Assessing the Security Vulnerabilities and Countermeasures of Connected and Smart Devices

Dimah Almani and Steven Furnell
University of Nottingham, UK

dimah.almani@nottingham.ac.uk
steven.furnell@nottingham.ac.uk

Abstract: Traditional devices are evolving into more automated, and smart entities forming Internet of Things (IoT) technology a huge complex network composed of millions of smart connected machines. The rapid proliferation of such a technology has a significant impact on various applications and domains daily, including domestic (smart home) devices, transportation, cities, energy, healthcare, manufacturing, and many others. However, in parallel with providing convenience to users, this technology comes with many concerns, risks, and vulnerabilities that threaten both the security and privacy of the users. Poor authentication practices include weak password policies and no multi-factor authentication, which can make devices vulnerable to unauthorized control, thereby giving the attacker access to sensitive user data or hijacking the device itself. Inadequate encryption techniques further worsen the problem by leaving communications unsecured and sensitive data open to interception and theft. Insecure network interfaces are common because of the lack of proper security measures in their design and thus give an attacker the entry point into otherwise secured devices. Moreover, due to the lack of consistent deployment of security by different manufacturers, some devices remain more open to attacks than others. While some of these vulnerabilities have been identified in the existing literature, there is still a need for a more holistic view that considers the spectrum of security issues in IoT devices and their application domains. In this paper, we assess the vulnerabilities, and the security challenges inherent in IoT networks including weak authentication practices, inadequate encryption, and insecure network interfaces, and lack of standardization. Through different case scenarios in transportation and health systems, we compare the effects and implications of inadequate systems towards security. For example, inadequate authentication in healthcare could compromise patient safety, while in transportation, it may lead to disruptions and safety hazards. The paper concludes by recommending some strategies that improve IoT security, encompassing policy development and standardization efforts along with areas of future research for mitigating associated risks effectively.

Keywords: Authentication, Smart devices, IoT, Security, Transportation, Healthcare, Attacks, Safety

1. Introduction

IoT technology has transformed old devices into smart, intelligent devices, interconnecting them with many sectors of the world. This has emerged to change healthcare, transportation, smart cities, and industrial sectors. The efficiency and convenience introduced have enhanced this technology so much that it has become an indispensable part of modern life. Nevertheless, alongside these advancements, IoT technology introduces a wide range of security vulnerabilities and risks that pose threats to both user privacy and system reliability.

Most IoT devices run with very weak or intermittent security controls, leaving them vulnerable to unauthorized access, data breaches, and even hijacking the entire system. Weak authentication protocols, inadequate encryption methods, and insecure network interfaces increase these risks and allow hackers to exploit the weaknesses and take full advantage of the system with devastating consequences. Adding insult to injury is that most IoT device manufacturers lack standardization, creating a patchwork quilt of security vulnerabilities to which some devices are more susceptible. This paper discusses the critical security challenges IoT networks and devices face. Examining real-world scenarios in domains like transportation and healthcare that rely heavily on interconnected smart technologies, making them prime targets for cyberattacks that affect and threat user's safety and privacy. The paper then highlights the tangible impacts of inadequate security measures.

The discussion of the study extended to touch upon the urgent requirement for policy frameworks, standardization processes, and future research dimensions to actively fix these emerging vulnerabilities and ensure protection for this growing IoT ecosystem. This discussion is divided into five further sections: Section 2 discusses an overview of connected and smart devices, highlighting the emerging trends and developments in healthcare and transportation. Section 3 then proceeds to examine common security vulnerabilities in IoT and the different elements of security that may be targeted, analysing the impact of these vulnerabilities in specific IoT domains. Sections 4 and 5 represent the paper's main contribution, consider the main countermeasures and best practices, and provide a comparative analysis and evaluation of case scenarios. Finally, section 6 concludes the discussion and highlights the resulting directions for future work.

2. The Landscape of IoT and Smart Devices

The discussion in this section provides an overview of recent connected and smart devices, highlighting the developments in the healthcare and transportation sectors.

