International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Internet of Things, Its Risks, And Ways to Address it

Raghad Yousif

Researcher, College of Science/University of Mosul

Abstract

The internet is a vast, interconnected network of computers and other network-enabled devices, which is: Globally available ,Easy to use, Compatible with other types of media, Affordable and Flexible .The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves. Thanks to the advent of inexpensive computer chips and high bandwidth telecommunication, we now have billions of devices connected to the internet. since 2008, machines outnumbered people as "users" of the Internet, so the Internet of Things (IoT) is an interlocking network of hardware, software, sensors and other "things" as the Internet of Things (IoT) can be compared to a social network or email provider, but the Internet of Things connects devices instead of people. These devices connect wirelessly, take action and generate data In several fields such as industry, agriculture and health, it may reach unprecedented levels, which allows new technological competencies and capabilities, but what if something goes wrong or external interference in its work?, enabling new technological efficiencies and capabilities. IoT attacks present unique challenges compared to traditional IT attacks – there are real warnings about the dangers of the Internet of Things (IoT). These warnings are a way to understand the nature of the risks and how to make technology that is safer. IoT security is important because it keeps data secure, which requires specialized security measures to provide protection against these risks, which are exploiting vulnerabilities in Internet-connected devices.

Keyword: The Internet of things, Risks and threats on the Internet of Things , Ways to protect the Internet of Things

Introduction

The term "Internet of Things" was first used in the nineties of the last century to describe computer networks and Internet addresses, and Internet of Things devices are the result of combining the worlds of information technology (IT) and operational technology (OT). It is the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-priced devices, and other technological advancements.

The Internet of Things has evolved rapidly over the past few years from the idea of smart homes to industrial automation to be used in almost all industrial fields to represent the start of the new era of technology and the new era of computing.

The device can be anything from a consumer product to a giant industrial machine. It can be as small as a thumb engine or the size of a train. All these things communicate with each other without the need for human interaction. One of the simplest examples is the sensors used in stores through which to discover

how long customers spend in different parts of the store, which products they return to often, and what is the most common path for customers around it. This data can be used to identify trends, make suggestions, and detect potential problems before they arise, and Internet devices can be operated. Software things that allow the device to "decide" when to take a specific action among the different actions. The Internet of Things automates many routine activities, allowing machines to make decisions without human interaction. Autonomous devices will control inventory, license online business transactions, and arrange shipments and deliveries without human intervention. The interactions will be fast and automatic, and are carried out according to a series of pre-programmed rules whose composition and nature may not differ and are accessible to the user. These changes provide tremendous economic benefits by increasing productivity and reducing costs. In this way, the impact of IoT will reflect the economic benefits.

In this white paper, we explore how these cyber attacks on IoT devices have changed and the regulations that are being developed to ensure systems are "acceptably secure by recognizing more security standards. In this paper, we will discuss six key security risks associated with IoT devices.

1- what is the internet of thing :-

Gradually, IoT devices will perform more functions and will be more efficient and cheaper than devices that are not connected to the network as computers have become smaller, faster, connected and integrated in functions ranging from simple to complex. Computers are becoming ubiquitous and mobile IoT devices are inherently designed for communication that enables the world to communicate through physical space, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the ability to analyze data and use results to better guide decision-making, change the physical environment, anticipate future events, and as demand increases, the IoT use process will increase so that businesses and consumers use smart devices to improve existing products and services or create new ones. This new implementation of digital network technology faces many policy challenges, ranging from spectrum management, privacy, data localization and staffing to include business software, or smart home devices, care monitoring systems, mobile phones and driverless trucks. Securing these devices to protect against IoT attacks is an important step for every security team[(1)] .

After the Internet was first marketed, information technology has been the key factor in improving productivity and performance in the economy in recent years. One analyst wrote: "What is it? What's exciting about IT is not its ability to replace capital but its ability to restructure every aspect of a business, in the process of creating new types of markets and organizations."

The associated risks are thus compounded across the entire network as IoT devices become increasingly valuable and important in regulatory and industrial infrastructure. What should be considered is the amount of increased risks compared to the cyber risks we face now, and how we can manage and reduce the risks that come from using new technologies such as the Internet of Things without overreacting in ways that harm innovation, entrepreneurship and economic growth. Because IoT devices are particularly vulnerable to network attacks such as data theft, phishing attacks, spoofing and denial of service attacks leading to other threats such as ransomware attacks and serious data breaches that can cause More spending by companies and more efforts to get rid of it.[(2).]

