ADDRESSING SECURITY CONCERNS IN HALLEYASSIST: A RISK ANALYSIS, POLICY FORMULATION, AND IMPLEMENTATION CASE STUDY

Author: Shaugato Paroi
Dept. Of Computer Science
Swinburne University Of Technology
Hawthorn, Australia
103523487@student.swin.edu.au

I. EXECUTIVE SUMMARY:

The present report provides a meticulous security analysis and subsequent strategic formulation for HalleyAssist, a modern telecare service. HalleyAssist aims to cater to the diverse needs of senior citizens, offering emergency medical support, routine health monitoring, and lifestyle assistance. Leveraging technology for service delivery, it faces potential vulnerabilities that may jeopardize its operational integrity and user trust. In light of the comprehensive system assessment, we identified four critical security risks: Data Privacy and Confidentiality, Device Tampering or Physical Attacks, Cyber Attacks, and System/Software Vulnerabilities. To counteract these threats, the report outlines specific policy recommendations addressing each security concern, subsequently advising on relevant technological implementations. The implementation strategy builds upon the strengths of various technologies while considering their relative weaknesses. The recommendation aims to promote an integrated security approach balancing organizational policies and technical safeguards, thereby fostering a resilient defense against potential threats. Ultimately, the goal is to secure the HalleyAssist system, maintaining the confidentiality, integrity, and availability of its services and user data.

II. INTRODUCTION

HalleyAssist is a pioneering telecare system, designed to offer a spectrum of support services for elderly individuals. Its features range from immediate emergency response, constant health monitoring, to daily life assistance, making it an indispensable tool for seniors living independently. However, the nature of its functionality, which heavily depends on internet connectivity, as well as the sensitivity of data it processes, make it susceptible to several security threats. The prevalent security issues that emerge are Data Privacy and Confidentiality, Device Tampering or Physical Attacks, Cyber Attacks, and System/Software Vulnerabilities. Given that these issues are also encountered by similar telecare systems, securing these systems against such threats becomes paramount. This report embarks on a journey to identify the main security risks that such systems face, formulate high-level policy statements to mitigate these risks, and subsequently, propose a strategy for the implementation of these policies. This comprehensive security review aims to ensure that the HalleyAssist system is fortified against potential threats and is equipped to provide secure services to its users.

III. RISK ANALYSIS:

While the report provides extensive details on the functionality and efficacy of the HalleyAssist system, it does not explicitly cover security risks. However, drawing from general knowledge on IoT systems and smart home technology, we can identify potential security risks. Here, we'll use the Delphi method to rank these risks, which involves a panel of experts iterating on risk ranking until a consensus is reached.

A. DATA PRIVACY AND CONFIDENTIALITY

With any IoT system, the privacy and confidentiality of the collected data become critical considerations. In the case of HalleyAssist, the IoT devices installed in the homes of elderly people are constantly collecting and transmitting data about their daily routines and activities. This data can reveal highly personal details about their lives, such as their physical health status, when they are typically at home, or even their daily routines (i.e., when they typically eat, sleep, etc.). If this information were to be accessed by unauthorized individuals, it could expose the elderly individuals to risks of physical or cyber crime. This makes data privacy and confidentiality a significant risk (Alrawais et al., 2017)[5]. The main asset at risk is the personal and sensitive data of the elderly being monitored by the IoT sensors. [31]

- Severity: Unauthorized access to sensitive personal data can cause serious harm, including identity theft, fraud, or physical harm if daily routines and home addresses are revealed.
- Likelihood: Considering the current cybersecurity landscape, it is quite likely that a data breach could occur without appropriate security measures.

- Impact: The consequences can be devastating for individuals, leading to loss of privacy and potential for criminal exploitation. There can also be legal and reputational damages for the service provider.