1.1 IoT Devices Overview

IoT is an extensive network of connected components working in unison by coordinating, acknowledging and sharing the resources in the network. IoT devices can connect, share, and interact with the user, as well as other smart devices, in real-time, using sensors and communication protocols forming the Internet of Things (IoTs) (Poslad, 2011), (Silverio et al, 2018). IoT examples range from personal devices, such as smartwatches, to industrial-grade factory equipment and smart city infrastructure, such as smart parking. The distinct functionality between these devices enables them to automatically complete tasks, respond to the surrounding environment, and interact with other systems without or with minimal human intervention. IoT devices have the following features:

Table 1: Outlining the main features of the smart devices

Feature	Description
Connectivity	The connectivity to the internet or local networks via Wi-Fi, Bluetooth, Zigbee, or cellular.
Automation	The ability to perform a task automatically based on specific events without human intervention.
Sensing	The ability to sense the surrounding environment to perform different tasks based on measured events.
Context-Awareness	The device ability to detect, understand then analyse its surroundings to perform an accurate decision.
Accessibility	Providing flexible and remote accessibility to the user operating the device remotely.
Self-Learning	The ability to adapt specific settings based on the user preferences or historical usage patterns.
Real-Time Monitoring	Collect and process data in real-time for immediate feedback or decision-making.

The highlighted IoT features in Table 1 are achieved through integration with machine learning algorithms, cloud computing, and edge computing, thus allowing both local and remote data processing. Despite these features, IoT connectivity also introduces some significant risks to the users, as vulnerabilities in any device may lead to a network compromise. Moreover, the rapid development might outstrip security measures, and thus, IoT networks will be increasingly attractive targets for cyber-attacks. It should be noted that such devices are used to facilitate users' lives and increase efficiency, convenience, and decision-making in many fields, especially in healthcare and transportation. Healthcare and transportation, in particular, rely heavily on interconnected smart technologies, making them prime targets for cyberattacks with potentially severe real-world consequences.

1.2 Emerging Trends and Developments in Healthcare and Transportation

The discussion in this section explores emerging trends and developments that shaping healthcare and transportation domains, highlighting their potential to enhance efficiency, safety, and quality of use.

- IoT in the Healthcare Sector

IoT-based healthcare systems are growing enormously, including remote health monitoring, wearable devices, fitness programs, etc., thus changing how health services are offered. Most research works to develop the IoT-based healthcare system to detect several symptoms more efficiently and accurately predict diseases. For example, wearables can continuously track heart rates, blood glucose levels, or physical activities and then send this information to health professionals for further analysis. Despite these advantages, the IoT-based healthcare system has some security issues due to the utilization of many devices that can compromise data and threaten the safety of patients (Li et al., 2024).

- IoT in the Transportation Sector

IoT developments play a major role in Intelligent Transportation Systems (ITS). Vehicular communication using IoT will be a new era of communication that forms ITS. An IoT-based ITS system utilizes a combination of smart and connected sensors to achieve and assist in managing the traffic system effectively. As a result, this

technology helps promote communication in railways and roadways, which enhances the driving experience (Whig et al., 2024). It is worth noting that vehicular communication networks are open-access and self-organized, so they are prone to potential attacks. Some attacks aim to disseminate fake messages to disrupt safety-related services or misuse the VANET's communication systems, leading to various types of damage, such as Denial of Service (DoS) (Almani et al, 2022).

In both these sectors, the coming trends are really pushing the boundaries of IoT technology: in healthcare, toward better diagnostic precision and treatment according to the patient's condition; in transportation, including the development of smart highways and predictive maintenance of vehicles to open ways toward safer and more efficient mobility. While these developments are highly promising, they also raise the stakes for security measures that must be implemented to protect sensitive data and ensure system reliability.

3. Security Vulnerabilities and Their Impact Across IoT Domains

Smart devices continue to expand across various domains, and they bring a wide array of security vulnerabilities that threaten the interconnected systems' confidentiality, integrity, and availability Understanding these vulnerabilities and their impact on systems is crucial so that appropriate security controls may be implemented based on the peculiar requirements of each IoT environment.

