Information Security Management in Internet of Things

line 1: Deepak Gowda Nilavadi Rajamudi
line 2: MSc Computer Science
line 3: *Manchester Metropolitan University*
line 4: Manchester, United Kingdom
line 5: 23703617@stu.mmu.ac.uk

***Abstract*—Internet of Things is an emerging technology that makes lives simpler, but it has become vulnerable to cyber-attacks & threats, and it's possible to mitigate the risks by applying certain policies, procedures & strategies. This paper classifies into four main categories 1) Information Security Threat and Attack Landscape 2) Risk Management and Audits 3) Security Culture and 4) Technical Security Controls. The paper is mainly focused on identifying threats and attacks and protecting assets by applying risk management strategy, plan, and policies. It has also discussed about implementing security culture for IoT. Furthermore, developed the most efficient mechanisms to secure information assets.**

Keywords—Internet of Things, Information security threat & attack landscape, risk management audit, security culture, technical security control.

I. INTRODUCTION

Internet of things is a recent technological trend it's about connecting objects to internet that can send & receive data. In this report, initially I have discussed about Information security threat and attack landscape, in this concept I reviewed the current information security threats such as data breach, Denial-of-service attacks, Physical attacks, Man-in-the-middle attacks, Sybil attacks, DDoS attacks, Wormhole attacks and Eavesdropping attacks in Internet of Things. Further I have discussed about identifying the assets and analyzing vulnerabilities & threats, I have performed risk management strategy that includes policies, procedures & controls to overcome the risks and secure the information assets in IoT and protect them from threats and attacks. Furthermore, I proposed a strategic information security culture for IoT technology and how it should be consistent with traits and challenges, also implemented plan and policies required for security culture. In the end, I reviewed about technical security control in IoT and recommended the most effective protection mechanisms such as AES, RSA, ECC, SHA-256, and Camellia that secures the assets against threats and attacks.

II. SECURITY THREAT AND ATTACK LANDSCAPE

IoT technology has been widespread and integrated because of this, the complexity of security threats are rising and threats like these cause many risks to the security of information and data within IoT systems. Therefore, to mitigate these problems it's important to execute vigorous security measures for the software and programs on IoT devices.

1)Data breach: Addressing fundamental security requirements at the application level is important to prevent unauthorized access, and information leakage in IoT devices, organizations can protect their data by giving importance to the security requirements.[1]

2)Denial-of-Service attacks: Attackers can launch DoS attacks to disrupt IoT services and make devices unavailable to legitimate users. This attack can disrupt the availability of IoT systems by overwhelming them with a high volume of traffic and unable to perform their functions.

3)Physical attacks: Sometimes IoT devices are vulnerable to a range of physical attacks that can settle their functionality and security, it is important to protect IoT devices against threats like physical tampering, malware infections, and also man-in-the-middle attacks to make sure the overall security of the IoT ecosystem.[2]

4)Man-in-the-Middle attacks: Attackers intercept communication between two parties without their knowledge, they can manipulate the data being exchanged. They may use techniques like ARP spoofing, DNS spoofing, or SSL stripping to perform the attack. Attackers can steal important data, login credentials, financial information and personal data. They manipulate the data to do fraudulent activities, and gain unauthorized access to systems.

5)Sybil attacks: It is a type of security threat in which a single node creates multiple fake identities to deceive a network, by creating fake identities they manipulate the network and interrupt communication. Due to sybil attacks, it reduces the efficacy of fault tolerance schemes therefore it causes a major threat to geographic routing protocols.[3]

6)DDoS attacks: DDoS attacks can target fragility in networked devices such as PCs servers, and IoT devices in this system. Attackers gain access to these devices to perform coordinated DDoS attacks and because of this, services' availability would be impacted.[4]

7)Wormhole attacks: In wormhole attack two remote areas of network are connected by a malicious node that builds a tunnel or in other words it's called out of band fast transmission link. Through the use of wormhole, the attackers transfers data packets that are intercepted at one point in the network to other malicious node that is present in different area of the network. The impacts of wormhole attacks are**:**

a)Challenge in detecting: Malicious nodes exploit quick transmission paths that's why it's difficult to detect the attacks.

b)Degradation of performance: Wormhole attacks impact the performance of services like data fusion, time synchronization by delaying and inconsistencies in data transmission.

