the most usual methods to cyber security tools –but it also increases the risk suppose the device is stolen or lost.

V.IoT THREATS & RESULTS

- Artificial Intelligence
- Cloud Technology
- Machine Learning
- Internet Of Things (IOT) etc.,

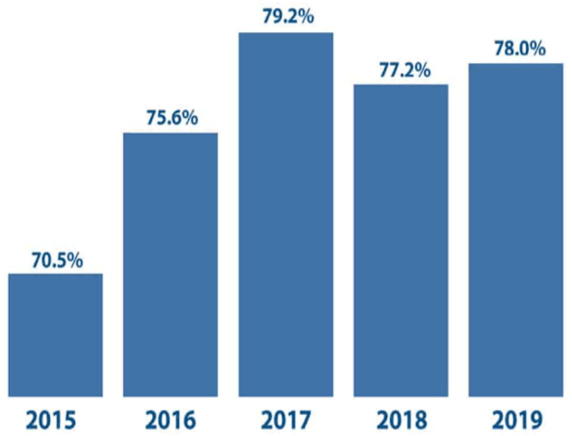


Fig 3. Smart phone Attacks.

A Internet of Things

Internet of things (IoT) is integrated with combination of mechanical and digital machines [1]. computer systems. Objects and people are referred as unique identifiers. They are capable of transferring over network without human to computer interaction and human to human interaction. IOT is worked on the basis of network connectivity and web based technology [7].

B Secure Integration

- Smart cities
- Smart Home applications
- Agriculture
- Industrial Automation
- Health care

Main reason for need of security is to prevent the data from illegal access of online fraud and to data corruption in IOT applications. Due to increase of mobile applications more than computers and laptops everyone are in the world of technology [9]. world to explore something new and gathering technology in fraction of second, so in this world only 30-40% of people know and securing their devices before any malware attack or any other cybercrime activities. Everyone must be give an alert or security breaching to them, in IOT is based on network and mobile devices in this world.

Security is the main issue in IOT connecting devices in which to avoid online fraud or hackers. In which IOT has played a vital role in the digital world in each applications. IF the multiple device or connected together one system is hacked by someone then the whole security network can be access easily. Some are the issues,

Network is main part of IOT to handle the connected devices with in the smart activities. So network is been important to store data in cloud and the access the IOT.

That main thing is that IOT network is wireless and being challenging to handle the online frauds and some protocols. We must be secure by using the strong password to connect to our network.

C Device Authentication

To access the device, network that connected to the devices must secure using the authentication. In that way we can use two step authentications [6], it is authorized to transfer the data of IOT devices access. The authentication may contain user name and passwords and the biometric to access data which is to Connect IOT.The access of each device using the only mobile application to connected IOT devices for the quick access. That mobile application must be safe and secure it needs to prevent from any malware attack to hack that mobile application to access the devices. The application must give an update and common bug must be fixed and patches or some other lope wholes must handle and fix the problems of the application.Due to the unknown application there is high risk of getting attack of the malware in the connected devices. It may make improper function of IOT connected devices. So we must be safe and secure our devices and by the knowledgeable application to given permissions on[10] your devices. Malware may use your devices and access to get hardware access to network database in wireless IOT.