3.1 Common Vulnerabilities

The common vulnerabilities faced by the smart devices currently are listed below:

- **Weak Authentication:** Most IoT devices are deployed on default passwords, or their passwords are easily guessable, and they do not support multi-factor authentication. This leads to unauthorized access to the device, which could easily be used against the attacker through such weak authentication (Alsheavi, 2024).
- **Inadequate Encryption:** Failure of encryption or poor implementation may result in the interception of sensitive data in transit across devices. This exposes personal and confidential information to potential breaches (Jain, 2024).
- **Insecure Network Interfaces:** Poorly secured communication protocols and open network ports can be used by malicious attackers to siphon critical information or inject malicious commands that may hamper the integrity and functionality of IoT systems (Sevinch, 2024).
- **Standardization Challenges:** There is a lack of uniformity in security standards by various manufacturers. This makes the implementation of security variable and can hardly comprehensive security across disparate IoT ecosystems (Szczepaniuk, 2022).

Figure 1 highlights some of the real case scenarios that show a few common IoT system vulnerabilities among different industries. Such cases are the result from the weakness mentioned above and underscore the need for robust security measures to protect devices, networks, and sensitive data from such malicious actors.

3.2 Impact of Vulnerabilities in Specific IoT domain

In healthcare and transportation domains, the effect of vulnerabilities in smart devices can be different based on the devices and their purpose. Explaining these effects is essential for customised security solutions considering domain-specific challenges and threats.

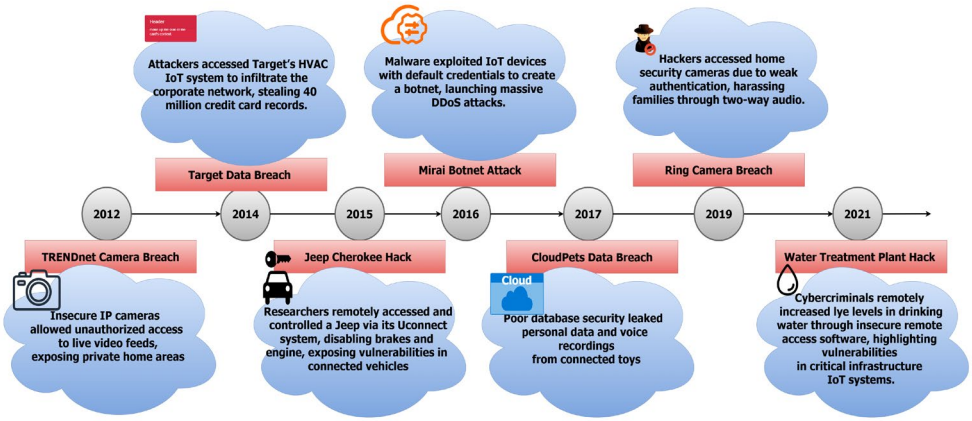

Figure 1: Examples of IoT application security breach

- Healthcare

While the integration of IoT in healthcare, such as smart medical devices and wearables, has dramatically improved patient care and monitoring, it poses serious risks:

Patient Safety: Insecure network in the health sector causes vulnerabilities in connected medical devices-including but not limited to pacemakers or insulin pumps-and actual malicious tampering can result in loss of lives.

Data privacy: Data privacy: Weak authentications and inadequate encryption systems might lead to serious privacy breaches and potential misuse. A breach can occur in the form of unauthorized access to Electronic Health Records (EHRs) or personal health data, exposing sensitive information that could be used for fraud.

As an example of this context, in 2024, several U.S. hospitals were targeted by a ransomware attack. The attack affected the connected medical devices, which gained control of patient monitoring systems, forcing hospitals to revert to manual procedures (van, 2024).

- Transport.

IoT improvements in transportation facilitate navigation, communication, and safety but also introduce following critical risk factors:

Communication Disruptions: Weakness in in Vehicle-to-Everything (V2X) communication networks can easily break the real-time sharing of data.