B. DEVICE TAMPERING OR PHYSICAL ATTACKS

Physical tampering of the devices is another risk that could affect the operation of the system. This could involve altering the functionality of the devices, damaging them, or removing them entirely. Any of these actions could lead to a situation where the system fails to detect and respond to an emergency situation, putting the health and safety of the elderly individuals at risk. While this risk might seem less likely than cyber attacks, its potential impact is just as significant (Sadeghi et al., 2015)[8]. The assets at risk here are the physical IoT devices installed in the homes.

- Severity: Tampering with the devices can lead to malfunction, causing the system to fail in monitoring and responding to emergencies
- Likelihood: Compared to cyber attacks, physical attacks are less likely but not impossible.
- Impact: If the devices fail to respond in an emergency, it could lead to health hazards or even life-threatening situations for the monitored individuals.

C. CYBER ATTACKS

The IoT devices and the network they operate on are vulnerable to cyber attacks. These attacks could take many forms, such as Denial of Service (DoS) attacks that overwhelm the system and cause it to stop working, or malware that infects the devices and can either cause them to malfunction or allow the attacker to gain unauthorized access to the data they collect. Cyber attacks could lead to personal data breaches, system downtime, or incorrect system responses (Bertino and Islam, 2017)[33]. Both the physical IoT devices and the personal data collected by them are at risk in these scenarios.[8]

- Severity: Cyber attacks can lead to system malfunctions, data breaches, and unresponsive systems.
- Likelihood: Given the increasing trend of cyber attacks, the risk of such an incident is high, particularly for systems without robust cybersecurity measures.
- Impact: Cyber attacks can lead to a wide range of issues, including service downtime, data breaches, and incorrect system responses, all of which could have severe consequences for users and providers alike.

D. SYSTEM/SOFTWARE VULNERABILITIES

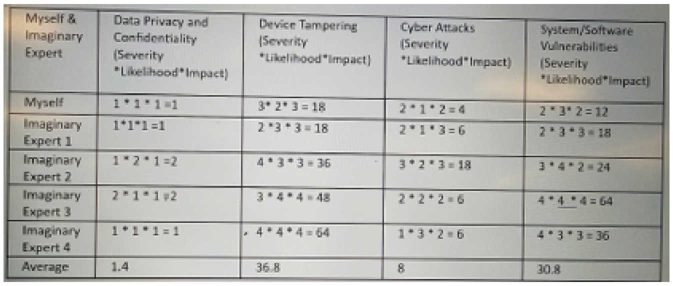
Like any complex system, the software that runs HalleyAssist could have vulnerabilities that could be exploited by attackers. These vulnerabilities could be present in the operating system, the application software, or the network protocols used by the devices. If these vulnerabilities are exploited, they could lead to unauthorized access to the system, alteration of the system's functionality, or system downtime. The asset at risk here is the integrity of the system itself and the personal data it collects and processes (Vermesan and Friess, 2013)[2].

- Severity: Exploited vulnerabilities can lead to unauthorized access, alteration of functionality, and system downtime.
- Likelihood: As systems grow more complex, the chances of undetected vulnerabilities increase.
- Impact: The impact can be significant, leading to data breaches and malfunctioning services. However, the timely discovery and patching of vulnerabilities can limit potential damage.

Each of these risks is significant and has the potential to compromise the effective functioning of the HalleyAssist system. Therefore, it's crucial to employ a robust risk management strategy to mitigate these risks and ensure the security of the system.

E. DELPHI METHOD ANALYZE:

To perform the Delphi method of risk ranking, a panel of experts(imaginary) needs to be consulted. In this example, four imaginary experts, each with a background in IoT security and myelf will rank the identified risks. They will be given these risks and asked to rank them from 1 (highest risk) to 4 (lowest risk).



