Hypothesis

A Framework for the Integration of Safety and Security in the IoT

Mohammad Rezaul Karim *, Sohag Kabir, Ci Lei, Raluca Lefticaru

Posted Date: 7 August 2025

doi: 10.20944/preprints202508.0565.v1

Keywords: IoT; hazard; vulnerability; safety; security

 doi:10.20944/preprints202508.0565.v1

Article

A Framework for the Integration of Safety and Security in the IoT

Mohammad Rezaul Karim [1,*], Sohag Kabir [2], Ci Lei [1] and Raluca Lefticaru [1]

[1] University of Bradford

[2] Faculty of Engineering and Digital Technologies, University of Bradford, Bradford BD7 1DP, UK

* Correspondence: mrkarim2@bradford.ac.uk; Tel.: +0045 22660077

Abstract

The proposed framework for integrating safety and security in Internet of Things (IoT) systems addresses the complex interplay between these two critical aspects of system design. By recognizing that security vulnerabilities can directly impact safety and that safety hazards can create security risks, the framework takes a holistic approach to risk mitigation. This integrated perspective is particularly crucial in IoT environments, where interconnected devices and systems often operate in sensitive or critical contexts, such as healthcare, transportation, or industrial control systems. The framework's utilization of analytical tools like Fault Tree Analysis (FTA) and Attack Trees (AT) provides a structured methodology for identifying potential failure modes and attack vectors. This systematic approach enables developers and system architects to anticipate and address vulnerabilities proactively, rather than reactively responding to incidents. Furthermore, the inclusion of a structured remediation and validation process ensures that identified risks are not only recognized but also effectively mitigated and tested. This comprehensive cycle of analysis, remediation, and validation is essential for creating IoT systems that are both secure and safe, capable of maintaining reliability and trustworthiness in the face of evolving threats and operational challenges.

Keywords: IoT; hazard; vulnerability; safety; security

1. Introduction

The integration of safety and security considerations in IoT ecosystems is crucial as these systems become more complex and interconnected. This work proposes a unified approach to address both safety and security challenges within IoT systems, aiming to develop a comprehensive framework that ensures secure operations while maintaining safety standards across diverse IoT environments. The current practice of treating safety and security as separate concerns fails to account for their interdependencies, as security vulnerabilities can lead to safety hazards and vice versa. A combined framework enables real-time monitoring, secure communication of safety status, and guidance on preventive or corrective actions, reducing the likelihood of unsafe conditions [1]. To build robust and resilient IoT ecosystems, a co-analysis methodology that simultaneously addresses both safety and security domains is essential. The lack of integrated solutions that protect both digital assets and the physical environment is a major barrier to widespread IoT adoption [2,3]. This research emphasizes the need for a unified safety-security paradigm to strengthen trust and reliability in IoT systems. By developing a comprehensive approach that considers both aspects, this work aims to enhance the overall

2. Combining Safety and Security of IoT

The safety and security of Internet of Things (IoT) devices are critical for protecting both users and the broader network infrastructure. To strengthen the security posture of IoT environments, a

 doi:10.20944/preprints202508.0565.v1

combined detection and prevention methodology is essential [4]. One promising approach involves integrating Fault Tree Analysis (FTA) and Attack Trees (AT), which together provide a robust framework for addressing both safety and security challenges. FTA is traditionally used to identify potential failure modes in safety-critical systems, while AT focuses on mapping out possible attack paths that compromise system security. When these methods are combined, they enable a holistic analysis that considers how security vulnerabilities might lead to safety failures—and vice versa. This integrated approach allows for the identification of both accidental faults and intentional threats, enabling the development of effective countermeasures. By leveraging the strengths of both FTA and AT, designers can perform a compre-hensive risk assessment of IoT systems, particularly in safety-critical applications. This dual-analysis strategy supports the creation of resilient systems that maintain safe and secure operation, even under adverse conditions.