Safety Threats: As a result of inadequate encryption, malicious actors can hack into Connected and Autonomous Vehicles (CAVs) and shut down key systems such as the brakes and steering, endangering the passengers.

Scenarios of Accidents: In correct data such as fake reports and altered emergency messages can

Slow Adoption of Secure Technologies: Standardization challenges in connected vehicles lead to inconsistent security practices and interoperability issues across manufacturers, creating vulnerabilities (V2X) communication. These gaps increase the risk of cyberattacks.

As an example of this context, in 2016, researchers remotely accessed and controlled a Tesla Model S via its CAN bus, exposing weaknesses in its firmware (Banks, 2018).

4. Countermeasures and Best Practices

Various security systems have been globally employed to protect IoT users from the safety and security risks discussed earlier. Table 2 summarises some indicative countermeasures and best practices for improvement and strength in the security aspects with these systems. These span a series of categories, evidencing that the required elements span different perspectives and fall within the responsibility of different stakeholders (e.g. some rest with those designing and developing the technologies, and others with those deploying them).

Table 2: Countermeasures and Best Practices in IoT Security

Category	Countermeasures	Best Practices
Technical Solutions	Stronger authentication mechanisms	Use multi-factor authentication to enhance login security (ALSaleem & Alshoshan, 2021).
	Better encryption standards for data protection.	Implement AES-256 encryption for data protection (Nyarko et al, 2017).
Policy and Standardization	Establish global standards like ISO 27001 and NIST guidelines.	Adopt frameworks such as NIST Cybersecurity Framework (Möller, 2023).
	Introduce regulatory legislation for IoT security compliance.	Mandate IoT security certifications for manufacturers.
Manufacturer Responsibility	Incorporate security into the design lifecycle.	Design devices with a secure-by-design.
	Provide periodic software updates with security patches.	Regularly release updates addressing newly identified vulnerabilities.
User Awareness	Educate users on secure practices (e.g., strong passwords).	Encourage strong passwords and avoid default credentials (Furnell, 2018).

	Promote training for proper configuration and use of IoT devices.	Conduct user workshops and provide accessible security guides.

In some cases, there is a case to be made theat the security features and default provisions ought to be mandated rather than offered at the discretion of individual providers. Indeed, recognising this as an issue, the European Union and the United Kingdom have made legislative efforts to enhance the security of smart devices.

- **United Kingdom:** To improve consumer connectable products' cybersecurity, the government introduced the Product Security and Telecommunications Infrastructure (PSTI) Act (Decian and Jaafar, 2024) that requires manufacturers, importers, and distributors in healthcare and transportation domains to adopt certain security requirements to keep insecure products out of the UK market as listed below:

Mandatory security Controls: Manufacturers need to implement baseline security controls such as robust passwords and vulnerability disclosure policies to secure devices against emerging threats.

Incident Response Responsibilities: Upon discovering a security vulnerability, manufacturers are responsible for swiftly remedying the issue and notifying relevant stakeholders, including consumers.

Record-Keeping: Manufacturers are also required to maintain records of failures in compliance and investigations for a period of 10 years in order to enhance accountability and traceability.

European Union: The European Union's Cyber Resilience Act (CRA) strives to establish common standards for cybersecurity in products containing digital elements, both hardware and software (Chiara, 2022). The CRA is an integrated effort towards enhancing the EU's cybersecurity horizon so that digital goods are adequately positioned to combat impending threats, and seeks to do this by:

- Implementation of Secure by Default Principles: Healthcare and transportation sectors should have products designed and developed to demonstrate cybersecurity considerations so that they are less reliant on consumers to properly configure security controls.
- Risk Assessments Required: Healthcare and transportation manufactures should perform cybersecurity risk assessments before marketing their products and hold them for a minimum of 10 years from the time that the product comes out.
- Incident Reporting: Firms have the obligation to submit any significant incidents to the European Union Agency for Cybersecurity (ENISA) within 24 hours of their discovery and implement measures to manage the risks.
- Compliance and Penalties: Non-compliance with the CRA will invoke penalties of up to €15 million or 2.5% of the global annual turnover of the organization, emphasizing the need for compliance with the rules.

