A Study of Threats, Vulnerabilities and Countermeasures: An IoT Perspective

Yash Choudhary
Department of CSE, JECRC University, Sitapura, Jaipur, Rajasthan, India

B. Umamaheswari
Assistant Professor, Department of CSE, JECRC University, Sitapura, Jaipur, Rajasthan, India

Vijeta Kumawat
Associate Professor, Department of CSE, JECRC University, Sitapura, Jaipur, Rajasthan, India

OPEN ACCESS

Manuscript ID:
ASH-2021-08043583

Volume: 8

Issue: 4

Month: April

Year: 2021

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 09.12.2020

Accepted: 20.01.2021

Published: 01.04.2021

Citation:
Choudhary, Yash, et al. "A Study of Threats, Vulnerabilities and Countermeasures: An IoT Perspective." *Shanlax International Journal of Arts, Science and Humanities*, vol. 8, no. 4, 2021, pp. 39-45.

DOI:
https://doi.org/10.34293/sijash.v8i4.3583

Abstract
IoT or the Internet of things refers to all the physical devices connected to the internet. IoT consists of computing devices that are web-enabled and have the capability of sensing, collecting, and sending data. IoT provides the ability to remote control appliances and has many more applications. Since IoT is becoming a big part of society, it is necessary to ensure that these devices provide adequate security measures. This paper discusses various security issues in IoT systems like threats, vulnerabilities and some countermeasures which can be used to provide some security. Developing a secure device is now more important than ever, as with the increase in digitization, much of a user's data is available on these devices. Securing data is a primary concern in any system, as internet-enabled devices are easier to hack. The idea of this paper is to spread awareness and improve the security of IoT devices.

Keywords: IoT, Confidentiality, Availability, Integrity, Vulnerabilities, Threats, Counter measures, Guidelines

Introduction

As the term "IoT" suggests, the Internet of things (IoT) is electronic device that have networking capabilities. The term internet of things was produced by Kevin Ashton in 1999 to promote RFID (radio frequency identification) technology. The term did not gain any popularity until 2010 due to an information leak that Google's Street-View service stored tons of user's personal data along with 360-degree pictures. Additionally, Google's Street View cars collected emails and passwords from unprotected Wi-Fi networks. For this malicious act, Google was fined 13 Million USD. In January 2014, the term internet of things reached mass-market awareness as Google bought Nest, a home automation company, for 3.2 billion USD.

The increase in communicating and networking capabilities of machines and everyday appliances used in different sectors and the development of small and cheap computer chips has led to an increase in the production of IoT devices. Now anything as small as a pea to something as big as a whale can be a part of an IoT system.

According to American research and advisory firm Gartner, the Internet of Things (IoT) market will grow up to more than 5 billion devices in 2020. Utilities like electricity and smart metering will be the highest user and are expected to increase by 17% in 2020, reaching 1.37 billion devices. Security and indoor surveillance will be the second-largest user of IoT devices in 2020.

According to a business technology news website ZDNet, the rise of a global Internet of Things network is creating a giant, internet-connected global robot which is so disparate and insecure that cyber-attacks against it are going to cause major problems if it isn't regulated by the authorities. With the increase in the number of IoT devices, soon cyber-security professionals will need to ensure all the connected devices in the world are secure. "As everything turns into a computer, computer security becomes everything security," said cyber-security expert Bruce Schneier, speaking at the Info-security Europe conference in London.

Applications of IoT Devices

Utilities are major users of IoT devices, with smart grid technology and monitoring devices to avoid leaks and wastage.

Homes are becoming intelligent, with smart home technology and HVAC (Heating, ventilation, and air conditioning) systems. These aim to provide central connectivity to control all devices through mobile applications.

Smarter cities are important to respond effectively to the rapid growth in urban living and improve lifestyle. Waste management, smart roads, smart parking, noise maps, smart lighting are some applications. Emergency services will also be able to respond quickly to incidents.