3. Proposed Model

A combined approach represents a significant strategy for enhancing the sustainability and efficiency of IoT by improving security across multiple protocol layers [5]. A comprehensive framework for integrating safety and security in IoT systems is proposed, as illustrated in Figure 1, drawing upon recent projects and an extensive review of the literature. The proposed model comprises seven interconnected components, each contributing to a holistic system protection strategy.

At the core of this framework is the IoT System component, which includes the network of devices, sensors, and infrastructure forming the Internet of Things ecosystem. Supporting this central element are two key protective layers: the Safety Component and the Security Component. The Safety Component focuses on preventing accidental harm, system malfunctions, and unintended consequences. In contrast, the Security Component targets deliberate threats, such as unauthorized access and malicious attacks.

The model's strength lies in its holistic approach, incorporating four additional blocks that facilitate a dynamic and iterative process of risk assessment and mitigation. The Co-analysis Block enables a joint examination of safety and security concerns, identifying potential overlaps and conflicts between these two domains. The Remediation Block is responsible for developing and implementing solutions to address identified vulnerabilities and risks. The Verification Block ensures that the proposed remediation measures effectively mitigate the identified issues without introducing new problems. Finally, the Comparing Block evaluates the overall system performance against predefined safety and security standards, allowing for continuous improvement and adaptation to evolving threats and challenges in the IoT landscape.

3.1. Working Procedure

The operational methodology of the proposed model employs a multifaceted approach that seamlessly integrates various interconnected steps and components. Fundamentally, this framework is designed to optimize the model's performance by leveraging the synergistic interactions among its constituent elements. Each component is meticulously calibrated to enhance the overall effectiveness of the system, ensuring that the model can adapt to diverse scenarios and deliver consistent results. This capability is crucial for maintaining accuracy and responsiveness, which are essential for real-time fraud detection[6]. The comprehensive nature of the methodology allows for a holistic approach to problem-solving, addressing potential challenges from multiple perspectives. This adaptability is vital for optimizing processes in real-time [7]. By incorporating a range of interconnected steps, the model can process complex inputs, analyze data from various sources, and generate outputs that are both accurate and relevant to the intended objectives. This intricate interplay of components not only enhances the model's robustness but also facilitates its ability to handle unforeseen variables and evolving requirements in real-world applications. The subsequent section provides a detailed exploration of the specific mechanisms and processes that underpin this operational framework, elucidating how these elements work in concert to achieve the model's goals. These frameworks

 doi:10.20944/preprints202508.0565.v1

extend beyond operational systems to areas such as adaptive control systems, where they contribute to real-time parameter estimation and model adaptation within IoT systems [8].

