IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW: IoT THREATS AND CHALLENGES

[1]NIMISHA RAI, [2]SHAMAL SONAWANE AND [3]CHAITALITIKHE

[1]Assistant Professor

[1]Department of Electronics, Dr. D. Y. Patil ACS College, Pimpri, Pune, India

[2]Assistant Professor

[2]Department of Electronics, Dr. D. Y. Patil ACS College, Pimpri, Pune, India

[3]Assistant Professor

[3]Department of E and Tc, PimpriChinchwad Polytechnic Pune, India

Abstract: The next era of communication is IoT. The emergence and rapid growth of Internet of Things (IoT) focus on automating different task and trying to empower the physical objects to act without human interaction. The existing and upcoming IoT applications are highly promising to increase the level of comfort, efficiency, and automation for the users.IoT devices and application increase operational efficiency by enabling centralized monitoring and management of manufacturing equipment, critical infrastructure, or remote sites. However, IoT based systems and applications are vulnerable to various security threats and attacks which leads to other cyber security threats. Moreover, due to the lack of standardization due to heterogeneity of devices and technologies implementing security in IoT is real challenge. In this paper, detailed review of sources of threats in IoT and challenges in IoT and their solutions are presented**.**

Index Terms- IoT, IoT security, Threats, Security Solutions

I. INTRODUCTION

The Internet of Things (IoT) is a network of integrated bias, software, detectors, and other ‘effects’ which enable the world to be connected throughout physical space. This can include business software, smart home bias, care monitoring systems, mobile phones, or driverless exchanges, and can be as small as a thumb drive to the size of a train. All of these effects communicate with each other without the need for mortal commerce. This spider web of connectivity is fascinating but poses serious peril to information security.

The number of sectors enforcing IoT operation is on the increase, which means the number of IoT things and operations created will also increase. One similar sector is consumer IoT, which is introducing wearable technology with detectors to cover and transmit the extension and health data of a person. The healthcare assiduity is introducing IoT things and operations (4) similar as remote case monitoring, sanitarium operations, glucose monitoring, connected inhaler, connected contact lens, robotic surgery, effective medicine operation, cancer discovery, and stocked reality headsets and smart hail aids to their cases. “Smart Home” IoT things and operations (5) available on the request moment include smart door cinches, smart heating, smart gardening, videotape doorbells, particular sidekicks to smart bulbs, smart coffee machines, and smart refrigerators. The “Smart megacity” sector has created IoT Things and operations that are used in smart parking, smart road lights, and smart waste operation that are used in smart parking, smart road lights, and smart waste operations (6, 7). Companies leading the charge of introducing new operations for artificial IOT are Alibaba Cloud in cooperation with Siemens. They are working on industrial IoT operating systems (8). DHL is a logistics company, working on end-to-end IoT results and operation, monitoring and prophetic conservation (10).

The growing number of IoT devices available on the request is a suggestion of a successful IoT assiduity, but numerous of these things suffer from resource constraints. As a result, classical security results aren't applicable to numerous IoT devices and it's explosively needed to give the IoT devices with feather light security results. (17) Classifies security constraints as limitations grounded on tackle, software, and networking of IoT bias. Limitations grounded on tackle include computational, storehouse, power, and memory constraints. Limitations grounded on software include bedded software constraints. Limitation grounded on networking includes, mobility, scalability, slow intermittent network connections which is due to the perpetration of low power radios which results in low data rates.

II. RELATED WORKS

Hassija et.al. (18) Handed a detailed review of the security-related challenges and sources of trouble in the IOT operations. The paper gave detailed and realistic recommendations to ameliorate the IOT structure to grease author bandied how living and forthcoming technologies similar as block chain, fog computing, edge computing and machine literacy can be used to increase the position of security in IoT.

Also, Jurcut et.al. (19) Bandied the problems related to safety and security in IoT. This is done by relating general trouble and attack vectors against to a breach of security. Also, this paper presented some results to compromised bias along with styles for forestallment and security advancements to minimize pitfalls.