During the first half of 2021, attacks on IoT devices grew by more than 100 percent. While the previous six months saw 649 million attacks on IoT devices, there were 1.5 billion IoT attacks during the January-May 2021 period. The sudden rise in attacks is associated with the sudden spread of the

technology class - from consumers' personal devices to industrial information technology. And across the reality of working from home for post-COVID employment, IoT is ubiquitous[3].

2- The risk of internet of things

Despite the benefits and bright prospects of IoT, there are some unresolved security issues All new technologies come with risks that need attention Since IoT means connecting multiple devices and storing a lot of data System failure can cause too many problems for computer networks and sensitive .data[4]

The growing concern about the security of IoT devices includes the fact that threatened actors can not only damage the network and software that support IoT devices, but also the devices themselves, some of these risks are easy to see and understand, such as unpatched operating systems or unsecured passwords that are easy targets for cyber attacks.

As organizations in almost every industry increase their operational reliance on IoT devices at a faster rate than processes and protocols that provide secure and reliable communications, as economic opportunities become available, the potential for risk increases as the context of IoT policy thinking exponentially increases. Security teams should consider simple and complex risk factors specific to the IoT world [5]..

Risk can be managed by limiting autonomous functions and ensuring that manual control is adopted. There are also serious and long-standing concerns about the risks of autonomy being being overdone, competing with and replacing humans. Progress towards such systems is conditional on the development of artificial intelligence, where computers work intellectually like humans rather than working through specific software, and this suggests that in order to be more confident about the reliability and safety of IoT devices, it is important to design systems that allow manual control of systems that provide vital services. For a small group of IoT devices that can manage a specific function, the increased risk justifies this[6] . Currently, the challenges created by IoT will be more realistic and include data protection, unauthorized access and control prevention, as well as authentication and encryption to manage IoT risks Technological solutions to make IoT more secure with encryption and identity authentication, increase the use of encryption and improve two-factor authentication. There are steps that organizations can take to secure the IoT attack surface but require staff and technical expertise to develop policies that can proactively detect threats and interactively implement measures to reduce the size of the attack surface.

3- Top IoT Security Risks to Address

Most researchers believe that computers used in the Internet of Things will be more vulnerable than the Internet technologies we are used to, due to the technical limitations of Internet of Things computing devices, as this computing lacks the ability to perform the traditional security functions of desktop computers and laptops, making it easy targets for attackers to access any computer device, process, extract or control data, or interrupt services, as H ackers has the ability to launch attacks on thousands. Or millions of connected devices that are unprotected or infrastructure destroyed, networks disrupted, or access confidential data. The threat represents an activity that exploits security gaps in the system to achieve a military, economic or social benefit, which has a negative impact on humans and the environment, which are the main sources of security threats, which can be classified into:

- Unregulated threats: mainly consist of beginners who use readily available hacking software.

- Organized threats: People who are aware of system vulnerabilities and can understand, build, and exploit code and scripts are known as structural risks.
- Advanced Persistent Threats (APT): A coordinated attack is an example of advanced persistent threats. APT is a sophisticated network attack that seeks to steal data from high-value information in industries such as manufacturing, banking, and national defense. (7)

Compared to a threat that can be intentional or unintentional, an attack is always intentional and malicious to cause damage to continue security attacks within the framework of the Internet of Things, to pose serious challenges to the IoT environment from a security perspective Here are some of the most frequent cyberattacks that illustrate common IoT vulnerabilities and some external threats that pose the most important risks which are six IoT attacks and security risks that you should be aware of.. .(8):