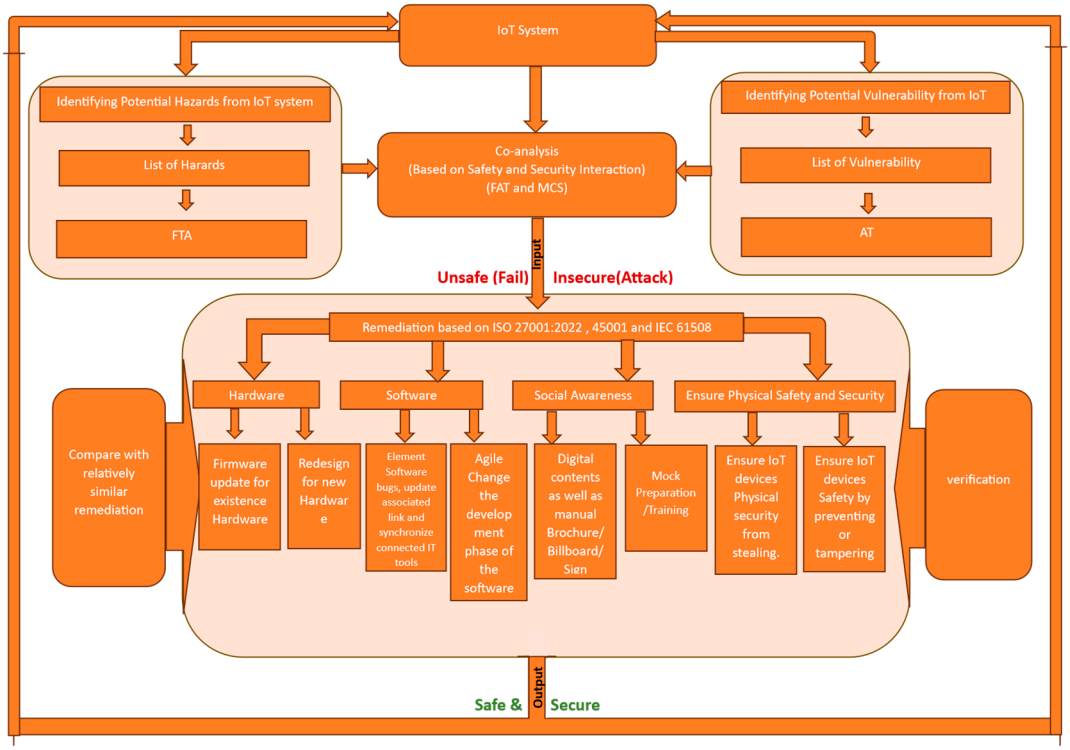

Figure 1. Propose model for combining Safety and Security of IoT.

3.1.1. IoT System

Figure 2. IoT System.

IoT systems are characterized by their ability to collect, process, and transmit data through networked sensors and devices embedded in the environment or worn on the body[9]. These systems utilize technologies such as RFID, wireless sensor networks, and smart objects to enable seamless communication and data exchange[10,11]. Interestingly, some advanced IoT systems incorporate artificial intelligence features, allowing devices to become self-inferenceable and self-monitorable, as seen in the concept of "Smart Things" [12].

 doi:10.20944/preprints202508.0565.v1

3.1.2. Safety Procedure

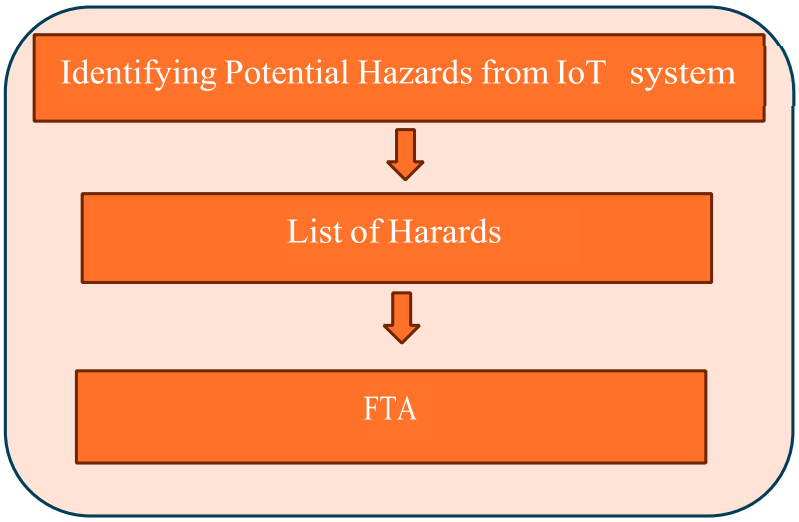

Figure 3. Safety Module.