In (20) Mishraetal reviewed the elaboration of IOT, operations, and challenges of IoT. A layered perspective was used to punctuate the security issues faced in IOT. A comparison of anomaly discovery ways and the most recent Intrusion Discovery System (IDS) was employed to ameliorate IOT security.

Noor (21) presented information on recent exploration trends in IoT security from 2016-2018. This paper looked at applicable tools and simulators, outlined simulation tools, modelers, and computational and analysis platforms tools used by experimenters in the field of IoT security.

Kouicemet.al.(25) bandied the security benefits arising technologies similar block chain and software defined network(SDN) bring to IoT networks. The main security benefits of these two systems are inflexibility and scalability. The paper also looked at security conditions and challenges in different IoT operations. Security results are distributed as classical and new approaches.

In(26) Harbi et.al. Anatomized IoT security grounded on a taxonomy of security conditions that included data security, communication security, and device security. For a list of IoT operations that paper bandied the challenges and proposed security results.

III. IoT THREATS

IoT threats are the malicious thing that can cause the vuluenrabilites in the IoT devices and services. It affects the computer security, network security, information security etc. It is divided into two parts active and passive threats

3.1 Active Threats

In this attack attacker directly take the action against the system or the network. An attacker can make an attempt to destroy, modify or disturb the system or network. This type of attack affects the integrity and availability of a system or network. It will reduce the availability of system resources which will lead to significant damage and financial loss for the targeted organization.

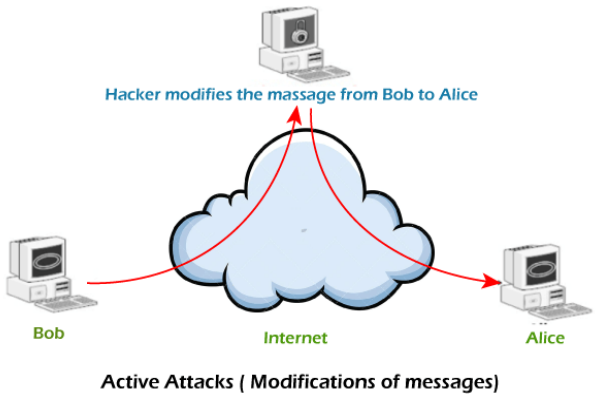

Fig.1.Active Threats

3.2 Types of Active Threats:

3.2.1 Masquerade:

Masquerade is a type of cybersecurity attack in which an attacker pretends to be legitimate user to gain access to systems or data. The attacker will get the permission to gain unauthorized access to confidential information or perform malicious actions.

There are several types of masquerade attacks

- **Username and password masquerade:** In a username and password masquerade attacker uses stolen or forged credentials to log into a system or application as a legitimate user.
- **IP address masquerade:** In an IP address masquerade attack, an attacker spoofs or forges their IP address to trick the people that they are accessing a system or application from a trusted source.
- **Website masquerade:** In a website masquerade attack, an attacker creates a fake official website in order to trick users into providing sensitive information or downloading malware.
- **Email masquerade:** In an email masquerade attack, an attacker sends an email that appears to be from a trusted source, such as a bank or government agency, in order to trick the recipient into providing sensitive information or downloading malware.

- **Modification of messages:**

In this attack part of message is modified, delayed or recorded to produce an unauthorized effect and affect the integrity of the original data. In this attack unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data.

3.2.2 Repudiation:

Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message. These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

There are several types of repudiation attacks, including:

- **Message repudiation attacks:** In a message repudiation attack, an attacker sends a message and then later denies having sent it. This can be done by using spoofed or falsified headers or by exploiting vulnerabilities in the messaging system.
- **Transaction repudiation attacks:** In a transaction repudiation attack, an attacker makes a transaction, such as a financial transaction, and then later denies having made it. This can be done by exploiting vulnerabilities in the transaction processing system or by using stolen or falsified credentials.
- **Data repudiation attacks:** In a data repudiation attack, an attacker modifies or deletes data and then later denies having done so. This can be done by exploiting vulnerabilities in the data storage system or by using stolen or falsified credentials.