With the decrease in environmental conditions, the need for a smarter environment is a must. Air pollution monitoring, forest fire detection, and earthquake early detection are some features of a smart environment.

IoT Architecture

There are four stages in IoT architecture. Each stage helps perform specific functions like data gathering, transportation, processing, or analysis. The 4 stages of IoT architecture:

Stage 1 consists of sensors and actuators. Actuators take action in the physical reality based on the inputs, whereas sensors take input from the environment like heat, pressure, humidity, etc. This data is sent to layer 2.

Stage 2 consists of internet gateways and data acquisition systems. It gathers data from sensors and also sends the commands to the actuators. This layer helps digitalize and aggregate the data to reduce the volume of data.

Stage 3 consists of EDGE IoT and performs enhanced analysis and pre-processing of data.

Stage 4 consists of data centers and the cloud, where the user data is stored. It also performs in-depth processing, along with a follow-up revision for feedback.

IoT is a combination of application, network, cloud, and mobile technologies, which means that IoT also includes the vulnerabilities present in all of them. There are too many attack vectors available for an attacker. All IoT devices are web-enabled, and thus it is necessary to make sure that these devices are secure before using them in critical environments like airports, banks, etc.

IoT Device Size

An IoT device consists of both hardware and software components. Generally, IoT devices use small components to produce smaller devices. This limits the device's resources and thus its security measures. The operating systems (OS) installed on these devices are also limited in size and thus provide less security than a traditional OS. Some of the operating systems used by IoT devices are RIOT, Brillo, Zephyr, etc.

Literature Review

Brian Russel et al. Cloud Security Alliance "Security Guidance for Early Adopters of the Internet of Things (IoT)" The alliance has discussed the threats and challenges in IoT technology. It has recommended several security controls like implementing layered security, data protection practices, privacy-by-design approach, and many more. They have also suggested putting more effort into the standardization of security guidelines for IoT.

US Department of Homeland Security "Strategic Principles for Securing the Internet of Things (IoT)" The DHS has discussed various strategic principles for securing IoT devices, like incorporating security at the design phase, promoting updates, using secure coding practices, etc. They conclude by first stating the consequences of vulnerable IoT devices and then

giving four lines of effort to fortify the security of IoT devices.

Vignesh et al. "Security on the Internet of Things (IoT) with Challenges and Countermeasures" The authors have discussed the different layers in the IoT structure and the security issues within them. The author concludes that if security disciplines like privacy, confidentiality, authentication, access control, end-to-end security, trust management, global policies, and standards are consigned completely, then a transformation of everything by IoT can be realized soon.

Microsoft Corporation "The Right Secure Hardware for Your IoT Deployment" The corporation has discussed the concept of secure hardware for IoT devices. They have discussed stand-alone and integrated hardware and types of secure hardware along with some common questions which arise from this topic.

IoT Alliance Australia "Internet of Things Security Guideline" The alliance has discussed IoT, their security in different layers, domain viewpoints, different guidelines like OWASP, Internet of Things Security Foundation (UK), etc. They have suggested following the principle of 'security by design'. They have also discussed some of the relevant legislation around privacy and security.

OWASP "IoT Top 10 2018" The Open Web Application Security Project (OWASP) is a nonprofit organization that improves security in the digital world. OWASP's top 10 is a document that lists the most critical vulnerabilities to a project. This document lists the top 10 vulnerabilities in IoT devices in 2018.

Threats and Vulnerabilities in IoT

A cyber threat is any malicious activity intended to harm cyberspace (anything with a computer). Stealing data, identity theft, data ransom, damaging data, etc., are examples of cyber threats. When an attacker tries to hack a system, they try to affect the confidentiality, integrity, or availability of the system. These three principles together form the CIA triad or also called the AIC triad, to avoid confusion with the Central Intelligence Agency. They are the cornerstone of any organization's security infrastructure. The CIA triad is explained below:

Confidentiality refers to the privacy of data. The data should only be accessed by those with authority to do so.

Integrity refers to the authenticity of the data. The data should not be tampered with during transit or at storage by an unauthorized user.