The PSTI Act and Cyber Resilience Act both point to benchmarking measures of the futuristic orientation of regulatory responses to minimizing vulnerability in smart devices with a perspective towards consumer protection and securing the overall cybersecurity landscape in each jurisdiction.

5. Putting the Controls into Practice

Implementing security countermeasures in the transport and health sectors tackles vulnerabilities and boosts operational resilience, data integrity, and users' trust. The sub-sections below offer a deeper review of each of the measures proposed in each category and their potential effect, with related details and examples offered from the perspective of the two sectors under consideration.

5.1 Technical Solutions

Technical cybersecurity solutions are clearly an important element of securing the core technologies in use, and key aspects here will always relate to the appropriate authentication of users, and the safeguarding of stored and transmitted data.

- **Stronger Authentication Mechanisms:** Multi-factor authentication (MFA) systems provide an extra layer of security to authenticate a user (e.g., a password) (Madhu et al, 2025). In MFA, additional verifications are required, such as a one-time password (OTP) that is sent to a user's email address or mobile device to generate a time-based code, which means that at least two factors have been

verified. Here is an explantion of using the benefits of using MFA in the healthcare and transportation domains.

MFA in the Healthcare Domain: (MFA) drastically reduces unauthorized access risks. For example, hospitals adopting MFA have significantly declined phishing-related breaches. In the healthcare sector, the confidentiality of patient personal and health status data is of the essence, and MFA ensures that only authorized individuals can access such sensitive information. The authorized individuals must provide a security token, fingerprints, facial recognition, or biometric data (Saxena & Sharma, 2024). Data Breach Investigations, 2023, a report by Verizon, shows that credential theft accounts for about 74% of breaches in healthcare, which can be reduced by as much as 90% with the use of MFA (Muir et al, 2024).

MFA in the Transportation Domain: In the Intelligent Transportation System (ITS), vehicles are connected to share critical and safety data. Adopting MFA in the vehicular network prevents unauthorized access to onboard systems, enhancing passenger safety. Vehicles rely on Advanced Driver Assistance Systems (ADAS) to strengthen their cyber-physical landscape in such a network (Almani et al, 2024). Deploying MFA mechanisms adds an additional layer of defence, ensuring that only authorized users can access and control their vehicles. The MFA-based ADAS can proactively identify and thwart potential cyber-attacks, safeguarding the integrity of critical vehicular systems. For instance, Tesla's introduction of MFA for its ADAS significantly reduced the risk of account compromise (Yousseef, 2024).

- **Better Encryption Standards for Data Protection:** AES (Advanced Encryption Standard) is a symmetric block cypher algorithm that encrypts data in blocks of 128 bits using cypher keys of 128, 192, or 256 bits to ensure the confidentiality of transmitted data (Allwine et al, 2025). The followings are the explantions of using the benefits of using AES in the healthcare and transportation domains.

AES in the Healthcare Domain: AES plays an important role in healthcare for securely protecting sensitive patient data being transmitted and stored by various connected medical devices within the ecosystem of the Internet of Medical Things (IoMT), through encryption. For example, medical devices such as an insulin pump are encrypted with AES to protect patients from cyberattacks, demonstrated by Medtronic adopting the encryption after vulnerabilities were exploited (Mohanta et al, 2025).

AES in the Transportation Domain: In transportation, encrypted vehicular communication reduces the risk of cyberattacks. The common and lighter encryption mode for securing shared information among vehicles, called Elliptic Curve Cryptography (ECC), reduces computational overhead and latency, which is critical for real-time decision-making in vehicular networks. For instance, a 256-bit key in ECC provides equivalent security to a 3072-bit key in RSA, making it both secure and lightweight for V2V systems (Hakeem et al, 2023).

5.2 Policy and Standardization

Globally-recognised standards from ISO and NIST help to ensure cybersecurity reaches the next level in vital sectors like healthcare and transportation.