1- **Breadth of the attack area**: Arguably, the basic level of the attack surface is the total number of entry points and unauthorized access to the system and includes all the potential security vulnerabilities of IoT devices, connected software, and network connections, one of the biggest threats to an organization's ability to secure its IoT environment is its sheer size. Estimates of the actual number of connected devices in the world vary from researcher to researcher, but are in the billions and constantly increasing. For example, in the "State of the Internet of Things - Spring 2023" report, IoT Analytics put the number of active IoT endpoints in 2022 at 14.3 billion – an increase of 18% over the previous year's number. IoT Analytics estimated that the global number of connected IoT devices will grow by 16% in 2023 to reach 16.7 billion active endpoints(9).Of course, the sole proprietorship has far fewer devices to secure; however, the number is rapidly multiplying. A recent report titled "Risk and Cost Management at the Edge" conducted by the Ponemon Institute and sponsored by Adaptiva, found that the average organization manages nearly 135,000 endpoint devices. In addition, IoT devices generally operate around the clock, seven days a week with an indefinite number continuously connected(10)

2- **Unsafe devices** people's endpoint device itself can represent a security risk to the entire IoT ecosystem as device-level firewalls, strong encryption, and making devices invisible on the network are integral to preventing endpoints from connecting to IoT devices before attackers have had the opportunity to initially gain access to your network. And ultimately, on the enterprise IT environment. ... Devices often lack built-in security controls due to their limitations, i.e. their small computational capacity and low-power design. As a result, many devices cannot support security features such as authentication, encryption, and access control. And even when endpoints have some security controls, such as passwords, some organizations still deploy them without using or enabling the available security options. .(11)

3- **Maintenance and modernization challenges** :- Challenges to proper peripheral maintenance and software update create more vulnerabilities, for example, a security patch to address the vulnerability that hackers can exploit, especially if the endpoint device is old-fashioned, as many organizations use older devices in data storage that do not contain the latest security standards. When organizations with legacy devices are integrated with the Internet of Things, it can expose the network to security vulnerabilities. .(12)These devices often rely on DNS, a decentralized system

from the eighties, which may not correspond to the scale of IoT deployments that can grow to thousands of devices. Hackers can use DNS vulnerabilities in attacks to obtain data or introduce malware. Second, connectivity constraints as well as limited device capabilities and power supplies that make hardware modernization a task may make it impossible despite possible updates, and therefore the lack of visibility for their endpoints is the most important obstacle to achieving a strong security posture[13]

4- **IoT ShadowOne** :-related risk is Shadow IoT, which means deploying IoT endpoints without official support or permission from IT or security department and so unauthorized IoT devices are personal items that have an IP address, such as fitness trackers or digital assistants, but may also be technologies specific to businesses and organizations, such as wireless printers. Either way, they create risks for the organization because they may not meet the organization's security standards, and even if they do, they may not be configured and deployed in ways that follow security best practices. In addition, IT administrators and security teams generally lack knowledge of these deployments and, therefore, may not monitor them or monitor their traffic, giving hackers a greater chance of successfully hacking them undetected. Hackers can also attack the IoT ecosystem by inserting or injecting fake nodes into the network of legitimate communication nodes, thereby enabling hackers to alter or control the data flowing between the fake and legitimate nodes[14].

5- **Unencrypted data transfers** IoT devices collect packets of data as they measure and record everything from temperature readings to object speed. They send much of that data to central locations – usually in the cloud – for processing, analysis, and storage; they also often receive information that frequently informs devices of actions to take. Studies have shown that much of that data sent is not encrypted. A 2020 report from Palo Alto Networks found that 98% of IoT device traffic was unencrypted, exposing personal and confidential data on the network and allowing attackers the ability to listen for unencrypted network traffic, collect personal or confidential information, and then exploit that data for profit on the web. By accessing the network through an IoT device, attackers could steal cloud data and then threaten to keep or delete the data, or Make it public unless they pay a ransom. Sometimes .[15] Ransomware can affect companies or basic institutions, such as government services or food suppliers and thus physical devices are tampered with, which means that attackers physically access the IoT device to steal data from it, tamper with the device as a way to install malware on it, or access its internal ports and circuits as a way to break into the organization's network, as hackers can target known security vulnerabilities in the firmware. in IoT devices just as they target vulnerabilities in software deployed in an organization's IT environment..[16]

6- **IoT NetworksIn addition to vulnerabilities**, there are threats that come from outside the IoT environment. One such threat is bots. IT and security leaders in the organization have consistently listed this as a major threat in the wake of major botanic attacks, such as Mirai, that originated nearly a decade ago.In these types of attacks, an attacker infects an IoT device with malware through an unprotected port or phishing scam and engages in turning it into an IoT botnet used to launch massive cyberattacks. Hackers can easily find malicious code on the Internet that detects sensitive

devices or hides code from detection before another code unit points to the devices to launch an attack or steal information[17].