Availability refers to the accessibility of the service or data. Authorized users should be able to access the services and data at any time.

Table 1: IoT threats and their Description

Threats	Description
DDoS Attack	This attack compromises the availability of a server to provide services to its clients. This attack uses multiple machines to flood the targeted system with malicious/fake requests.
Sybil Attack	This attack uses a node to operate multiple identities actively at the same time. The main objective is to obtain the majority of the control in the network.
Selective Forwarding Attack	The attacker uses malicious nodes to drop packets selectively or randomly and use those nodes to forward a malicious request.
Wormhole Attack	The attacker uses malicious nodes to create a fake route which is shorter than the original one. Now the traffic passes through these nodes and the attacker can modify these data packets.
Hello Flood Attack	An attacker with the use of high-powered transmitter can trick the nodes of network into believing it is a neighbor.
Sinkhole Attack	Under this attack, all the data flowing through the network is diverted to one compromised node in the network by making it an attractive routing path.
BlueBorne Attack	The attacker exploits the vulnerabilities of Bluetooth to compromise the device. It is an attack that an attacker can use to own the device.
Attack on HVAC systems	HVAC (Heating, ventilation, and air conditioning) system vulnerabilities are exploited by attackers to steal information such as user credentials.
Jamming Attack	The attacker jams the signal between the sender and the receiver with malicious traffic.

Man in the Middle Attack	An attacker pretends to be a legitimate sender who intercepts all the communication between the sender and the receiver and hijacks the communication.

The Open Web Application Security Project (OWASP) top 10 is a document that lists the most critical vulnerabilities to a project. This document lists the top ten vulnerabilities in mobile applications, web applications, IoT devices, etc. It is a globally recognized document that serves as a guideline towards secure coding.

Table 2: OWASP Top 10 Vulnerabilities in IoT

Vulnerabilities	Description
Weak, guessable, or hard coded passwords	Many IoT devices come with weak default passwords which can be easily guessed or broken. Users often do not change these default passwords or are not given the option to change them.
Insecure network services	Unneeded or insecure network services running on the device itself, especially those exposed to the internet, which can compromise the CIA (confidentiality, integrity or, availability) triad of information.
Insecure ecosystem interfaces	An IoT device can be accessed via the internet, thus raising attack vectors in the web, cloud, or mobile interfaces outside of the device ecosystem.
Lack of secure update mechanism	IoT devices are smaller, use less power, and last longer. This increases the difficulty to update their software. Problems like lack of firmware validation on a device, lack of secure delivery, etc. are also present.
Use of insecure or outdated components	IoT devices have a long shelf life and thus can easily get outdated and become more vulnerable as time goes on.
Insufficient privacy protection	An IoT device and its ecosystem may contain a lot of personal data. It can be used insecurely, improperly, or without permission.
Insecure data transfer and storage	It's not easy to encrypt data with the IoT device's lack of computing power. Simple sniffing techniques may be used to capture data.
Lack of device management	The maintenance of IoT devices after deployment is lacking. This includes update management, asset management, system monitoring, etc.
Insecure default settings	Less secure default settings make IoT devices more user friendly but more vulnerable. They also restrict the user's ability to modify those to avoid adding those functions.
Lack of physical hardening	Physical access to IoT devices can introduce risks. Attacks can be used to harm the devices or extract information from them.

Recent IoT Hacks

There are currently billions of IoT devices. But how many of them are secure. IoT devices connect to the internet using our home or enterprise networks. If they are compromised, our whole network may also be compromised. At the same time, it is true that no device is 100% secure, but there are still minimum requirements for security that must be fulfilled. Due to many reasons, not many IoT devices have been able to provide a satisfactory security mechanism. There have been numerous IoT hacks in recent years due to a lack of security implementations in IoT devices. Some of these recent hacks are discussed below:

Somebody's Watching: Hackers Breach Ring Home Security Cameras - A couple installed a ring camera in their children's room for security purposes was hacked on December 4, 2019. After four days of installing the camera, the speaker started piping the song "Tiptoe Through the Tulips." When the couple's 8-year-old daughter checked on the music, a man claiming to be Santa Claus spoke to her, which terrified them. There have been at least three similar cases reported that month - the others were in Connecticut, Florida, and Georgia. Other breaches, involving Google's Nest (smart home device) and Taococo (smart home security camera), a baby monitor sold on Amazon, have also drawn scrutiny and prompted concerns about privacy.