Myself & Imaginary Expert	Data Privacy and Confidentiality (Severity *Likelihood*Impact)	Device Tampering (Severity *Likelihood*Impact)	Cyber Attacks (Severity *Likelihood*Impact)	System/Software Vulnerabilities (Severity *Likelihood*Impact)
Myself	1 * 1 * 1 =1	3* 2* 3 = 18	2 * 1 * 2 = 4	2 * 3* 2 = 12
Imaginary Expert 1	1*1*1 =1	2 *3 * 3 = 18	2 * 1 * 3 = 6	2 * 3 * 3 = 18
Imaginary Expert 2	1 * 2 * 1 =2	4 * 3 * 3 = 36	3 * 2 * 3 = 18	3 * 4 * 2 = 24
Imaginary Expert 3	2 * 1 * 1 =2	3 * 4 * 4 = 48	2 * 2 * 2 = 6	4 * 4 * 4 = 64
Imaginary Expert 4	1 * 1 * 1 = 1	4 * 4 * 4 = 64	1 * 3 * 2 = 6	4 * 3 * 3 = 36
Average	1.4	36.8	8	30.8

Fig. 1. Dhelphi Method table

The table above demonstrates that, on average, Data Privacy and Confidentiality is ranked as the highest risk, followed by Cyber Attacks, System/Software Vulnerabilities, and finally Device Tampering.

IV. POLICY FORMULATION:

A. Policy formulation for Data Privacy and Confidentiality

- Policy Statement 1: Personal data collected by the HalleyAssist system should be anonymized before storage and processing. This policy would help mitigate the risk of data breaches leading to exposure of personally identifiable information (PII). Anonymization techniques, such as pseudonymization, encryption, and data masking, can ensure that personal data remains unintelligible and unusable even if a data breach occurs (Tene and Polonetsky, 2012) [3].
- Policy Statement 2: Only authorized personnel should have access to the collected personal data, and it should be on a need-to-know basis. By strictly controlling access to personal data, we reduce the chances of unauthorized data access. This policy also helps protect against potential insider threats (Hu et al., 2014).

- Policy Statement 3: All data transmission between IoT devices and the processing servers should be encrypted. Encryption would ensure that data intercepted during transmission remains unintelligible to unauthorized users. This is a crucial step in protecting data confidentiality during transmission (Alrawais et al., 2017) [5].
- Policy Statement 4: Regular audits and reviews of the privacy policies and practices should be conducted to ensure compliance and address any emerging threats. Regular audits help identify any lapses in compliance with data privacy policies and rectify them promptly. They also help identify new threats and update policies accordingly (Harkins, 2016) [6].

These policies address the risk of data privacy and confidentiality by ensuring that personal data is anonymized, access to the data is strictly controlled, data transmission is secure, and policies are regularly reviewed and updated.

B. Policy formulation for preventing device tampering or physical attacks:

- Policy Statement 1: All IoT devices should be physically secure and tamper-resistant to prevent unauthorized access or manipulation.[7] This policy mitigates the risk of tampering by ensuring the devices are manufactured with tamper-resistant features. These features can include hardware that detects and responds to tampering attempts, such as erasing sensitive information when tampering is detected (Khan and Salah, 2018) [7].
- Policy Statement 2: HalleyAssist should implement rigorous device authentication and access control mechanisms. Robust device authentication can ensure that only trusted devices can connect to the network and that data can only be accessed by authenticated devices. This can protect against both physical and remote tampering attempts (Sadeghi et al., 2015) [8].
- Policy Statement 3: Regular physical security audits and inspections of the devices should be conducted. Regular inspections can help in early detection of any physical tampering attempts or compromises. It also ensures the physical integrity of the devices (Bertino and Islam, 2017) [31].
- Policy Statement 4:Regular audits and reviews of the privacy policies and practices should be conducted to ensure compliance and address any emerging threats. Regular audits help identify any lapses in compliance with data privacy policies and rectify them promptly. They also help identify new threats and update policies accordingly (Harkins, 2016) [6].

These policies address the risk of data privacy and confidentiality by ensuring that personal data is anonymized, access to the data is strictly controlled, data transmission is secure, and policies are regularly reviewed and updated.