IoT networks are frequently used for DDoS attacks to confuse target network traffic. Botnet regulators find IoT devices an attractive target due to poor security configurations and the amount of devices that can be sent to the botnet used to target organizations. The 2023 Nokia Threat Intelligence Report found that the number of IoT bots involved in robot-based DDoS attacks increased from around 200,000 to one million devices compared to the previous year[18].

7. **How to protect against IoT security risks:** IT teams must take a multi-tiered approach to mitigate IoT security risks. There are some broad methods, practices, and strategies that organizations can put in place, but administrators must also have specific defenses in place appropriate to the different types of IoT attacks. IoT security is a combination of policy and software application to detect and address any threats. IT teams overseeing IoT devices should have policies such as strong passwords for any devices on the network and use threat detection software to anticipate any potential attacks. They should also have comprehensive asset detection and management software. The more IT teams see their organization's deployed endpoints and the data on their IoT devices, the easier it is to proactively detect security risks and threats[19]

Key strategies that IT administrators can use to prevent security attacks and enable resiliency include device vulnerability assessments, disruption of unnecessary services, regular data backups, disaster recovery procedures, network segmentation, and network monitoring tools, as well. Protect device security. In other words, prevent the device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other organizations, eavesdropping on network traffic, or hacking other devices on the same network sector. This objective applies to all IoT devices, as well as data security protection i.e. the confidentiality, integrity or availability of data (including personally identifiable information [PII]) collected, stored, processed or transmitted to and from an IoT device. This goal applies to every IoT device except devices that do not contain any data that needs to be protected. Finally, protecting the privacy of individuals. Protect the privacy of individuals affected by the processing of personally identifiable information (PII) beyond the risks managed by protecting the security of devices and data. Applies This target is on all IoT devices that process personally identifiable information (PII) or that directly or indirectly affect individuals.Organizations must ensure that they address cybersecurity considerations and challenges (expressed as the exploitation of security vulnerabilities by threat actors to threaten the confidentiality, integrity, or availability of devices or data). Privacy risk (defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event, usually a function of the negative impact, or the magnitude of damage that may arise in the event of an event; or the likelihood of occurrence) throughout the life cycle of an IoT device to achieve appropriate objectives and areas to mitigate risks, including understanding the risk considerations of IoT devices and the challenges they may cause to mitigate cybersecurity and privacy risks for IoT devices in appropriate risk mitigation areas. Adjust regulatory policies and processes to address cybersecurityProtection from IoT vulnerabilities and malware can be obtained in the following ways:

1. Assess the general cyber health of your business through e-health screening.

2. Assist you in creating new plans or reviewing and updating existing cybersecurity incident response plans.
3. Help you test whether these plans will be effective against DDoS attack, phishing attacks, etc. caused by a security vulnerability in IoT with Cyber Attack Table exercises.
4. Start your ransomware protection and prevention journey.
5. Helping you obtain your company's Cyber Essentials certification. You can then be sure that your IoT devices are at least protected against the most common attacks on the internet. (20)

Finally we can say .....

1- The introduction of intelligent computing devices using the Internet of Things has made daily life more convenient. All data analytics, automation, and smart devices have benefited from the introduction of the Internet of Things in human life. However, the unprecedented growth in IoT has been paralyzed by many vulnerabilities and challenges. Moreover, the heterogeneous design of IoT expands the attack surface and adds new challenges to the already weak IoT network. Successful settlement of system security can have serious consequences for users. The overall safety of the device must be considered to ensure that critical vulnerabilities are mitigated. Policies and protocols should be applied as much as possible to deter threats and attacks. In this paper, we presented a more comprehensive survey on the Internet of Things from the perspective of security threats and attacks

2- The Internet of Things (IoT) plays a vital role in connecting embedded physical and virtual objects with sensors, software and other technologies aimed at communicating and exchanging data with devices and systems around the world via the Internet. With so many features to offer, IoT is a boon for humanity, but just like both sides of the coin, technology, with its lack of information security, could lead to a big predicament if Internet of Things (IoT) devices lack sufficient security, we can only speculate on how much valuable data hackers might take from them. According to Finances Online, 98% of IoT device traffic is unencrypted. It is also reported that 83% of desktops do not support threats to IoT devices.