Tesla cars tricked into autonomously accelerating up to 85 MPH in a 35 MPH zone while cruising control using just a two-inch strip of electrical tape - Security researchers at McAfee have tricked the 2016 Tesla Model X and Model S into speeding with just a 2-inch strip of black tape. The researchers could fool the Mobileye EyeQ3 camera to read wrong information and feed bad information to the vehicles. Adding the 2-inch black tape to the sign with a speed limit of 35 MPH caused the camera to read it as 85 MPH. The vehicle started accelerating autonomously and was stopped at 50 MPH by researchers for safety. Though it is an adversarial attack that could have fooled even humans, it still shows how much more security is required.

Countermeasures

IoT devices require a "security by design" approach, which will minimize the vulnerable coding errors and flaws. To achieve this, developers must follow some guidelines. The following are some guidelines that have been developed by some organizations to promote IoT security:

- Groupe Spéciale Mobile Association (GSMA) "GSMA IoT Security Guidelines & Assessment"
- IoT Security Foundation "Secure Design Best Practice Guides"
- The Cloud Security Alliance's "Future Proofing the Connected World: 13 Step to Developing Secure IoT Products"

Table 3: OWASP Vulnerabilities and their Countermeasures

Vulnerability	Countermeasure
Weak, guessable, orhardcoded passwords	Enable default credentials to be changed and conduct periodic assessment of web application. Enable two-factor authentication and lockout mechanisms.
Insecure network services	Close open ports, disable unwanted services, and review network services vulnerabilities.
Insecure ecosystem interfaces	Conduct an assessment of all interfaces and use strong and complex passwords with two-factor authentication.
Lack of secure update mechanism	Secure update servers. Encrypt the updates and verify using signed updates.
Use of insecure or outdated components	Use the latest components and check their vulnerabilities and provide patches.
Insufficient privacy protection	Minimize data collection and provide end-users the ability to decide what data is collected.
Insecure data transfer and storage	Maintain SSL/TSL encryption and store data in an encrypted format.
Lack of device management	Provide simple device management manuals to users and provide stable updates to devices.
Insecure default settings	Allow users to change such settings and customize the device to a degree. Use strong and secure default settings.
Lack of physical hardening	Minimize external ports like USB ports. Include the ability to limit administrative privileges.

Using IoT security tools help organizations to vastly limit security vulnerabilities, thereby protecting the IoT devices and networks from different kinds of attacks. They provide security via all the phases of development and deployment.

Table 4: IoT Security Tools

Security Tools	Description
Bitdefender BOX	Provides malware, antivirus, network intrusion protection for all web-connected devices.
SeaCat.io	SeaCat.io is a security-first SaaS technology to operate IoT products in a reliable, scalable, and secure manner.
DigiCertIoT Security Solution	DigiCert IoT Device Manager gives the user total visibility and control over every connected device in their ecosystem.
Google Cloud IoT	Google Cloud IoT is a tool that provides many features like collecting and analyzing data, secure connection, and management.

Cisco IoT	Cisco IoT helps in protecting the deployment of IoT devices. Users get more visibility and control over the network.
Blackberry Secure Software Services	BlackBerry provides users with software and services like endpoint management, endpoint protection, and secure communication.
Darktrace	Darktrace uses AI to learn and respond to newer attacks. It provides faster responses to attacks.
Subex	Subexspecializes in identifying, assessing, categorizing, and mitigating existing and emerging threats.
AWS IoT Device Defender	AWS IoT Device Defender is a tool that helps to maintain and enforce IoT configurations like authorization and encryption.
Zing Box	Zingbox is AI-powered and combined with shared knowledge of millions of IoT devices, it enables the user to identify never before seen threats on the network.