8)Eavesdropping attacks: In eavesdropping attacks, unauthorized communication between network nodes is intercepted which is to enable attackers to get private information without the parties knowing about it. Wireless devices and networks such as IoT devices and WSNs are specifically vulnerable to eavesdropping attacks because of their wireless communication.[5]

III. RISK MANAGEMENT AND AUDITS

a) Assets that need to be protected and impact of threats

Assets to be protected	Threats and Vulnerabilities	Potential impacts of threats & vulnerabilities on IoT
Data	Attackers gain unauthorized access to sensitive data which may leak sensitive information or get manipulated.	• Financial losses. • Damage to reputation. • Legal consequences. • Data loss.
Network Infrastructure	Issues such as data interception, unauthorized access and network disruptions are caused by attackers. Therefore, network infrastructure like routers, switches, firewalls, and servers have to be protected.	• Interruptions to services. • Unauthorized access. • Segmenting a network. • Exhaustion of resources.
Physical Infrastructure	Access to IoT devices, data centers and servers can result in theft, tampering, and unauthorized access.	• Critical services are disrupted, such as malware infections and software exploits. • Damage of infrastructure such as data manipulation and backdoor access. • Hardware vulnerabilities such as malfunction of device and risks to safety.
Firmware and Software	IoT devices may include firmware and software vulnerabilities that attackers might use to escalate privileges, gain unauthorized access or execute arbitrary code.	• Ransomware and Malware can disrupt firmware and software operations. • Unsecured authorization and authentication. • Devices become worthless or bricked when vulnerabilities in firmware and software are exploited.

b) RISK MANAGEMENT STRATEGY:

Policies	• To prevent unauthorized access to IoT devices and networks, it’s important to implement strong authentication and access control policies. • It’s necessary to develop and execute explicit policies that will prioritize data integrity, authentication. • By educating about security awareness training to administrators and users about security protocols. • To develop strong IoT security policies that outlines data encryption, response protocols and security criteria.
Procedures	• To establish procedures for secure data transfer so that data is not changed during transfer. • To address and recognize cyber threats its necessary to setup protocols to monitor network infrastructure. • Incident response should be established to quickly detect and address attacks on IoT devices and systems. • Performing penetration tests and security assessments on IoT devices and networks which can find and address vulnerabilities.
Controls	• To establish security solutions by addressing technological heterogeneity and resource utilization to upgrade IoT security. • To promote sustainable growth and enhance security it’s good to utilize authentication codes and IoT protocols. • Keeping track on IoT networks for doubtful activities and blocking harmful traffic. • To have safe data transmission between IoT servers and devices it’s important to deploy encryption protocols like SSL/TLS.

c) Implementation of risk management strategy

Stakeholders and their responsibilities	Responsibilities and mitigation strategies	Range of resources needed for risk management.
• Risk management team, such as cybersecurity experts, and managers.	• Conduct risk assessments, meetings, create guidelines, protocols and monitor risk reduction measures.	• Tools and technologies for security.
• Executives, and board members.	• They provide resources, offer strategic direction, supporting the risk management strategy.	• Financial and human resources
• IT professionals	• They are in charge of setting up and maintain security actions like firewalls, encryption methods, intrusion detecting systems.	• Advisory and consultation services.
• Legal and compliance team	• They provide advice on liability concerns, regulatory requirements and contractual duties, they conduct privacy implication assessments.	• Investing in legal and regulatory resources.
• Operations and maintenance department	• Their responsibility is to manage and maintain IoT devices, networks and sensors daily. They have to respond to operational problems or security breaches and keep track of system performance.	• To mitigate risks it's important to invest in incident response tools and technologies.

d. Cyber threats and attacks are constantly evolving, so here is the risk management plan that would handle this periodic change.

- **Integration of threat Intelligence:** Threat intelligence feeds, security alerts, and industry studies can offer important insights into the most recent cyber threats, attack patterns, and developing attack vectors that target IoT devices and infrastructure when incorporated into the risk management plan. Organizations can improve their situational awareness and modify their security procedures to efficiently handle developing dangers by utilizing threat intelligence sources.

- **Planning based on scenarios:** Creating scenarios based on possible assaults and cyber threats that might affect the company. To evaluate reaction plans and pinpoint areas for development, do simulations and tabletop exercises. By planning for many eventualities, the company can react to real-world incidents more skilfully.

- **Educating and training employees:** To improve the human element in risk management, organizations might fund cybersecurity awareness campaigns, training courses, and skill-building projects for staff members, stakeholders, and outside suppliers. Employees can be better equipped to identify and proactively address changing cyber risks by receiving training on cybersecurity best practices, incident response protocols, and emerging threats.