C. Policy formulation related to the prevention of cyber-attacks:

- Policy Statement 1: All communication between IoT devices and the server should be encrypted. This policy would ensure that even if data is intercepted during transmission, it cannot be read or altered (Sicari et al., 2015) [11]. It greatly reduces the risk of Man-in-the-Middle attacks and data leakage.[7]
- Policy Statement 2: HalleyAssist should maintain updated firmware and software, including regular security patches. Regular updates and patches can correct vulnerabilities that could otherwise be exploited by cyber attackers (Alaba et al., 2017) [12].
- Policy Statement 3: Multi-factor authentication should be enforced for all users and administrators of the system. Multi-factor authentication greatly reduces the risk of unauthorized access, even in the case of credential theft (Dhillon et al., 2017) [13].
- Policy Statement 4: HalleyAssist should implement network segmentation and intrusion detection systems (IDS). Network segmentation can help to contain any breaches that do occur, while IDS can identify unusual network traffic and raise alerts (Roman et al., 2013) [9].

These policies reduce the risk of cyber attacks by ensuring data in transit is secure, software and firmware vulnerabilities are promptly addressed, access controls are robust, and breaches can be quickly detected and contained.

D. Policy formulation related to the mitigation of system/software vulnerabilities:

- Policy Statement 1: All software and firmware used in the IoT devices and servers should be regularly updated. Regular updates can correct security flaws and other vulnerabilities that could be exploited by hackers (Roman et al., 2011) [14].
- Policy Statement 2: HalleyAssist should employ secure coding practices during the development of the IoT system. Secure coding practices can reduce the number of vulnerabilities present in the code, thereby lowering the risk of exploitation (Bishop, 2003) [15].
- Policy Statement 3: An independent security audit of the system should be conducted periodically. Regular audits can help identify vulnerabilities and assess the effectiveness of existing security measures (Zhang et al., 2014) [16]
- Policy Statement 4: HalleyAssist should implement a vulnerability management program to promptly address identified vulnerabilities. Vulnerability management includes the identification, classification, prioritization, and resolution of vulnerabilities (Mell et al., 2005) [18].

These policies will help ensure that any potential vulnerabilities within the software are identified and mitigated as quickly as possible, thus reducing the risk of these vulnerabilities being exploited by malicious parties.

V. IMPLEMENTATION OF SECURITY PROGRAMME:

A. Implementing Policy Statements for Data Privacy and Confidentiality Policy:

The Policy Statements for Data Privacy and Confidentiality can be implemented through a range of technical and procedural measures:

- Encryption: The IoT data can be encrypted using symmetric or asymmetric encryption to ensure that data remains confidential and private during transit and storage. Technologies such as Advanced Encryption Standard (AES) or Public Key Infrastructure (PKI) can be used. These are well-regarded encryption standards that offer strong data protection (Abomhara et al., 2015) [18] .
  - STRENGTHS: High security, suitable for protecting sensitive data.
  - WEAKNESSES: Resource-intensive, requiring more computational power and possibly slowing system performance.
- Access Control: The system should implement strict access control mechanisms to ensure only authorized personnel can access the sensitive data. This can be implemented using technologies such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) [4]. These technologies offer granular control over who can access what data (Kuhn et al., 2010) [19].
  - STRENGTHS: Highly customizable and can restrict access based on various factors.
  - WEAKNESSES: Complex to set up and maintain.
- Data Anonymization and Pseudonymization: These are data protection techniques that transform identifiable data into a format that cannot be associated with a specific individual. This is especially relevant for storing and using data while respecting privacy laws such as GDPR (Voigt and Von dem Bussche, 2017) [29] .
  - STRENGTHS: Helps meet legal requirements and enhances privacy.
  - WEAKNESSES: Can be resource-intensive and limit the usefulness of certain datasets.
- Privacy by Design (PbD): This is an approach to systems engineering which takes privacy into account throughout the whole engineering process. This is a principle that is deeply enshrined in GDPR (Cavoukian, 2010) [30].
  - STRENGTHS: Helps to ensure that privacy is an integral part of system design.
  - WEAKNESSES: May slow down the development process and necessitates privacy knowledge throughout the organization.