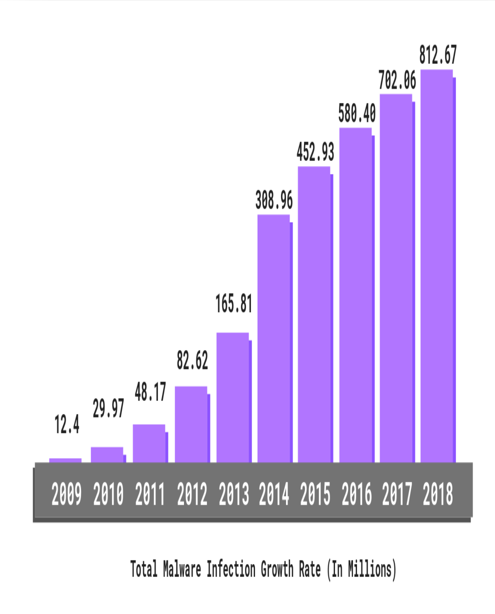
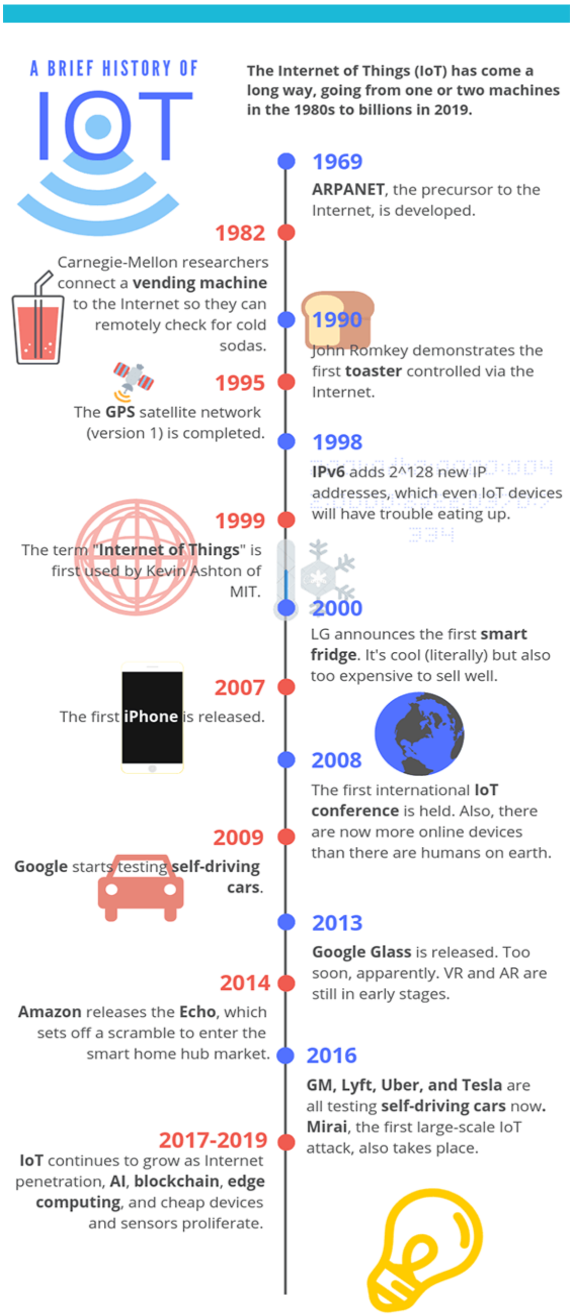


Fig 5: Total Malware infection growth rate (in millions).



The Internet of Things (IoT) has come a long way, going from one or two machines in the 1980s to billions in 2019.

1969
ARPANET, the precursor to the Internet, is developed.

1982
Carnegie-Mellon researchers connect a vending machine to the Internet so they can remotely check for cold sodas.

1990
John Romkey demonstrates the first toaster controlled via the Internet.

1995
The GPS satellite network (version 1) is completed.

1998
IPv6 adds 2^128 new IP addresses, which even IoT devices will have trouble eating up.

1999
The term "Internet of Things" is first used by Kevin Ashton of MIT.

2000
LG announces the first smart fridge. It's cool (literally) but also too expensive to sell well.

2007
The first iPhone is released.

2008
The first international IoT conference is held. Also, there are now more online devices than there are humans on earth.

2009
Google starts testing self-driving cars.

2013
Google Glass is released. Too soon, apparently. VR and AR are still in early stages.

2014
Amazon releases the Echo, which sets off a scramble to enter the smart home hub market.

2016
GM, Lyft, Uber, and Tesla are all testing self-driving cars now. Mirai, the first large-scale IoT attack, also takes place.

2017-2019
IoT continues to grow as Internet penetration, AI, blockchain, edge computing, and cheap devices and sensors proliferate.

Fig 4. History of Internet of Things

We must monitor all these types of some issues on IOT to have safe and secure the IOT connected to the devices and the network database and securing the password IOT wireless.

D Solution to IoT security

It is important that we have to use strong authentication such as passwords and some biometric lock[9] to access of data in the IOT. Because it has wireless network so that we can safe and secure the data.

It is very important in every place where IoT connected devices. By using the password need of secure and strong password to have prevented it from online fraud.

Applications to access the IoT connected devices must be regularly updated and monitor the accessing devices that is secured or not. Once there is any mistake or bug it must be updated.

VI. CONCULSION

Internet of Things (IoT) is the concept in which the near world of technology is connected to the real things of world. IoT makes us more comfortable by providing remote access to the things in the real world at same time it leads to a lot of security problems. This paper gives the various security issues and the mechanisms to overcome it. Everything is invented to make us more comfortable it is now in our hand to handle it safely..