- **Constant evaluation of Risk:** Continuous risk assessment procedures to find, examine, and assess new cyber threats and vulnerabilities in Internet of Things systems should be part of a proactive risk management strategy. Organizations may stay updated about emerging threats and evaluate their potential impact on network and physical infrastructure by conducting regular security assessments, penetration tests, threat intelligence monitoring, and vulnerability scanning.

- **Active security protocols:** By using proactive security techniques to identify and neutralize new threats as soon as possible, such as anomaly detection algorithms, behavioural analytics, and intrusion detection systems, and by making use of machine learning and predictive analytics to detect possible security risks and to see future attack patterns in IoT environments.

e. Now, here is the contingency plan that outlines the steps to be taken in the event of a cyber-attack.

1. **Immediate detection:**
   - To spot indicators of a cyber-attack which is against IoT devices, and utilize intrusion detection systems, security monitoring tools, and anomaly detection procedures.
   - To prevent further attack impacted systems should be immediately disconnected and isolated from the network.

2. **Limitation and Mitigation:**

   - By creating a containment plan to stop the attack's advancement and decrease additional harm. This could entail resetting compromised passwords, applying security patches or upgrades, and putting in place temporary workarounds.
   - In order to mitigate the impact of the attack on key infrastructure, it's necessary to temporarily implement security controls, network segmentation, or access limitations.

3. **Investigating and interpreting:**

   - Investigating the extent, type, and effects of the cyber-attack on IoT systems and infrastructure by conducting a comprehensive investigation.
   - To aid with the investigation and analysis process, it's necessary to consult with incident response consultants, digital forensics specialists, or cybersecurity experts.

4. **Improvements:**

   - Analyse the incident after it has happened to determine how well the company handled the cyberattack, where security procedures were lacking, and what lessons could be used to move forward.
   - Conducting security awareness training, patch management, and frequent security audits and assessments into practice as preventive steps to fortify defences.

5. **Restoring and recovering loss:**

   - To recover from data loss, infrastructure damage or service disruptions it's important to implement data backups, system restoration techniques and recovery methods.
   - To determine what areas need improvement and to estimate how well the recovery operations worked, test the recovered systems, verify the security procedures, and perform post incident reviews.

IV. SECURITY CULTURE.

- When proposing a strategic information security culture for IoT technology, it's important to carry out a complete study to determine the relevant strategies. So, this requires careful analysis of current frameworks, industry practices, and new developments in Internet of Things security trends. The proposed culture should be consistent with the special traits and challenges of IoT systems, which are a huge number of linked devices, levels of computational power and number of communicational protocols.

A. Forming a strategic information security culture for IoT technology:

   - Due to its wide range of devices, IoT technology has unique risks and vulnerabilities. To determine which strategic information security culture is most relevant to IoT it's required to do extensive research.
   - Analyzing current frameworks: Resolve well-known frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and IoT-specific standards to decide their suitability and efficacy.
   - Analyzing the threat environment: By analyzing the possible threats and weaknesses that are unique to the IoT such as data breaches, illegal access, and device tampering.
   - Gaining knowledge and understanding of IoT ecosystem: It's necessary to gain insights of how complexity of IoT ecosystems also including protocols, networks, and data flows.
   - Analyzing industry practices: By studying the case studies and best methods that are adopted by top IoT organizations that are implemented to mitigate security risks and foster an information security culture.

Justifying the proposal with reasons and evidence:

- Evaluating the risks: By conducting an assessment to resolve the consequences of the security events, control mechanisms, and critical assets.
- By keeping up with the emerging technologies that improves IoT security posture such as cryptography, artificial intelligence, blockchain.
- Analyzing user behaviour: By analyzing user attitudes and behaviour on the IoT environment to adjust the strategic culture accordingly.
- We should be considering GDPR, HIPAA and industry specific regulations to make sure compliance with legal and regulatory frameworks.

B. Suggestions on how to enforce the proposed strategic information security culture:

- Requirements for security vendors: One of the requirements is to make IoT vendors and suppliers to follow the security rules like regular security checks, safe development practices and policies for vulnerabilities disclosure.
- Standards for encrypting data: By setting encryption standards for data that is sent and which is stored to safeguard private information from being disclosed and interception.
- Policies for controlling access: By using the idea of least privilege it's important to make clear access control policies that govern device authentication, and who are allowed to access data.

- Developing response plan: This can be achieved by developing a response plan that has procedures detecting attacks, responding to it, and recovering.