The Internet of Things (IoT) ecosystem constitutes a complex network of interconnected devices and systems, each presenting distinct potential hazards and vulnerabilities. These hazards encompass a range of issues, from data breaches and privacy violations to physical safety risks associated with malfunctioning devices. The interconnected nature of IoT systems implies that a vulnerability in a single device can potentially compromise the entire network, resulting in cascading failures or security breaches. Common hazards include unauthorized access to sensitive data, device hijacking for malicious purposes, and the potential for IoT devices to serve as entry points for larger network attacks. This approach aids in preventing potential infringement incidents and enables rapid response to severe IoT hazards, thereby mitigating potential damage [13]. For instance, faulty IoT systems can lead to direct physical consequences, such as unlocking doors, modifying vehicle functions, or causing fire damage [14]. The vulnerabilities within the IoT ecosystem are equally diverse and may originate from various sources, including weak authentication mechanisms, insecure communication protocols, outdated software or firmware, and inadequate encryption practices. Physical vulnerabilities, such as unsecured hardware interfaces or easily accessible reset buttons, also pose significant risks. Fault Tree Analysis (FTA) will serve as a crucial tool in mapping these hazards and vulnerabilities, illustrating how different failure modes can interact and potentially lead to more severe consequences. This analysis will not only assist in identifying critical points of failure but also aid in developing targeted mitigation strategies to enhance the overall safety and security of IoT systems. This endeavor involves persistent research, fostering collaborations with experts, and promoting safety protocols tailored for IoT environments [15].

3.1.3. Security Procedure

This section focuses on identifying and cataloging security vulnerabilities within the IoT system. A comprehensive enumeration of all vulnerabilities present in the system is conducted, providing a detailed overview of potential weak points that could be exploited by malicious actors. This thorough analysis serves as a crucial foundation for understanding the system's security landscape and forms the basis for subsequent risk assessment and mitigation strategies.

 doi:10.20944/preprints202508.0565.v1

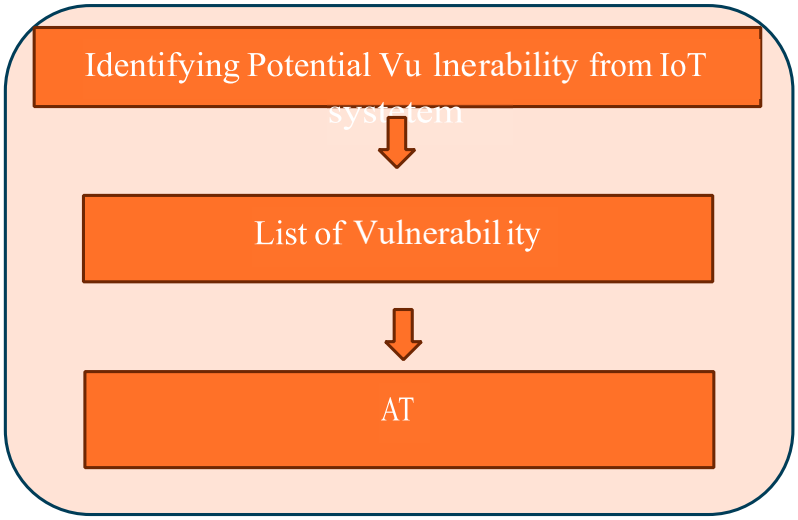

Figure 4. Security Block.

Following the vulnerability identification, an Attack Tree (AT) is constructed based on the vulnerability table. The AT is a graphical representation that illustrates various potential attack scenarios and their hierarchical relationships. It visually maps out the different paths an attacker might take to compromise the system, starting from the root (the ultimate goal) and branching out to show intermediate steps and alternative methods. This tree structure helps in visualizing the system's weak points, prioritizing security measures, and developing a comprehensive defense strategy against potential threats.

3.2. Co-Analysis of Safety and Security in the Internet of Things (IoT) Ecosystem

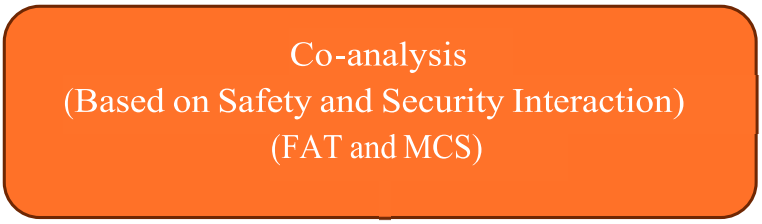

Figure 5. Safety-Security Co-analysis.