3.2.3 Replay:

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

3.2.4 Denial of Service:

In Denial of Service (DoS) attack a system or network is made unavailable to its intended users by overwhelming it with traffic or requests. In a DoS attack, an attacker make an attempt to consume the target system or network resources, such as bandwidth, CPU cycles, or memory to prevent legitimate users from accessing it. It is done by flooding a target system or network with traffic or requests.

The several types of DoS attacks includes:

- **Flood attacks:** In a flood attack, an attacker sends a large number of packets or requests to a target system or network in order to overwhelm resources.
- **Amplification attacks:** In an amplification attack, an attacker uses a third-party system or network to amplify their attack traffic and direct it towards the target system or network, making the attack

more effective.

3.3 Passive Threats

In a Passive attack attacker makes an attempt to learn or make use of information from the system but does not affect system resources. In Passive Attacks, attacker is continuously monitoring or silently listening the messages during transmission. The goal of the opponent is to obtain information that is being transmitted. In Passive attacks an attacker is just monitoring or collecting data without altering or destroying it. In Passive attacks an attacker listens silently in on network traffic to collect sensitive information and in sniffing where an attacker captures and analyzes data packets to steal sensitive information.

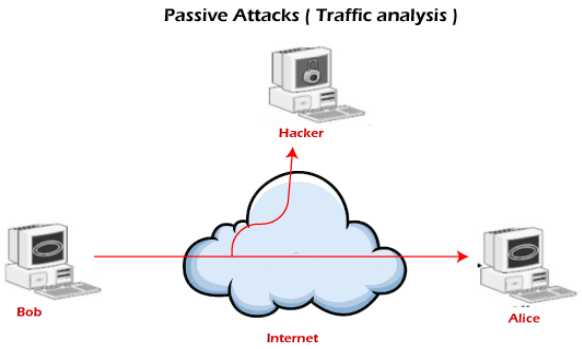

Fig.2. Passive Threats

3.4 Types of Passive Threats:

3.4.1 The release of message content:

Message can be transmitted through Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. An opponent should prevent it from learning the contents of these transmissions.

3.4.2 Traffic analysis:

When message is transmitted it is encrypted so that even if it is captured, an attacker could not extract any information from the message. But the attacker can determine the location and the identity of communicating host and could observe the frequency and length of messages being exchanged. By using this information an attacker could be able to guess the nature of the communication.

IV. CHALLENGES IN IOT

4.1 Lack of Standardization

Different IoT devices use different protocols and different platform. It becomes very difficult to ensure compatibility and interoperability between the devices. Different systems, products, or processes being incompatible with each other, leading to confusion, inefficiency, and decreased interoperability. This will increase the vulnerabilities that can be exploited by attackers.

Solution:

- Standard protocols and industry standards must be developed and adopted for IoT devices. Standard protocols and platforms ensures compatibility and interoperability.
- Certifying IoT devices and platforms ensures that they meet certain security standards. This can give organizations more confidence in the security of the devices they are using, and can also help identify devices that may be more susceptible to attack.
- Secure gateway ensures that all devices on the network are communicating securely. Secure gateway involves encrypting communications, authenticate devices, and monitor network traffic for suspicious activity. This will reduce the risk of attacks and increase the overall security of the network.

4.2 Weak or Non-Existent Authentication

IOT devices uses weak or non-existent authentication. They are designed with minimal security, making them vulnerable to attacks.

Solution:

- Strong authentication methods must be implemented, such as two-factor authentication which ensure that only authorized users can have access to the device.
- Secure gateway must be used which ensure that all devices on the network are communicating securely. Public Key Infrastructure (PKI) can ensure that all devices on the network are authentic.