C. Implementing and managing the policies:

- Designing a security roadmap: To develop security roadmap to help implementing and management of the suggested policies and roadmap should have resources and timelines to implement.
- To setup a security team: The security team should consist of IoT security experts, incident response team.
- Implement, monitor, and evaluate the policies: The team should be trained on the new policies and those policies should be implemented, along with these regular audits should be conducted, and the implementation of these polices should be monitored on daily basis.
- Improving the security culture: Establishing improvement in security culture by updating security policies, conducting regular audits, training the employees, metrics analysis.

V. TECHNICAL SECURITY CONTROL

A.

- Advanced Encryption standard (AES): AES is a symmetric method which is commonly used to protect data or information in many applications including IoT devices, and also provides decent balance of performance and security.[6]
- Rivest Shamir Adleman (RSA): It plays an important role in ensuring data integrity and securing communication in IoT networks. RSA is an asymmetric encryption method which is used for digital signatures and key exchange.[6]
- Elliptic Curve Cryptography (ECC): This is one of the cryptographic algorithms that is well suited for IoT devices that are resource constrained. This is another asymmetric encryption algorithm it is known for its efficiency in computing resource and key size resource.
- Secure Hash Algorithm 256(SHA-256): This is another cryptographic hash algorithm, and it is used for verifying data integrity and digital signatures. It ensures that data transmitted between IoT devices is not changed.[7]
- Camellia: Camellia is a symmetric encryption algorithm that requires strong robust encryption. This is designed to give efficiency, high security, and flexibility. It is also designed to be suitable for wide range of applications including IoT devices.[7]

B. Most effective controls that are currently used:

- Updates for firmware and secure boot: To prevent unauthorized changes to IoT devices and repair known vulnerabilities it's important to implement safe boot processes and ensuring firmware is updated with security patches.
- Identity of device management: To track, monitor, and control of devices in the IoT ecosystem is possible by giving unique identities to the IoT devices and securely managing these identities with the help of identity management system.
- Protocols to have secure communication: Datagram Transport Layer Security (DTLS) and Transport layer security (TLS) are protocols that create safe communication channels between backend servers and IoT devices, they are extremely effective in maintaining integrity and confidentiality of information.[8]
- Network segmentation: IoT networks can be segmented into separate zones with restriction rules that help in reducing the impact of hacked devices on the entire network.[8]
- Patch management and security updates: To mitigate risks and fixing vulnerabilities, regular security updates and patches are essential. Over-the-air (OTA) allows uninterrupted deployment of patches to IoT devices to make sure they are secured against evolving security threats.

C.

Updates for firmware and secure boot:

- <u>Strengths:</u> This helps to prevent unauthorized changes and directing known vulnerabilities through security updates. During the boot process, secure boot ensures only authenticated firmware is loaded.
- <u>Weakness:</u> If its updated are not maintained properly devices will stay vulnerable. The effectiveness of this control is dependent on convenient release and deployment of security repairs.
- <u>Impact:</u> It may have to face problems when failed to update firmware that leads to data loss, breaches, and reputational damage. Implementing properly will enhance device security.

Identity of device management:

- <u>Strengths:</u> It's efficient to track, monitor, and control devices with unique identities. Therefore, identity management systems help in safely managing these identities.
- <u>Weakness:</u> There might be problems such as misusing of sensitive data and unauthorized access of data if device Identities are compromised.
- <u>Impacts:</u> Failure in identity management causes customers to lose trust and data breaches. Efficient device identity management improves security and reduces risk of unauthorized access.

Protocols for secure communication:

- <u>Strengths:</u> Protocols like DTLS and TLS create safe communication channels that make sure confidentiality and integrity between backend servers and IoT devices.

- Weakness: DTLS and TLS protocols are generally and believed to be safe, but vulnerabilities do exist. Therefore, it is necessary to conduct regular updates and patches.
- Impacts: Unauthorized access, leakage of data and reputational damage are caused by breaches in communication security. Builds customer trust by implementing vigorous encryption protocols that ensures data and privacy is safe.

Network segmentation:

- Strengths: IoT devices are segmented into different zones with limited access that reduces the chances of potential attacks and minimizes impacts of hacked devices and allows precise monitoring and controlling.
- Weakness: Complicated networks face difficulties in managing efficient segmentation, it requires monitoring and planning.
- Impacts: Insufficient segmentation causes data leaks and network intrusions.