The co-analysis of safety and security in IoT systems has become increasingly significant due to the complex interplay between these two critical domains. Safety is primarily concerned with preventing unintentional harm or accidents, whereas security focuses on protecting systems from deliberate malicious actions. In IoT environments, these concerns are deeply intertwined — a security breach can lead to safety hazards, and conversely, safety failures may open avenues for exploitation, creating new security vulnerabilities.

3.2.1. Importance of Integrated Analysis

A co-analysis approach involves the simultaneous consideration of safety and security requirements across the entire lifecycle of an IoT system. This integrated method allows for the identification of potential conflicts and synergies between safety and security mechanisms, ultimately leading to more resilient and robust systems. Particularly in critical sectors such as healthcare, industrial automation, and smart transportation, the consequences of failures can be catastrophic, necessitating a holistic and proactive approach.

 doi:10.20944/preprints202508.0565.v1

3.2.2. Layered Vulnerabilities in IoT Architecture

The layered architecture of Internet of Things (IoT) systems, while beneficial for modularity and scalability, introduces complex security challenges across multiple attack surfaces. Each layer, from the perception layer to the network and application layers, presents unique vulnerabilities that require specific security measures. The perception layer, being the foundation of data collection in IoT systems, is particularly critical. It demands robust security protocols to protect against unauthorized access, data tampering, and device impersonation. Secure routing protocols ensure that data is transmitted through trusted paths, while key management systems safeguard the encryption and decryption processes. Authentication mechanisms verify the identity of devices and users, and access control systems regulate permissions to prevent unauthorized operations [16]. Moving up the IoT stack, the network and application layers face their own set of security challenges. The network layer must contend with threats such as man-in-the-middle attacks, denial of service, and traffic analysis. It requires secure communication protocols, intrusion detection systems, and network segmentation to maintain data integrity and confidentiality. The application layer, which interfaces directly with users and processes data, must guard against software vulnerabilities, insecure APIs, and data privacy breaches. Implementing end-to-end encryption, secure coding practices, and regular security audits are essential at this level. The interconnected nature of these layers means that a vulnerability in one can potentially compromise the entire system, underscoring the need for a comprehensive, multi-layered security approach in IoT deployments.

3.2.3. Integrated Security Frameworks and Emerging Threats

The implementation of integrated security frameworks is crucial in addressing threats such as denial-of-service attacks, phishing, and broader cyber-physical vulnerabilities. These frameworks must continuously evolve to address emerging risks, particularly as the adoption of IoT accelerates across various domains [17]. Interaction threats between applications and devices may lead to unintended behaviors, posing both safety and security risks [18]. As critical components in IoT devices, batteries present unique risks such as overheating and system failure. A layered security perspective—encompassing the physical layer, battery management systems, and applications—is essential for mitigating these risks [19]. Integrated systems not only enhance cyber defense but also contribute to ensuring physical safety by mitigating risks associated with cyber-physical interactions [20]. In healthcare-focused IoT (H-IoT), for instance, ensuring the protection of personal health data and maintaining the integrity of medical operations are of paramount importance. Integrated safety and security mechanisms serve as the foundation for building trust and reliability in such high-stakes environments [21].

3.2.4. Remidation Procedure

The Remediation section, based on ISO 27001:2022, ISO 45001, and IEC 61508 standards, outlines four key areas for addressing IoT system vulnerabilities: hardware, firmware and software, social awareness, and physical security. For IoT hardware, the focus is on updating existing firmware and potentially redesigning devices to enhance their security features. This may involve implementing stronger encryption protocols, improving authentication mechanisms, or adding tamper-resistant components to protect against physical attacks.

In terms of firmware and software, the emphasis is on rectifying potential bugs, updating associated links, and ensuring synchronization with connected tools. An agile development process is recommended for efficient bug fixes, allowing for rapid identification and resolution of security issues. Social awareness plays a crucial role in maintaining IoT safety and security. This can be achieved through various means, including digital content distribution, printed materials such as brochures and safety handbooks, and visual aids like billboard signs. Additionally, conducting mock drills can help reinforce security protocols and prepare users for potential threats. The physical security of IoT devices is equally important, requiring measures to prevent theft and unauthorized

 doi:10.20944/preprints202508.0565.v1

access. This may involve implementing secure storage solutions, access control systems, and tamper-evident seals to protect against physical manipulation of devices.