3- Internet of Things (IoT) is a highly developed space that houses a huge amount of sensitive data, making it a very attractive target for cybercriminals. Threats and risks continue to evolve as hackers devise new ways to penetrate unsafe systems – posing a threat to the ecosystem itself. The fear that the future may see the interdependence of machines that challenge or replace their human masters began with the industrial age and the Internet of Things is only the latest tool to expand human performance, the latest stage in automating routine activities dating back to the beginning of industrialization.

المصادر :

1. James Andrew Lewis , managing risk for the internet of things , a report of the CSIS strategic technologies program,Feb2016 .TARIQ AHAMED AHANGER, ABDULLAH ALJUMAH, Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms,IEEEAccess , vol.7, February 4, 2019.
2. Wei Zhou, Yan Jia, and other , The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEEXplore , 2018 .
3. AZANA HAFIZAH MOHD AMAN and other , A Survey on Trend and Classification of Internet of Things Reviews,IEEE Access , vol.8, June 26, 2020.

4. Lewis , managing risk for the internet of things ..,op.cit.,& 8 Internet of Things Threats and Risks to Be Aware of, security scorecard ,08/04/2021
5. TARIQ AHAMED AHANGER, ABDULLAH ALJUMAH, Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms, IEEE Access , vol.7, February 4, 2019.
6. Christian Henke, IoT attacks, hacker motivations and recommended countermeasures, 11.12.2020 , emnify.
7. AZANA HAFIZAH MOHD AMAN and other , A Survey on Trend and Classification of Internet of Things Reviews,IEEE Access , vol.8, June 26, 2020.
8. Louise Downing and Jim Polson, "Hackers Find Open Back Door to Power Grid with Renewables," Bloomberg Business, July 2, 2014, http://www.bloomberg.com/news/articles/2014-07-01/renewable & Sravya Bhamidipati, Examining Approaches to Quantifying Cyber Risk for Improved Cybersecurity Management, Master of Engineering in Computer Science and Engineering, MASSACHUSETTS INSTITUTE OF TECHNOLOGY September 2019.
9. Wei Zhou, Yan Jia, and other , The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEEXplore , 2018 , & ,**8 Internet of Things Threats and Risks to Be Aware of, security scorecard ,**08/04/2021.
10. Lewis , managing risk for the internet of things …,op.cit. & CHRISTOPHER S. YOO, The Emerging Internet of Things, CIGI,2020.
11. Katie Boeckl and other , Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks , This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8228 , NISTIR 8228 , June 2019 & Mary K. Pratt , Jessica Lulka,Top 12 IoT security threats and risks to prioritize , Published: 27 Jun 202 ,techtargt
12. Wei Zhou, Yan Jia, and other , The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved, IEEEXplore , 2018 , & ,**Christian Henke ,** What Is IoT Security? Risks, Examples, and Solutions, emnify,24.02.2023
13. Mary K. Pratt , Jessica Lulka, Top 12 IoT security threats and risks to prioritize , Published: 27 Jun 202 ,techtargt
14. Christian Henke , What Is IoT Security? Risks, Examples, and Solutions, emnify,24.02.2023& , 8 Internet of Things Threats and Risks to Be Aware of, security scorecard ,08/04/2021
15. Boeckl and other , Considerations for Managing …,op.cit. & Internet of Things (IoT) Security, HC3: Analyst Note August 04, 2022 TLP: White Report: 202208041700
16. Sravya Bhamidipati, Examining Approaches to Quantifying Cyber Risk for Improved Cybersecurity Management, Master of Engineering in Computer Science and Engineering, MASSACHUSETTS INSTITUTE OF TECHNOLOGY September 2019.
17. Elama and Anna , internet of things IoT CHALLENGES AND BEST PRACTICES , APRIORIT ,17 FEB 2022.
18. Usman Tariq,and other , A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review , MPDI, 19 April 2023
19. Ibid .
20. Sravya Bhamidipati, Examining Approaches to Quantifying Cyber Risk for Improved Cybersecurity Management, Master of Engineering in Computer Science and Engineering, MASSACHUSETTS INSTITUTE OF TECHNOLOGY September 2019.