ISO 27001 and NIST in the Healthcare Domain: For instance, ISO 27001, in the health sector, protects electronic health records, medical devices, and IoT systems from unauthorized access to sensitive patient information and against being subjected to cyberattacks. Implementation of ISO 27001 reduces data breaches by a certain percentage, thus giving an organized framework for building an effective ISMS that will assist organizations in proactively identifying and mitigating security risks, hence reducing the possibility of data breach. An example in this context: When the National Health Service (NHS) in the UK implemented security policies that aligned with NIST after the WannaCry attack in 2017, it worked effectively by reducing ransomware risks (Patel, 2023).

ISO 27001 and NIST in the Transportation Domain: In the vehicle networks domain, NIST Special Publication 800-53 offers a comprehensive catalogue of security and privacy controls applicable to various systems, including those in the automotive sector. These controls are designed to protect organizational operations and assets from a diverse set of threats and risks, including hostile attacks and human errors (Ramli, 2024).

5.3 Manufacturer Responsibility

This section explores the critical responsibilities of manufacturers in ensuring safety, security, and reliability in healthcare and transportation domains through security-by-design and periodic software updates.

- **Security-By-Design**: Manufacturers are critical in embedding robust security measures into the foundational design of smart and connected devices.

Security-By-Design in the Healthcare Domain: Companies like Abbott have implemented encrypted communication protocols in their medical devices, such as pacemakers and glucose monitors, to prevent data breaches and unauthorized control (Davis & John, 2022).

Security-By-Design in the Transportaion Domain: Toyota integrates secure-by-design principles into their connected cars, deploying intrusion detection systems and secure communication channels to protect vehicles against hacking, such as remote access attacks (Husni, 2016).

- **Periodic Software Updates:** Periodic software updates help keep healthcare and transportation systems secure, reliable, and up-to-date with the latest technology and safety standards.

Software Updates in Healthcare: Periodic software updates are essential for mitigating vulnerabilities in life-critical devices. For instance, Philips addressed identified vulnerabilities in its IntelliVue patient monitoring systems by releasing patches, ensuring the continued protection of sensitive patient data and device functionality (Kant, 2022).

Software Updates in the Transportation: Tesla has led the way with over-the-air (OTA) updates, which not only fix software bugs and vulnerabilities in real-time but also introduce new security features. This approach enhances both user convenience and device safety, ensuring vehicles are safeguarded against ever-evolving cyber threats (Banks, 2018).

5.4 User Awareness

This section discusses the essential roles of user awareness in ensuring safety, security, and reliability in healthcare and transportation domains through education on secure practices and training on IoT configuration.

- **Education on Secure Practices:** Educating users about secure practices helps reduce human error, which is one of the leading causes of cyber breaches.

Education on Secure Practices in Healthcare: Training programs aimed at staff using connected medical devices and systems have shown measurable benefits. For instance, the NHS implemented training focused on phishing awareness, resulting in a 60% reduction in successful phishing attempts, safeguarding patient data and hospital systems (Priestman, 2019).

Education on Secure Practices in Transportation: Educating users of ride-hailing services like Uber about app security—such as recognizing fraudulent links and setting strong passwords—has reduced instances of fraud and also increased user confidence in the platform (Ramli, 2024).

- **Training on IoT Configuration:** Properly configured IoT devices ensure security in operation and reduce vulnerabilities occurring due to default settings or other forms of improper setting.

IoT Configuration Training in Healthcare: Hospitals that have provided specialized training to IT teams for the configuration of IoT-enabled medical devices, such as infusion pumps and monitors, showed a reduction in misconfigurations, preventing breaches or device malfunctions (Mohanta, 2025). Most effective has been ensuring that users understand the importance of changing default passwords, enabling encryption, and applying timely updates.

IoT Configuration Training in Transportation: The training enables the users of connected cars to make configurations in the on-board systems, whether it be in infotainment or even diagnostic systems, to avoid connecting to unverified devices or networks, and thus greatly reduces the possibilities of hacking. Driver awareness campaigns provided by carmakers are important for personal data protection and car systems.