Patch management and security updates:

- Strengths: Vulnerabilities can be fixed, and device security can be improved by regular security updates and patches.
- Weakness: Incorrect or delay in patch management causes devices to the vulnerabilities and compatibility issues can be caused by OTA updates.
- Impact: If the patches are not applied it can cause security incidents, losing customer trust and data breaches. Organizations may face legal consequences if they fail to follow important security updates by resisting the regulatory standards.

D.

There are gaps in the current technical security controls that causes threats and attacks to the information assets.

- Defect in firmware and secure boot: To inject malicious code, attackers use vulnerabilities in firmware mechanisms and boot processes threatening the boot sequence's integrity.
- Identity management is insufficient: Unauthorized access to data and devices is caused by fragility in device identity management systems like storage of device identities is insecure and insufficient robust access controls.
- Implementation of secure communication protocols is not sufficient: When the implementation of secure communication protocols such as DTLS and TLS is not sufficient and has any vulnerabilities it's easy for attackers to manipulate data and intercept.
- Insufficient network segmentation: IoT devices are not isolated from the other network segments when they are not properly implemented. The hackers will be able to cross network boundaries and get access to sensitive resources.
- Delay in patch management and security updates: When the security patches are not applied on fixed schedule or if there is lack of patch management processes it might cause devices to be exposed to threats and attacks.

E.

The recommended mechanisms that are most effective to protect the information assets and align with the IoT's goals and objectives:

- Protecting firmware and boot procedures: Make sure firmware is safely updated, when the device turns on check if the firmware is genuine, and to stop unauthorized changes secure bootloaders have to be used.
- Identity of device management: Executing secure systems for device identities can be done by enhancing device identity management, applying robust authentication protocols, also monitoring, and auditing the device identity on regular basis.
- Encryption and secure protocols of communication: To build secure communication routes between cloud platforms, backend servers, and IoT devices it's recommended to use protocols like DTLS or TLS/SSL.
- Enhancing network segmentation: The best way to prevent flow of threats in IoT networks it's necessary to use network segmentation based on the least privilege principle. Also, by using technologies like network access control to apply segmentation rules and separating assets from devices that are less secure.
- Creating a strategy for patch management: By ensuring that security updates are executed in a timely manner over all IoT devices by implementing a centralized patch management system.

VI. CONCLUSION

In conclusion, Internet of Things is evolving rapidly and becoming advance, it is helping organisations and users for their business, but due to number of connections to devices and sharing of information is being a target for hackers to steal confidential and sensitive data. Therefore, this paper aims to analyse the information security threats and attacks in IoT devices and systems also discussed the necessity of robust security measures to mitigate those attacks and threats that cause problems to organisations, users etc. To secure the information assets in IoT and to safeguard from constantly evolving threats, risk management strategy has been implemented and measures to be taken during cyber-attacks have been discussed. Furthermore, discussed how managing and implementing security culture in Internet of Things can be formed such as designing a security roadmap, forming a security team & training them etc. In the end, discussed about what type of technical security controls are used to protect assets from threats and attacks including effective controls that are currently being used, also discussed the potential impacts of the controls on IoT devices and systems and gaps in these controls that exposes the assets to attacks, along with this the most effective protection mechanisms have been recommended to ensure the safety of information assets.

REFERENCES

1. Mishra, N. and S. Pandya, *Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review.* IEEE Access, 2021. **9**: p. 59353-59377.
2. Khanam, S., et al., *A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things.* IEEE Access, 2020. **8**: p. 219709-219743.
3. Murali, S. and A. Jamalipour, *A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things.* IEEE Internet of Things Journal, 2020. **7**(1): p. 379-388.
4. Doss, A.N., et al., *A Comprehensive Analysis of Internet of Things (IOT) in Enhancing Data Security for Better System Integrity - A Critical Analysis on the Security Attacks and Relevant Countermeasures*, in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. 2022. p. 165-167.
5. Butun, I., P. Osterberg, and H. Song, *Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures.* IEEE Communications Surveys & Tutorials, 2020. **22**(1): p. 616-644.
6. Rocha, V.D., et al., *Soft Error Reliability Assessment of Lightweight Cryptographic Algorithms for IoT Edge Devices*, in *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*. 2022. p. 457-460.
7. Regla, A.I. and E.D. Festijo, *Performance Analysis of Light-weight Cryptographic Algorithms for Internet of Things (IoT) Applications: A Systematic Review*, in *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*. 2022. p. 1-5.
8. Windarta, S., et al., *Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions.* IEEE Access, 2022. **10**: p. 82272-82294.