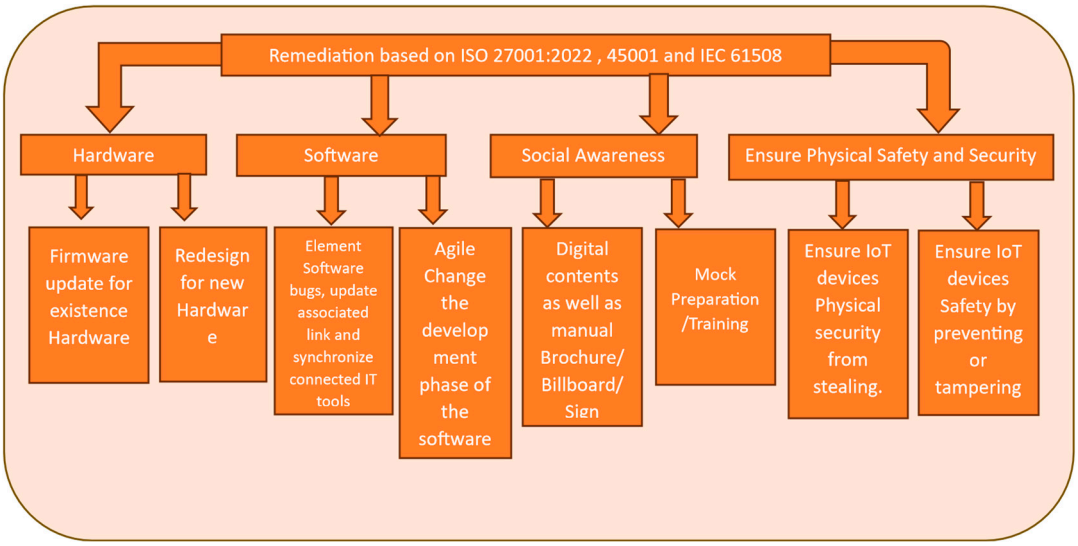

Figure 6. Remidation Process.

3.2.5. Comparing with Similar Remediation

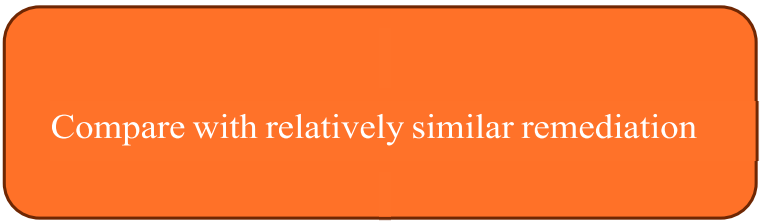

Figure 7. Model Comparing.

The proposed remediation approach is evaluated in the context of existing methods, offering a nuanced comparison that illuminates its distinctive features and potential advantages. This analysis delves into the core aspects of environmental remediation techniques, including their efficacy in addressing contamination, the economic feasibility of implementation, practical challenges encountered during execution, and the long-term viability of the solutions. By examining these critical factors, the section provides a holistic view of how the proposed method aligns with or diverges from current industry standards and practices.

Furthermore, this comparative analysis serves to elucidate the unique contributions of the proposed remediation strategy to the field. It highlights specific areas where the new approach may offer improvements or fill gaps in existing methodologies, potentially leading to more effective or efficient contamination management. The section also considers how the proposed method might complement or be integrated with current techniques, fostering a comprehensive understanding of its place within the broader landscape of environmental remediation. This thorough examination not only substantiates the value of the proposed approach but also provides stakeholders with a clear perspective on its potential to advance the field and address pressing environmental challenges.

 doi:10.20944/preprints202508.0565.v1

3.2.6. Verification and Validation

Figure 8. Model Verification.