5.5 Overview and Implications of the Discussion

In short, protecting healthcare and transport systems has to be a combined effort of robust technical measures, policy alignment, and user education. More secure authentication, newer encryption, and adherence to international standards like ISO 27001 and NIST are required to safeguard data. Security by design has to be a priority for manufacturers, while routine software updates ensure protection in the long run. Equally important is educating users on security best practices and the risks of IoT devices. By combining these approaches, we can build a resilient and secure framework for both sectors.

6. Conclusion and Future Work

Smart and connected IoT devices facilitate human life across different domains, including transportation, homes, hospitals, and factories. However, the growing popularity of smart and connected devices is increasing attention towards security and safety issues. This paper discussed severe cases of threats to IoT devices. We presented an overview of vulnerabilities in smart devices and existing weak systems that could affect user safety and privacy, particularly in healthcare and transportation domains. Furthermore, we briefly discussed the security countermeasures and the best practices that improve the security levels in both domains. Finally, we provided a comparative analysis and evaluation of these countermeasures to open the discussion for further investigation. Additionally, we emphasize the need for ongoing research that address the regulatory landscape's impact on IoT security.

References

Allwine, A., Atim, S. B., & Afdhaluddin, M. (2025). Advanced encryption standard (AES) cryptography application design. Journal of Computer Science, Information Technology and Telecommunication Engineering, 6(1).

Almani, D., Furnell, S., & Muller, T. (2022, June). Supporting Situational Awareness in VANET Attack Scenarios. In *ECCWS 2022 21st European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

Almani, D., Muller, T., Carpent, X., Yoshizawa, T., & Furnell, S. (2024). Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments. *Future Internet*, *16*(3), 77. https://doi.org/10.3390/fi16030077

ALSaleem, B. O., & Alshoshan, A. I. (2021, March). Multi-factor authentication to systems login. In *2021 National Computing Colleges Conference (NCCC)* (pp. 1-4). IEEE.

Alsheavi, A., Hawbani, A., Othman, W., Wang, X., Qaid, G., Zhao, L., ... & Al-Qaness, M. A. (2024). IoT Authentication Protocols: Challenges, and Comparative Analysis. *ACM Computing Surveys*.

Banks, V. A., Plant, K. L., & Stanton, N. A. (2018). Driver error or designer error: Using the Perceptual Cycle Model to explore the circumstances surrounding the fatal Tesla crash on 7th May 2016. *Safety science*, *108*, 278-285.

Chiara, P.G., 2022. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review, 3(2), pp.255-272.

Davis, C., & John, E. (2022, August). Shared round core architecture: A novel AES implementation for implantable cardiac devices. In *2022 IEEE 65th International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 1-4). IEEE.

Decian, J. and Jaafar, F., 2024, November. Wiki-IoT: Registering and Evaluating the Security and Resilience of Internet of Things and Connected Devices Using a Collaborative Platform. In 2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC) (pp. 9-14). IEEE.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Furnell, S. (2018). Assessing website password practices–over a decade of progress?. *Computer Fraud & Security*, *2018*(7), 6-13.

Hakeem, S. A. A., & Kim, H. (2023). Authentication and encryption protocol with revocation and reputation management for enhancing 5G-V2X security. *Journal of King Saud University-Computer and Information Sciences*, *35*(7), 101638.

Husni, E., Hertantyo, G. B., Wicaksono, D. W., Hasibuan, F. C., Rahayu, A. U., & Triawan, M. A. (2016, July). Applied Internet of Things (IoT): car monitoring system using IBM BlueMix. In *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)* (pp. 417-422). IEEE.

Jain, K., Titus, B., Krishnan, P., Sudevan, S., Prabu, P., & Alluhaidan, A. S. (2024). A Lightweight Multi-Chaos-based Image Encryption Scheme for IoT Networks. *IEEE Access*.