REFERENCES

1. Yang Lu ; Li Da Xu "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics" IEEE Internet of Things Journal, Volume: 6 , Issue: 2 , April 2019.
2. Aishah Abdullah, Reem Hamad, Mada Abdulrahman, Hanan, Moala Salim "CyberSecurity: A Review of Internet of Things (IoT)Security Issues, Challenges and Techniques", 2nd International Conference on Computer Applications & Information Security (ICCAIS) , 2019.
3. A. Abubakar, H. Chiroma, S. Muaz and L. Ila, "A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven Based Intrusion Detection Systems", Procedia Computer Science, vol. 62, pp. 221-227, 2015.
4. R. Alguliyev, Y. Imamverdiyev and L. Sukhostat, "Cyber-physical systems and their security issues", Computers in Industry, vol. 100, pp. 212-223, 2018.
5. "Cyber Security" by Nina Godbole and Sunit Belapure, 1 January 2011.
6. "Cryptography and Network Security "- Principles and Practice by Stallings William, 30 June 2017.
7. "Online Safety: Scams, SPAM, Viruses and Clouds (Cyber Security Community Book 1)" by A. M. Perry.
8. JooChan Lee ; JangHoon Kim ; JungTaek Seo" Cyber attack scenarios on smart city and their ripple effects", 2019 3rd IEEE International Conference on Advanced Information and Communications Technologies (AICT).
9. Dr. Adhikari Jeevan Prasad," A critical study on cyber security in IT organization", International Journal of Management, IT and Engineering, Volume : 9, Issue : 3, 2019.
10. Boris Svilicic,Junzo Kamahara,Jasmin Celic, Johan Bolmsten," Assessing ship cyber risks: a framework and case study of ECDIS security", WMU Journal of Maritime Affairs, pp 1-12, October 2019.
11. https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cyber crime-trends-of-2019/ [Mar 4 2019]
12. Kam-Fung Cheung Michael G.H.Bell, "Attacker-Defender Model against Quantal Response Adversaries for Cyber Security in Logistics Management: An Introductory Study", Elsevier Science direct, October 2019.
13. Boris Svilicic, Igor Rudan, Alen Jugović and Damir Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System",Journal of Marine Science and Engineering, volume 7, Issue 10, 2019.
14. K. Krishna Jyothi and Dr. Shilpa Chaudhari, "A Survey on Security Aspects of Machine Type Communications in Long Term Evolution Networks", Volume 11, Special issue 3, Pages: 1874-1888.
15. https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cyber crime-trends-of-2019

AUTHORS PROFILE

Malathy S received her Master degree in Computer Science and Engineering in 2012, and the Bachelor degree in Computer Science and Engineering in 2010 from Anna University, Chennai. She is currently pursuing her Ph.D degree in Information and Communication Engineering at Anna University, Chennai. She is currently working as an Assistant Professor in Computer Science and Engineering department at Kongu Engineering College. Her research interests include Wireless Sensor Networks, Cybersecurity and IoT. She published her works in various International journals, such as Computational and Theoretical Nanoscience, Computing and Communication. She presented her views in 4 International and 6 National Conferences.

Dr.C.N.Vanitha is a Professor of Department of Computer Science and Engineering, Kongu Engineering College, Perundurai, TamilNadu, India. She has been awarded Ph.D in wireless sensor networks titled "Secure Routing in wireless sensor networks with pruning and pattern synthesis process" from Anna University Chennai. She completed her Master degree in Computer Science and Engineering with distinction from Anna University, Chennai, India in 2008. She obtained her M.Phil., M.Sc. and B.Sc. degree in Computer Science from Bharathiar University in 2004, 2002 and 1999 respectively. She has a teaching experience of about Eighteen years. She was awarded as Best Faculty Award on May 2019 at Kongu Engineering College, Perundurai. She is a life member of ISTE. She has edited 4 books for placement and training. Her research interests are in the area of Wireless Sensor Networks, Network Security and Neural Networks. She published about 14 articles in refereed journals and 20 articles in various National and International Conferences. Her recent publications have appeared in Wireless Personal Communications, Springer. She has organized a Workshop on R – Tool Programming in association with KEC, Perundurai. She has given invited talk at Infosys Campus Connect Seminar held at Dr. Mahalingam College of engineering and technology, Pollachi. She also served as Session Chair for International Conference ICCNS 2016 held at Singapore