Cyber Security and Internet of Things

Deepak K.R. Singh

Department of Information Technology

B.K. Birla College of Arts, Science, and Commerce (Autonomous)

Abstract

This paper shows the Cybersecurity and IoT devices. According to SYSCOMM, the demand for IoT devices will be getting an increase. IoT devices are very reliable to use but they have a high rate of risk from the cyber-terrorist. With the rapid growth of the Internet-of-things (IoT), concerns about the security of IoT devices have become notable. This paper also shows some company methods to overcome the cyber-attack problem and demand for cybersecurity. Cyber-attacks are not new, but most IoT devices have not the ability to prevent themselves from cyber-attacks.

- Keywords: Internet of Things, Cyber-attack, Cyber-Security.

1 Introduction

The rate of demand for IoT devices and technology is increasing day by day. Cyber-attack is an attack that causes us major damage to our social life. We have to try to protect our social life.

The major disadvantage of IoT devices is they work only if they are connected to the internet, so any other attackers get access to the same network, then they get a high chance to control IOT devices with their device. IoT devices are used for the security purpose of the high-value product, it has to secure. It is going to easy for attackers and tough work for a developer to replace IoT devices with a small and cheap product. Here, this paper tries to shows the demand for cybersecurity, the Attack rate of cybersecurity. There are some industries where anonymous authentication is needed, and there are schemes which are designed to provide functionality as the server-aided attribute-based signature with revocation scheme proposed and the privacy authentication and key agreement protocols for group discussion in rigidly following the access policy is crucial in most application. There might be times where previously unauthorized users need to access encrypted data. E.g., Yang, Liu, and Deng proposed a lightweight break-glass access control system that supports the typical attribute-based access and unexpected break-glass access. Specifically, in the latter, a break-glass access mechanism allows one, say a medical practitioner at an overseas emergency department, to bypass the access policy to gain access to

the patient's data stored in his/her home country healthcare system to formulate an immediate treatment plan

Objectives

- The main target is government websites, financial systems, news, and media websites, military network, are the main targets for cyber-attacks in cybersecurity threats.
- IoT devices can provide computing function, large data storage, and network connectivity for equipment that previously lacked them, enabling new efficiencies and technological capabilities for the equipment like remote access for monitoring IoT devices, configuration, and troubleshooting of the IoT devices.
- The objective of cybersecurity is to protect network devices which require a cybersecurity framework covering all layers of IoT systems and across platform boundaries.
- IoT requires a cybersecurity framework covering all layers of the IoT systems and platform boundaries. However, the existing security solutions are not appropriate since they don't scale to a large network of devices and cyber-physical systems with resources or real-time requirements.

Methodology

There are different types of cybersecurity assessment. The following sections show methodologies and provide additional information on the strengths and weaknesses of each. This document includes information on the methodologies:

• network scanning
• vulnerability scanning
• password cracking
• log review and analysis
• file integrity checking
• malware detection
• wireless testing
• penetration testing

- **NETWORK SCANNING:** Network scanning involves tools to identify all hosts connected to a network and find the operating system and network services running on those hosts. Network scanning is typically accomplished using port scanners for network scanning that identify active hosts in a user-specified address range. Once the active hosts have been identified, they are scanned for open ports in the system port numbers are used to identify the network services that are likely operating on that host.

- **VULNERABILITY SCANNING:** Vulnerability scanning involves a vulnerability scanner to identify out of date or expire software version, to identify applicable or manageable patches or system upgrades, and to validate compliance with the deviations from the security policy. As a network scanner, a vulnerability scanner identifies open

ports in the system, and major software applications running on hosts in the operating system.

- **PASSWORD CRACKING:** User identification (ID) and passwords may be used as part of a defense in strategy for critical situations, like process control and safety operating systems, on the NPPDN. Access control to the NPPDN and NPP systems can be accomplished using access control lists (ACL), assignment of user ID and password, and levels of authorization in the system.

- **FILE INTEGRITY CHECKING:**
Checking the integrity of files involves a checksum for every guarded file and storing that file checksum in a database for future use. File integrity checkers are a tool for the system administrator to recognize unauthorized changes. Stored checksums should be recomputed daily to test the current value against the stored value to identify any file modifications. A file integrity checker capability is usually included with any commercial host-based IDS in the system.

- **MALWARE DETECTION:** Malware detection involves software to detect viruses, worms, keystroke loggers, rootkits, or spyware on information processing systems, no matter the source of infection. And the overwhelming majority of malware attacks are not associated with energy production and control systems. These systems are becoming increasingly connected with IP networks and, therefore, are more susceptible to Internet threats.

- **WIRELESS TESTING:** Wireless technology is rapidly growing in the area of networking. The use of wireless communications in energy production has been associated with the connection of distance through radio, microwave, or sometimes satellite to provide distant reach back. With the introduction of substation automation, the use of wireless applications is expanding in recent years. Wireless local area networks (WLAN) are rapidly replacing unauthorized system as the most popular back door into networks, because they may provide attackers the means to bypass firewalls and ID if the access point is placed within the security perimeters in the IoT system.