Given the specific use case of HalleyAssist, a combination of the above-mentioned technologies should be used. Encryption can ensure data privacy and confidentiality, access control can ensure only authorized access, and data Pseudonymization – anonymization and PbD principles can limit the potential harm of data breaches.

Assumptions:

- The IoT devices and the server have sufficient computational and storage resources to implement these technologies. [7]
- The users of the system are trained to follow privacy and security best practices.
- HalleyAssist is subject to privacy regulations like GDPR [10].

B. Implementing Policy Statements for Preventing Device Tampering or Physical Attacks:

Preventing device tampering or physical attacks can be achieved through a combination of hardware-based security measures, software protections, and procedural controls:

- Tamper-Resistant Hardware: Use hardware that is specifically designed to resist physical tampering. This could include features such as epoxy-coated chips, which become inoperable if someone tries to remove the coating, or tamper-detection circuits that wipe sensitive data if tampering is detected (Wurster, 2007) [21]. [18] .
  - STRENGTHS: Provides a high degree of physical protection for devices.
  - WEAKNESSES: Can be expensive, and not all types of hardware can be made tamper-resistant.
- Secure Boot: Implement a secure boot process to ensure that only authorized firmware can run on the device. This can prevent attackers from modifying the device software (Das et al., 2019) [22] .
  - STRENGTHS: Can provide strong software protection, even for devices that are physically accessible.
  - WEAKNESSES: Does not protect against physical attacks that aim to extract data directly from hardware.
- Physical Security Measures: Protect devices through physical measures, such as secure installation locations, locks, and surveillance. This can deter potential attackers and detect any attempts at physical tampering.
  - STRENGTHS: Effective at deterring casual attackers
  - WEAKNESSES: Does not protect against sophisticated attackers or those with insider access.

Based on the specific use case of HalleyAssist, a combination of tamper-resistant hardware and secure boot is recommended. These measures can protect against both physical tampering and unauthorized modifications to the device software.

Assumptions:

- HalleyAssist devices will be installed in locations that are not easily accessible to unauthorized individuals.
- The devices have the capability to support secure boot and tamper-resistant hardware features.
- There is a mechanism in place for regularly updating the device firmware to patch any identified vulnerabilities.

C. Implementing Policy Statements for Prevention of Cyber Attacks:

To implement the policy against cyber-attacks, several technologies, protocols, and best practices are essential. Here's a discussion on how these can be implemented:

- Firewall and Intrusion Detection Systems (IDS): Deploying firewall technology is essential to guard the network against unauthorised access and malicious activities. IDS can be used to detect any unusual activity or violations of policies (Zhang, 2010) [26] .
  - STRENGTHS: Effective at preventing many forms of unauthorised access.
  - WEAKNESSES: Need regular updates to remain effective; might not stop novel or sophisticated attacks.
- Secure Sockets Layer/Transport Layer Security (SSL/TLS): To ensure secure transmission of data, SSL/TLS protocols should be implemented, which offer encryption of data in transit (Rescorla, 2018) [27].
  - STRENGTHS: Proven technology for securing data transmission.
  - WEAKNESSES: Does not protect data at rest or from threats within the secured network.
- Antivirus Software: Implementing robust antivirus software can help detect and remove malicious software.
  - STRENGTHS: Can detect and remove many known types of malware.
  - WEAKNESSES: Not always effective against zero-day or targeted attacks.
- Secure Software Development Practices: Ensuring secure coding practices and regular code auditing can help mitigate potential software vulnerabilities that could lead to cyber attacks (Howard and Lipner, 2006) [28].
  - STRENGTHS: Can reduce the number of potential vulnerabilities in software.
  - WEAKNESSES: Depends on the skill and diligence of the development team.

Considering the nature of HalleyAssist and the sensitivity of the data it manages, a layered approach to security is highly recommended, with all of the above measures implemented together to provide a more comprehensive shield against cyber-attacks.