4.3 Inadequate Software Security

IOT devices often run on embedded systems with limited resources so it is difficult to secure them. This could lead to vulnerabilities that can be exploited by attackers. Embedded systems have specialized hardware and software which creates additional challenges when it comes to securing them.

Solution:

- By implementing secure software to develop IoT app such as threat modelling and code reviews. By incorporating these practices into the development process, organizations can help to reduce the risk of attacks and increase the security of their IoT devices.
- The secure boot and secure firmware update processes ensures that the device is running trusted software. Secure firmware update processes ensure that the device is running with the latest version of the firmware. It ensures that updates are authentic and have not been tampered with.
- Secure gateway ensures that all devices on the network are communicating securely. A secure gateway acts as a central point of control for all devices on the network and it ensures that all devices are communicating securely. This will reduce the risk of attacks and increase the overall security of the network.

4.4 Insufficient Network Security

IoT devices mostly connected to unsecured networks using internet and makes them vulnerable to attacks. Due to unsecure network an attacker could intercept communications between an IoT device and potentially gaining access to sensitive data.

Solution:

- By Implementing secure network protocols, such as VPN and HTTPS, ensures that data is transmitted securely. Virtual Private Networks (VPNs) are used to encrypt communications between IoT devices and the internet, to make it more difficult for attackers to intercept data. HTTP'S are used to encrypt communications between web servers and clients, which provides an additional layer of security for web-enabled IoT devices.
- Secure gateway ensures that all devices on the network are communicating securely. A secure gateway is used to encrypt communications, authenticate devices, and monitor network traffic for suspicious activity. Hence it will reduce the risk of attacks and increase the overall IoT security of the network.
- Network segmentation can be implemented to limit the impact of an attack on the network. In Network segmentation a network is divided into smaller sub-networks, or segments, to limit the scope of an attack.

4.5 Limited Physical Security

IOT devices are small and easy to conceal and limited physical security makes them vulnerable to physical attacks. A physical attack on an IOT device involves tampering, theft, or destruction of the device. This could be resulted in unauthorized access to sensitive information, system downtime, and loss of data.

Solution:

- Physical security can be implemented by using such as locks and cameras to protect the device against physical attacks. Physical security includes tamper-proof enclosures of devices, security locks, and surveillance cameras to monitor the location of the devices.
- Tamper-evident packaging ensure that devices have not been tampered with before they reach their final destination. This can include using special packaging materials that are designed to show signs of tampering, such as seals that will break if the packaging is opened.
- Devices are protected against physical attacks by regularly reviewing the physical security of devices and updating the software to the latest version. This includes conducting regular physical

security audits, monitoring the device's location, and ensuring that all devices are updated with the latest security patches.

4.6 Inadequate Data Protection

An IOT device generate and collects a large amount of data which includes personal information, financial information, and other sensitive information, which make them vulnerable to attacks. If this data is not properly protected than it could be stolen and can be used for malicious purposes.

Solution:

- Data encryption must be implemented to ensure that devices must be protected against attacks and only authorized users have access to it. Secure encryption algorithms, such as AES or RSA, must be used to encrypt data at rest and in transit.

4.7 Limited Privacy Protections

IOT devices collect and transmit personal data hence it is important to protect users privacy. IOT devices includes data such as personal information, location data, and other sensitive information. This data must be properly protected otherwise it can be used for targeted advertising, identity theft, or other malicious purposes.

Solution:

- Privacy-enhancing technologies, such as anonymization and pseudonomization must be implemented. Anonymization is the process of removing personal identifiers from data and Pseudonomization is the process of replacing personal identifiers with pseudonyms, making it difficult to identify individuals. These technologies ensures that user's personal data is secured and not be used for malicious purposes.
- To have a clear and transparent privacy policies to inform users about how their data is being collected, stored, and used. This will help user to give ability to opt-out or delete their data. By regularly reviewing the security of devices and updating the software to the latest version will ensure that any privacy vulnerabilities are addressed. This includes conducting regular security audits, monitoring the device's location, and ensuring that all devices are updated with the latest security patches.