- **PENETRATION TESTING:** Penetration testing is a methodology in which evaluators (e.g., the cybersecurity team or approved contractors) attempt to circumvent the security features of a system based on their understanding of the system and implementation. It is an iterative process where the testers attempt to leverage minimal access to gain greater access to the system. The purpose of penetration testing is to identify methods of gaining unauthorized access by using tools and techniques commonly used by attackers.

HERE WE GOING TO SEE A COMPANY METHOD TO OVERCOME WITH CYBER ATTACKS PROBLEM IN HER CARS.

The company name is Tesla. What if the Tesla car got hacked? Tesla owner said that the biggest risk of an autonomous vehicle is somebody achieving a fleet-wide hack that will be the end of Tesla. So, if the car is doing something weird, you can press a button that no amount of

software can override that will ensure that you gain control of the vehicles and cut the link to the servers.

EXPERIMENT

There are many insecurities in the Internet of Things (IoT) devices consequently leading to more calls for regulation – connected devices themselves seemingly stayed just as insecure. The most common attacks on IoT devices are DDOS attacks.
In these experiments, I try to check that how many people think that, India is not taking Cyber-Attack seriously with the help of the Chi-Square test.

RESULT

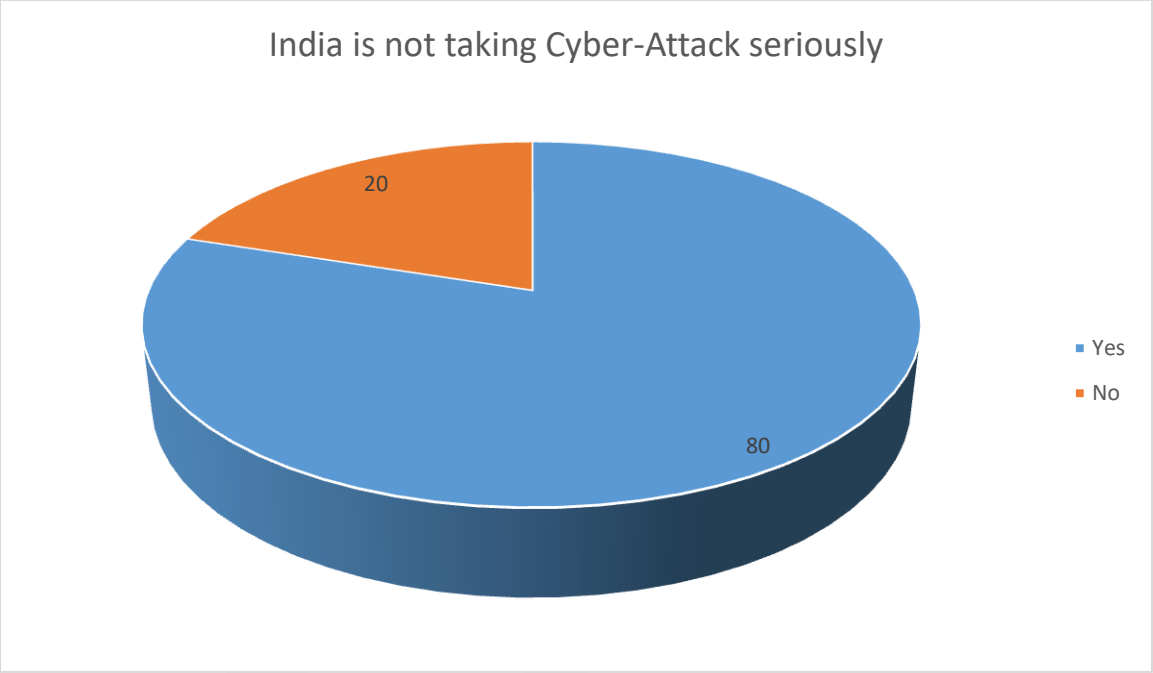

Fig 1.

The test results of paired samples rendered through survey analysis calculated using the chi square test resulted that the more amount of people thinks that India is not taking Cyber-attack seriously. According to **Herjavec Group** there will be 350% growth in open cybersecurity positions from 2013-2021.

According to **Herjavec Group** the importance of education and training for future IT professionals

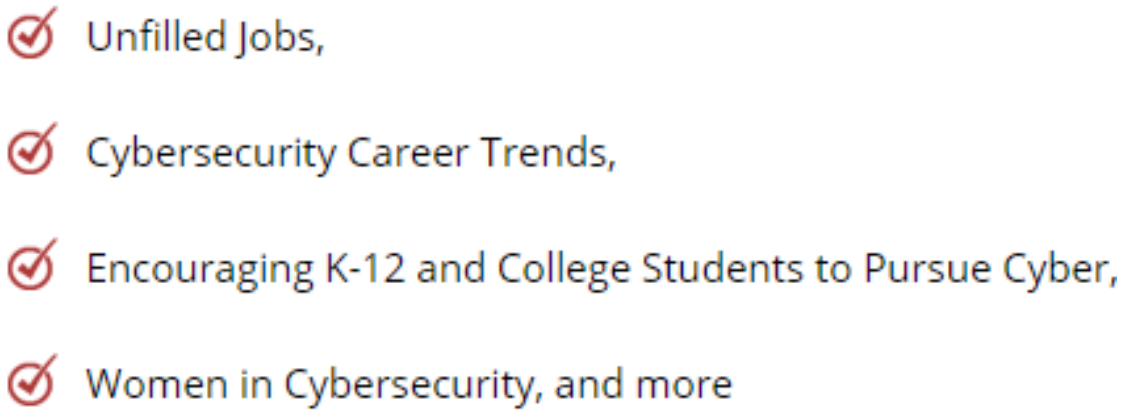

Fig 2.