The verification and validation process for remediation based on ISO 27001:2022, ISO 45001, and IEC 61508 involves a multi-layered approach to ensure comprehensive compliance and risk management. For ISO 27001:2022, organizations must conduct thorough risk assessments, implement appropriate security controls, and regularly review their effectiveness. This process includes identifying potential vulnerabilities in information systems, establishing robust access controls, and implementing encryption protocols where necessary. The validation phase involves testing these controls through various methods such as penetration testing, vulnerability scans, and simulated cyber-attacks to ensure they effectively mitigate identified risks.

In the context of ISO 45001 and IEC 61508, the remediation process extends beyond information security to encompass occupational safety and functional safety of critical systems. For ISO 45001, organizations must identify workplace hazards, assess associated risks, and implement control measures to ensure employee safety. This may involve redesigning work processes, providing personal protective equipment, or implementing safety training programs. The validation process for ISO 45001 includes conducting safety audits, analyzing incident reports, and gathering employee feedback to ensure the effectiveness of implemented safety measures. For IEC 61508, the focus is on ensuring the reliability and safety of electronic safety-related systems. This involves rigorous testing of safety functions, fault tolerance analysis, and systematic failure mode assessments. The validation process for IEC 61508 often includes extensive documentation, functional safety assessments, and third-party certifications to demonstrate compliance with required safety integrity levels.

3.2.7. Co-analysis of safety and security in IoT ecosystems

The co-analysis of safety and security in IoT ecosystems is not merely a technical consideration but a strategic necessity. As IoT systems increasingly mediate critical aspects of modern life, ensuring their safe and secure operation requires multi-disciplinary approaches that integrate technical safeguards, procedural protocols, and strategic oversight. By addressing both safety and security in a unified framework, developers and policymakers can foster resilient, trustworthy, and future-ready IoT solutions.

The co-analysis approach involves a comprehensive examination of both safety and security requirements simultaneously throughout the IoT system's lifecycle. This integrated method allows for the identification of potential conflicts between safety and security measures, as well as synergies that can enhance overall system resilience. By considering these aspects together, developers can create more robust IoT solutions that not only protect against cyber threats but also ensure the physical well-being of users and the environment. This holistic approach is particularly important in critical IoT applications such as healthcare, industrial control systems, and smart transportation, where the consequences of failures can be severe.

4. Conclusion

A unified strategy for IoT safety and security encompasses a multifaceted approach that addresses the complex challenges inherent in interconnected systems. This strategy involves

 doi:10.20944/preprints202508.0565.v1

implementing robust authentication mechanisms, encryption protocols, and access controls to safeguard data integrity and confidentiality. Simultaneously, it incorporates fail-safe mechanisms, redundancy measures, and real-time monitoring to mitigate potential safety risks. By integrating these elements, organizations can create a resilient IoT infrastructure that is better equipped to withstand both malicious attacks and unintentional system failures.

The implementation of such a unified strategy requires collaboration across various disciplines, including cybersecurity, systems engineering, and risk management. It necessitates continuous assessment and adaptation to evolving threats and technological advancements. This approach not only enhances the overall security posture of IoT systems but also promotes a culture of safety-consciousness among developers, operators, and end-users. As a result, IoT deployments become more reliable, fostering increased adoption and innovation across diverse sectors such as healthcare, smart cities, and industrial automation.