4.8 Inability to Update or Patch Devices

IOT devices are vulnerable to attacks since it is difficult or impossible to update or patch IOT devices. Once a vulnerability is discovered it cannot be fixed. Some devices are not supported by their manufacturers hence it is impossible to receive any security updates or patches. Due to lack of updateability and patch ability it is very difficult to protect IOT devices from known vulnerabilities and exploits, which makes them open to cyberattacks.

Solution:

- A secure gateway can be implemented to ensure security of IOT devices. A secure gateway acts as a central point of control for all devices on the network, and helps to monitor and control the communication between devices and makes them secure. This includes encryption and authentication to prevent unauthorized access to the network.
- Regularly reviewing and updating the software to the latest version ensures that devices are running the most recent version of the software, which includes security patches and updates. It is necessary to check the security settings of devices and configured them properly.

4.9 Limited Regulatory Oversight

The limited regulatory oversight of IoT devices makes it difficult to ensure that these devices are secure.

Solution:

- It is necessary to develop and enforce regulations for IoT devices. Governments and other regulatory bodies can develop and enforce regulations for IoT devices, which ensures that these devices are designed and manufactured to meet certain security standards. This includes requirements for encryption, authentication, and other security measures.
- Certifying IoT devices and platforms ensure that they meet certain security standards. This includes certifications for specific security features, such as encryption and authentication, as well as certifications for compliance with specific security standards, such as ISO 27001.

4.10 Lack of Visibility and Control

IoT devices are continuously operating in the background often without the user's knowledge or interaction. Hence it is very difficult to analyze their behavior and control their actions. For example IoT device such as a smart camera are sending the data to cloud without the user's knowledge. This lack of visibility into the device's behavior can make it difficult to detect and prevent malicious activity.

Solution:

- Developing tools to monitor and control IoT devices ensures that they are operating as intended by providing visibility into their behaviour. This include monitoring network traffic, identifying and blocking suspicious activity, and tracking device activity over time. These tools can control the actions of IoT devices, such as disabling specific features or shutting down devices that are behaving unexpectedly.
- Network segmentation can be used to limit the impact of an attack on the network by isolating IoT devices from the rest of the network. This includes creating separate networks for IoT devices and other devices, such as laptops and Smartphone's, and limiting the communication between these different networks. Network segmentation can be used to control the flow of traffic between different parts of the network, making it more difficult for an attacker to move laterally through the network.

V. CONCLUSION

In Conclusion, As IoT is beneficial but there are threats in IoT, some IoT threats are at low risk but there are few high impact threats that could cause serious damage. It involves accessing sensitive information stored on IoT devices such as personal information, financial information or even sensitive military information.

We have studied that in active attacks modification in information take place influences the service of the system and complexity is high where as in passive attacks modification in information does not take place and there is no harm to the system and complexity is low. IoT introduced many security challenges, these security challenges includes lack of standardization, device, data privacy concerns, network & software security. To address these challenges, an IoT app must be developed by a company who will implement robust security measures such as device authentication, encryption and regular software updates.

Additionally, IoT devices should be designed with security, and companies should have clear and transparent data privacy policy in place. By addressing these security challenges head-on, an IoT app development company with its reliable IoT app development services can ensure the safety and security of their devices and the data they collect and transmit.

References

[1] K. Ashton, "That 'Internet of Things' Thing," June 22, 2009. [Online].
Available: https://www.rfidjournal.com/that-internet- of-things-thing. [Accessed on Jul. 4, 2020].

[2] European Union Agency for Network and Information Security (ENSIA), "Baseline security recommendations for IoT," November 20, 2017. [Online].
Available: https://www.ensia.europa.eu/publications/baseline-security-recommendations-for-iot. [Accessed: Jul. 4, 2020].

[3] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (5) (2015) 164.