Conclusion

Internet of Things (IoT) is a famous key technology that makes the way for the next generation of industrial production systems. Smart factories will consist of self-organizing production systems that optimize themselves with regard to resource availability and consumption, even across company borders. These systems enable product individualization at costs of mass production and new smart services, including product optimization according to customer usage and de-centralized long-term product support. Today's IoT systems are not sufficiently enhanced to fulfill the desired functional requirements and bear security and privacy risks. Particularly, attacks on cyber-physical systems may cause physical damage and threaten human life. The ubiquity of IoT devices may lead to a transparent society through seamless supervision of employees and customers.

Acknowledgement

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Swapna Augustine Nikale. And a special gratitude to Deepak Singh Student in Department of Information Technology of B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane Mumbai.

Glossary

1. **IOT DEVICES:** IOT Devices has the ability to transfer data without requiring human to human and human to computer physical contact.

2. **SECURITY**: Security has been defined as a process to protect a pc against physical damage, unauthorized access, theft, or loss, by maintaining high confidentiality and integrity of information.
3. **CYBER SECURITY**: To protect social life of a person there is a department known as cyber security department, which play a important role in many victim's life
4. **Data Encryption:** It is a cryptographic technique to protect the data confidentiality and integrity. In this technique readable data is converted into not readable format by applying some function like MAC on the data.

References

https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[1] Check point 2018 security report. 2018. Available Online: https://www.checkpoint. com/downloads/product-related/report/2018- security-report.pdf.

[2] The Open Web Application Security Project (OWASP). 2018. Available online: https:// www.swascan.com/owasp/

[3] Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/ CheckPointSecurityReport2019_vol01.pdf

[4] The Open Web Application Security Project OWASP Top 10—the ten most critical web application security risks. The OWASP Foundation. 2018.

[5] Check Point Research Survey of IT Security Professionals, sample size: 443 participants. 2018.

[6] Checked from this Jobs report demands https://www.herjavecgroup.com/2019-cybersecurity-jobs-report-cybersecurity-ventures/

[7] Check Point Mobile Threat Research Publications. 2017. Available Online: https:// research.checkpoint.com/check-pointmobile-research-team-looks-back-2017/

[8] Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/ CheckPointSecurityReport2019_vol01.pdf

[9] International Organization for Standardization. ISO/IEC 27032:2012. Infor mation technology— Security techniques— Guidelines for cybersecurity. 2012

[10] Hazza Z.M., Aziz N.A. A new efficient text detection method for image spam filtering. Int Rev Comput Softw. 2015; 10(1):1–8.

[11] Reuters, Landis+Gyr Technology Enables Full Service Smart Grid Coverage, March 31, 2009. .

[12] .Kai Cao, Jiajia Gao, Song Gao, Chaobo Chen, "Application of Back-stepping Method on Innovative Indoor Quadrotor Test Platform", *Control Automation Robotics and Vision (ICARCV) 2018 15th International Conference on*, pp. 966-971, 2018.

[13] Alexander Kuzmin, Evgeny Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles", *Service Operations and Logistics and Informatics (SOLI) 2018 IEEE International Conference on*, pp. 32-37, 2018.

[14] andor Plosz, Pal Varga, "Security and safety risk analysis of vision guided autonomous vehicles", *Industrial Cyber-Physical Systems (ICPS) 2018 IEEE*, pp. 193-198, 2018.

[15] Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin EL MRABTI, Gabriele LUCULLI, "Methodology for risk management related to cyber-security of Unmanned Aircraft Systems", *Emerging Technologies and Factory Automation (ETFA) 2019 24th IEEE International Conference on*, pp. 695-702, 2019.

[16] Guo Rong-xiao, Tian Ji-wei, Wang Bu-hong, Shang Fu-te, "Cyber-Physical Attack Threats Analysis for UAVs from CPS Perspective", *Computer Engineering and Application (ICCEA) 2020 International Conference on*, pp. 259-263, 2020.

[17] .Seyyedali Hosseinalipour, Ali Rahmati, Huaiyu Dai, "Optimal Jammer Placement in UAV-assisted Relay Networks", *Communications (ICC) ICC 2020 - 2020 IEEE International Conference on*, pp. 1-6, 2020.

[18] I.H. Lim, S. Hong, M.S. Choi, S.J. Lee, T.W. Kim, S.W. Lee, B.N. Ha, Security protocols against cyber attacks in the distribution automation system, IEEE Transactions on Power Delivery 25 (2010) 448–455.