References

1. Kabir, S.; Gope, P.; Mohanty, S.P. A Security-Enabled Safety Assurance Framework for IoT-Based Smart Homes. *IEEE Transactions on Industry Applications* **2023**, *59*, 6–14. https://doi.org/10.1109/TIA.2022.3176257.
2. Celik.; Fernandes.; Earlence.; Pauley.; Eric.; Tan.; Gang.; McDaniel.; Patrick. Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities. *ACM Comput. Surv.* **2019**, *52*. https://doi.org/10.1145/3333501.
3. Meola, A. How the Internetof Things will affect security privacy. http://www.businessinsider.com/internet-of-things-security-privacy-2016-8, 2018. Accessed: 2021-12-28.
4. Mishra, A. Ai-Powered Cybersecurity Framework for Secure Data Transmission in Iot Network. *International Journal of Advances in Engineering and Management (IJAEM)* **2025**, *Volume 7*, 5–13. https://doi.org/10.35629/5252-07030513.
5. Mustafa, R.; Sarkar, N.I.; Mohaghegh, M.; Pervez, S. A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. *Sensors* **2024**, *24*. https://doi.org/10.3390/s24227209.
6. Bello, H.O.; Ige, A.B.; Ameyaw, M.N. Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. *World Journal of Advanced Engineering Technology and Sciences* **2024**, *12*, 021–034.
7. Boukouvala, F.; Muzzio, F.; Ierapetritou, M.G. Dynamic data-driven modeling of pharmaceutical processes. *Industrial & engineering chemistry research* **2011**, *50*, 6743–6754.
8. Pang, Z.H.; Ma, B.; Liu, G.P.; Han, Q.L. Data-driven adaptive control: An incremental triangular dynamic linearization approach. *IEEE Transactions on Circuits and Systems II: Express Briefs* **2022**, *69*, 4949–4953.
9. Singh, P. INTERNET OF THINGS BASED HEALTH MONITORING SYSTEM : OPPORTUNITIES AND CHALLENGES. *International Journal of Advanced Research in Computer Science* **2018**, *9*, 224–228. https://doi.org/10.26483/ijarcs.v9i1.5308.
10. Dudhe, P.; Kadam, N.; Deshmukh, M.S.; Hushangabade, R.M. Internet of Things (IOT): An
11. overview and its applications. institute of electrical electronics engineers, 2017, Vol. 8, pp. 2650–2653. https://doi.org/10.1109/icecds.2017.8389935.
12. Kavre, M.; Gadhade, Y.; Gadekar, A. Internet of Things (IoT): A Survey. institute of electrical electronics engineers, 2019, pp. 1–6. https://doi.org/10.1109/punecon46936.2019.9105831.
13. Samaniego, M.; Deters, R. Internet of Smart Things IoST: Using Blockchain and CLIPS to Make Things Autonomous. institute of electrical electronics engineers, 2017. https://doi.org/10.110 9/ieee.iccc.2017.9.
14. Yoon, S.; Kim, J. Remote security management server for IoT devices. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2017, pp. 1162–1164.
15. Van Oorschot, P.C.; Smith, S.W. The internet of things: security challenges. *IEEE Security & Privacy* **2019**, *17*, 7–9.
16. Olaniyi, O.O.; Okunleye, O.J.; Olabanji, S.O.; Asonze, C.U.; Ajayi, S. IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. *Asian Journal of Research in Computer Science* **2023**, *16*, 354–371.

 doi:10.20944/preprints202508.0565.v1

17. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth international conference on computational intelligence and security. IEEE, 2013, pp. 663–667.
18. Abbas, G.; Mehmood, A.; Carsten, M.; Epiphaniou, G.; Lloret, J. Safety, security and privacy in machine learning based internet of things. *Journal of Sensor and Actuator Networks* **2022**, *11*, 38.
19. Alhanahnah, M.; Stevens, C.; Bagheri, H. Scalable analysis of interaction threats in iot systems. In Proceedings of the Proceedings of the 29th ACM SIGSOFT international symposium on software testing and analysis, 2020, pp. 272–285.
20. Lopez, A.B.; Vatanparvar, K.; Deb Nath, A.P.; Yang, S.; Bhunia, S.; Al Faruque, M.A. A security perspective on battery systems of the Internet of Things. *Journal of Hardware and Systems Security* **2017**, *1*, 188–199.
21. Zhao, S.; Li, S.; Qi, L.; Da Xu, L. Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence* **2020**, *4*, 666–674.
22. Kumar, M.; Kumar, A.; Verma, S.; Bhattacharya, P.; Ghimire, D.; Kim, S.h.; Hosen, A.S. Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics* **2023**, *12*, 2050.