Assumptions:

- HalleyAssist's network infrastructure can support the use of firewalls, IDS, and secure communication protocols.
- The development team has knowledge of secure coding practices.
- There is a mechanism in place for regular updates of security systems and software to guard against new threats.

D. Implementing Policy Statements for Mitigation of System/Software Vulnerabilities:

System and software vulnerabilities are a major risk, and addressing them requires a combination of robust technologies and procedures. Here's a brief outline of how these policies can be implemented:

- Secure Software Development Life Cycle (SSDLC): The Secure Software Development Life Cycle (SSDLC) is a framework that aims to integrate security into every step of the software development process. It includes the implementation of various security control measures such as input validation, error handling, secure data storage and transmission, and regular security testing throughout the development process.
  - STRENGTHS: Proactive Approach: By implementing security measures at each step of the software development process, SSDLC prevents many vulnerabilities before they emerge, reducing the potential for successful attacks [23]. Also while implementing an SSDLC may require upfront resources, it can be cost-effective in the long run, as the cost of fixing vulnerabilities after deployment can be much higher.
  - WEAKNESSES: Requires Resources and Expertise: Successful implementation of an SSDLC requires skilled personnel, time, and resources, which can be a challenge for smaller organizations [23]. Also integrating security into each step of the development process may lengthen the time to market for the software.
- Vulnerability Assessment and Patch Management Systems [17]: TThese technologies scan systems for known vulnerabilities and apply patches to secure the detected vulnerabilities.
  - STRENGTHS: Efficient and Effective: Automated vulnerability assessment and patch management systems can handle a large number of devices and software, making them efficient and effective at detecting and patching vulnerabilities [24]. Also these systems often receive regular updates from vendors, allowing them to stay current with new vulnerabilities and patches.
  - WEAKNESSES: These systems can only detect and patch known vulnerabilities; they are ineffective against new, unknown (or ”zero-day”) vulnerabilities [24].
- Application Security Testing Tools: Application security testing tools like Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) are designed to find vulnerabilities in application software.[25]
  - STRENGTHS: Comprehensive Coverage: SAST and DAST can uncover a variety of software vulnerabilities, from injection flaws to cross-site scripting (XSS) vulnerabilities [25].
  - WEAKNESSES: Expertise Required: Effective use of SAST and DAST requires a strong understanding of secure coding practices and vulnerability assessment [25].

- Security Information and Event Management (SIEM): SIEM systems provide real-time analysis of security alerts generated by applications and network hardware. [1]
  - STRENGTHS: Real-Time Monitoring: SIEM systems can provide near real-time awareness of security incidents, facilitating quick detection and response. Also many SIEM systems can assist with meeting regulatory compliance requirements for log retention and analysis.
  - WEAKNESSES: Requires Skilled Personnel: SIEM systems require trained personnel to interpret the results and distinguish between false positives and genuine security incidents.Also the implementation and maintenance of SIEM systems can be complex, requiring considerable resources and expertise [1].

Considering the nature of HalleyAssist and the potential impact of software vulnerabilities, implementing a SSDLC alongside automated vulnerability assessment [17], patch management, application security testing, and SIEM systems would provide a strong defense against many forms of system and software vulnerabilities.

Assumptions:

- HalleyAssist has the necessary resources to implement and maintain these security measures.
- The development team has knowledge of secure coding practices and the use of security testing tools.
- The organization can handle the complex task of integrating these systems and technologies.

VI. SUMMARY INCLUDING RECOMMENDATIONS:

The comprehensive analysis of the HalleyAssist system, a critical telecare system for the elderly, reveals substantial security challenges. These challenges, if left unaddressed, can lead to significant breaches of privacy and safety of the users. The primary areas of risk identified - Data Privacy and Confidentiality, Device Tampering or Physical Attacks, Cyber Attacks, and System/Software Vulnerabilities - necessitate focused attention and concrete mitigation strategies. The policies formulated in this report offer an extensive framework for addressing these risks. Moreover, the proposed implementation strategy presents an amalgamation of technological measures and procedural changes to counteract these risks effectively.