End Sections

Future Efforts

IoT has limitless capabilities, as these devices are versatile and can be used in any industry. But these devices come with their security implications. Before using these devices in any critical capacity like medical, military, or airports, they must be secured to prevent security breaches. Efforts to resolve the security risks will develop more robust standards and technologies specific to IoT. These standards and technologies will help in making better and more secure IoT devices. IoT security can be improved through certain practices like applying encryptions to all data whether at transit or rest; using new technologies like Artificial Intelligence to predict future threats and fake accounts or pages; allowing only trusted networks to connect to the device; asking users to change their passwords at regular intervals, and only allowing strong passwords; minimize data collection; based on the device's usage and user, vendors must provide adequate security measures, they may also make a security declaration by having their system tested at the Evaluation Assurance Level (Levels 1-7); training developers to use "secure by design" approach, and implementing a security testing phase in the development cycle to check for security issues. Applying these strategies will result in safer IoT devices.

Conclusion

The growth in the number of IoT devices has been tremendous; however, to fully utilize these devices, strong security measures are required. These devices currently provide limited protection, which is a cause for major concern. It should be taken into account when building modern devices. Despite many attacks on IoT devices, there has been no significant improvement in their security. While it is true that no device is 100% secure, but there are still minimum requirements for security that must be fulfilled. Given the wide scope of IoT, there is no single solution that defines security for IoT. Designers need to identify the security requirements relevant to their products in the context of the design goals, the environment in which the product will be deployed, and regulatory obligations that might apply. IoT devices are built to last long; as small devices, they operate autonomously for long periods while consuming little power. This long period ensures that the devices will become more vulnerable as time goes on. Thus, it is important to provide timely updates and security patches to keep such devices secure over longer periods. To ensure that society reaps the appropriate benefit from IoT devices, security elements such as confidentiality, integrity, availability, authenticity, global policies, and standards must be achieved.

References

Best Practice Guides. IoT Security Foundation, 2019.

"Future Proofing the Connected World." *Cloud Security Alliance*, 2016.

"Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints will be in Use in 2020." *Gartner*, 2019.

GSMA IoT Security Guidelines and Assessment. Grou-peSpéciale Mobile Association.

Internet of Things Security Guideline. IoT Alliance Australia, 2017.

Li, Shancang, et al. "The Internet of Things: A Security Point of View." *Internet Research*, vol. 26, no. 2, 2016, pp. 337-359.

Liberatore, Stacy. "Tesla Cars tricked into Autonomously Accelerating up to 85 MPH in a 35 MPH Zone while in Cruise Control using just a Two-Inch Strip of Electrical Tape." *Daily Mail*, 2020.

"New Security Guidance for Early Adopters of the IoT." *Cloud Security Alliance*, 2015.

"OWASP Internet of Things Project." *Wiki OWASP*, https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

Palmer, Danny. "The Internet of Things? It's really a Giant Robot and we don't know how to fix it." *ZD Net*, 2017.

Strategic Principles for Securing the Internet of Things (IoT). U.S. Department of Homeland Security, 2016.

The Right Secure Hardware for Your IoT Deployment. Microsoft Corporation, 2017.

Vigdor, Neil. "Somebody's Watching: Hackers Breach Ring Home Security Cameras." *The New York Times*, 2019.

Vignesh, R., and A.Samydurai. "Security on Internet of Things (IOT) with Challenges and Countermeasures." *International Journal of Engineering Development and Research,* vol. 5, no. 1, 2017, pp. 417-423.

Author Details

Yash Choudhary, *Department of CSE, JECRC University, Sitapura, Rajasthan, India*

B. Umamaheswari, *Assistant Professor, Department of CSE, JECRC University, Sitapura, Rajasthan, India*

Dr. Vijeta Kumawat, *Associate Professor, Department of CSE, JECRC University, Sitapura, Rajasthan, India*