[4] M. Hasan, "IoT in healthcare: 20 examples That'll make you feel better," April 2, 2020. [Online].
Available: https://www.ubuntupit.com/iot-in-healthcare-20- examples-thatll-make-you-feel-better. [Accessed: Nov. 5, 2020].

[5] Lanner. "Examples of IoT devices in your next smart home," September 10, 2018. [Online].
Available:https://www.lanner- america.com/blog/5-examples-iotdevices-next-smart-home. [Accessed: October 10, 2020].

[6] A. Grizhnevich, "IoT for smart cities: use cases and implementation strategies," May 3, 2018. [Online].
Available: https://www.scnsoft.com./blog/iot-forsmart-city-use-cases-approaches-outcomes. [Accessed: Oct. 10, 2020].

[7] S. Chaudhary; R. Johari, R. Bhatia, K. Gupta and A. Bhatnagar, Craiot: concept, review, and application(s) of IoT. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019.

[8] Alibaba, "Siemens and Alibaba cloud partner to power industrial Internet of Things in China," [Online].
Available: https://www.alibabagroup.com/en/news/ press_pdf/p180709.pdf. [Accessed: Oct. 11, 2020].

[9] DHL, "Internet of Things," [Online].

Available: https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/internet-ofthings-in- logistics.html. [Accessed: Oct. 12,2020].
[10] Konux, "Transform railway operations for a sustainable future," [Online]. Available: https://www.konux.com. [Accessed: Oct. 12, 2020].
[11] Nexiot. [Online]. Available: https://nexxiot.com. [Accessed: Oct. 12, 2020].
[12] Scandit. [Online]. Available: https://www.scandit.com. [Accessed: Oct. 14, 2020].
[13] Apple. [Online]. Available: https://www.apple.com. [Accessed: Oct. 14, 2020].
[14] Cognigy. [Online]. Available: https://www.cognigy.com. [Accessed: Oct. 14, 2020].
[15] Huawei. [Online]. Available: https://www.huawei.com/us. [Accessed: Oct. 17, 2020].
[16] Samsung Electronics, "Samsung electronics to jointly build SKT World-First nationwide LoRaWAN network dedicated to IoT," [Online].Available:https://www.samsung.com/global/business/networks/insights/press-release/samsung-electronics-to-jointly-build-skt-world-first-nationwide-lora-wan-networkdedicated-to-iot. [Accessed: Nov. 4, 2020].
[17] M.M. Hossain, M. Fotouhi, R. Hasan, Towards an analysis of security issues, challenges, and open problems in the Internet of Things, 2015 IEEE World Congress Serv. (2015) 21–28.
[18] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.
[19] A. Jurcut, T. Niculcea, P. Ranaweera, et al., Security considerations for internet of things: a survey, SN Comput. Sci 1 (2020) 193.
[20] N. Mishra, S. Pandya, Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review, IEEE Access 9 (2021) 59353–59377.
[21] M. Noor, W. Hassan, Current research on Internet of Things (IoT) security: a survey, Elsevier: Computer Netw. 148 (2019) 283–294. P. Williams et al. Internet of Things 19 (2022) 100564 21
[22] H. HaddadPajouh, A. Dehghantanha, R. Parizi, M. Aledhari, H. Karimipour, A survey on internet of things security: requirements, challenges, and solutions, Elsevier: Internet of Things 14 (2021).
[23] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for Internet of Things (IoT) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685.
[24] S. Zaman, et al., Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey, IEEE Access 9 (2021) 94668–94690.
[25] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of Things security: a top-down survey, Comput. Netw. 141 (Aug. 2018) 199–221.
[26] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, A. Refou, A review of security in Internet of Things, Wirel. Pers. Commun. 108 (1) (Sep. 2019) 325–344.
[27] S.A. Hamad, Q.Z. Sheng, W.E. Zhang, S. Nepal, Realizing an internet of secure things: A survey on issues and enabling technologies, IEEE Commun. Surveys Tuts. 22 (2) (2020) 1372–1391, 2nd Quart.