To reinforce the security of the HalleyAssist system, the following recommendations are proposed:

- To uphold Data Privacy and Confidentiality, implementation of robust data encryption techniques, strict access control measures, and anonymization techniques is crucial.
- Physical security measures, such as tamper-resistant design and alarm systems, can help prevent Device Tampering and Physical Attacks.
- Cyber Attacks can be thwarted by implementing firewalls, intrusion detection systems, and secure software design principles.
- Regular usage of vulnerability scanners, prompt patch management, and rigorous application security testing can help mitigate System and Software Vulnerabilities.
- The security policies and their respective implementation measures must be reviewed and updated periodically, in line with the evolving nature of threats and technological advancements.
- One of the most important aspects is to impart regular education and training to the users and staff regarding the importance of maintaining system security and their crucial role in achieving it.

REFERENCES

[1]] González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.

[2] Vermesan, O., Friess, P. (2013). Internet of things: Converging technologies for smart environments and integrated

[3] Tene, O., Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, 64, 63-69.

[4] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations (No. Special Publication (NIST SP)-800-162). National Institute of Standards and Technology.

[5] Alrawais, A., Alhothaily, A., Hu, C., Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.

[6] Harkins, M. W. (2016). Managing risk and information security: protect to enable. Springer Nature.

[7] Khan, M. A., Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[8]] Sadeghi, A. R., Wachsmann, C., Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

[9] Roman, R., Zhou, J., Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

[10] Voigt, Paul, et al. "Practical implementation of the requirements under the GDPR." The EU General Data Protection Regulation (GDPR) A Practical Guide (2017): 245-249.

[11] Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[12] Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[13] Dhillon, G., Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

[14] Roman, R., Najera, P., Lopez, J. (2011). Securing the internet of things. Computer, 44(9), 51-58.

[15]] Bishop, M. (2003). Computer security: art and science. Addison-Wesley.

[16] Zhang, Y., Meratnia, N., Havinga, P. (2014). Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine. Ad Hoc Networks, 13, 235-249.

[17] Mell, P., Scarfone, K., Romanosky, S. (2007). A complete guide to the Common Vulnerability Scoring System Version 2.0. Published by FIRST–Forum of Incident Response and Security Teams, 1-23.

[18] Abomhara, M., Koien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65-88.

[19] Kuhn, D. R., Coyne, E. J., Weil, T. R. (2010). Adding attributes to role-based access control. IEEE computer, 43(6), 79-81.

[20] Dwork, C. (2006). Differential privacy. In 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006). Springer, pp. 1–12.

[21] Wurster, G., van Oorschot, P. C., Somayaji, A. (2007). A generic attack on checksumming-based software tamper resistance. In 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 127-138). IEEE.

[22] Das, R., Beinlich, M., O'connor, S., Healy, M., Maier, G. (2019). Secure boot and authenticated firmware updates in IoT devices. In 2019 29th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS) (pp. 1-8). IEEE.

[23] McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley Professional.

[24] Harris, S. (2013). All-in-One CISSP Exam Guide. McGraw-Hill Education.

[25] Shostack, A. (2014). Threat Modeling: Designing for Security. John Wiley Sons.

[26] Djahel, S., Nait-Abdesselam, F., Zhang, Z. (2010). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. IEEE communications surveys tutorials, 13(4), 658-672.

[27] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446.

[28] Howard, Michael, and Steve Lipner. The security development lifecycle. Vol. 8. Redmond: Microsoft Press, 2006.

[29] Voigt, Paul, and Axel Von dem Bussche. ”The eu general data protection regulation (gdpr).” A Practical Guide, 1st Ed., Cham: Springer International Publishing 10.3152676 (2017): 10-5555.

[30] avoukian, A. (2010). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.

[31] E. Bertino and N. Islam, ”Botnets and Internet of Things Security,” in Computer, vol. 50, no. 2, pp. 76-79, Feb. 2017.