Kant, N., Peters, G. M., Voorthuis, B. J., Groothuis-Oudshoorn, C. G., Koning, M. V., Witteman, B. P., ... & Doggen, C. J. (2022). Continuous vital sign monitoring using a wearable patch sensor in obese patients: a validation study in a clinical setting. *Journal of clinical monitoring and computing*, *36*(5), 1449-1459.

Li, C., Wang, J., Wang, S., & Zhang, Y. (2024). A review of IoT applications in healthcare. *Neurocomputing*, *565*, 127017.

Madhu, B., Shubhada, B. N., & Saras, S. K. (2025). Multi-factor authentication for smart internet transactions. Digital Defence: Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics, 111.

Mohanta, B. K., Awad, A. I., Dehury, M. K., Mohapatra, H., & Khan, M. K. (2025). Protecting IoT-Enabled Healthcare Data at the Edge: Integrating Blockchain, AES, and Off-Chain Decentralized Storage. *IEEE Internet of Things Journal*.

Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

Muir, A., Brown, K., & Girma, A. (2024, November). Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks. In *Proceedings of the Future Technologies Conference* (pp. 597-607). Cham: Springer Nature Switzerland.

Nyarko-Boateng, O., Asante, M., & Nti, I. K. (2017). Implementation of advanced encryption standard algorithm with key length of 256 bits for preventing data loss in an organization. *International Journal of Science and Engineering Applications*, *6*(03), 88-94.

Patel, A. U., Williams, C. L., Hart, S. N., Garcia, C. A., Durant, T. J., Cornish, T. C., & McClintock, D. S. (2023). Cybersecurity and information assurance for the clinical laboratory. *The journal of applied laboratory medicine*, *8*(1), 145-161.

Pathak, S., Islam, S. A., Jiang, H., Xu, L., & Tomai, E. (2022). A survey on security analysis of Amazon echo devices. *High-Confidence Computing*, *2*(4), 100087.

Poslad, S. (2011). Ubiquitous Computing: Smart Devices, Environments and Interactions. Hoboken, NJ, USA: Wiley.

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics*, *26*(1).

Ramli, A. H., Maarop, N., Zulkifli, M. S., Samy, G. N., Hassan, N. H., & Mohammad, R. (2024). Information Security Risk Assessment Measures of Facility Management in Transport Industry. *Malaysian Journal of Information and Communication Technology (MyJICT)*, 1-10.

Saxena, P., & Sharma, R. (2024, July). Future Integrating Intrusion Detection Systems and Multi-Factor Authentication in ADAS. In *2024 IEEE 4th International Conference on Sustainable Energy and Future Electric Transportation (SEFET)* (pp. 1-6). IEEE.

Sevinch, Q. (2024, June). NETWORK SECURITY IN THE INTERNET OF THINGS (IOT): CHALLENGES AND PROSPECTS. In *E Conference Zone* (pp. 35-42).

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? A conceptualisation within the paradigm of the Internet of Things. Visual Engineering, 6(1), 3. https://doi.org/10.xxxx/yyyy

Szczepaniuk, H., & Szczepaniuk, E. K. (2022). Standardization of IoT Ecosystems: Open Challenges, Current Solutions, and Future Directions. In *Internet of Things* (pp. 23-42). CRC Press.

van Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., ... & Barten, D. G. (2024). Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of emergency medicine*, *83*(1), 46-56.

Whig, P., Velu, A., Nadikattu, R. R., & Alkali, Y. J. (2024). Role of AI and IoT in Intelligent Transportation. In *Artificial Intelligence for Future Intelligent Transportation* (pp. 199-220). Apple Academic Press.

Yousseef, A., Satam, S., Latibari, B. S., Pacheco, J., Salehi, S., Hariri, S., & Satam, P. (2024). Autonomous Vehicle Security: A Deep Dive into Threat Modeling. *arXiv preprint arXiv:2412.15348*.

Zubairu, B. (2018). Novel approach of spoofing attack in VANET location verification for non-line-of-sight (NLOS). In Innovations in Computational Intelligence (pp. 45-59). Springer, Singapore.