Review Open Access

Enhancing IoT Security through Standardization: A Review

Reza Shahbazian [1*]

1. Department of Computer Engineering, Modeling, Electronics and Systems, University of Calabria, Rende, Italy

Abstract

The fast growth of Internet of Things (IoT) has created unprecedented opportunities for innovation and connectivity across a wide range of domains. With this exponential expansion, however, comes an urgent need to address the security challenges in IoT networks. This paper addresses IoT security standards, concentrating on the protocols, guidelines, and best practices created by prominent standardization groups. We study the standard role in developing the IoT ecosystem, emphasizing the relevance of interoperability, privacy, and ethical considerations. We examine significant standards developed by organizations such as the IEEE Standards Association, the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the Internet Engineering Task Force (IETF). This paper also discusses shortcomings, and future prospects of IoT security standards. We contribute to a better understanding of the efforts being made to fortify the IoT against growing security threats and emphasizes the importance of an interdisciplinary approach that considers not only technological concerns but also privacy, ethical, and societal ramifications.

Keywords Internet of Things (IoT); Security; Privacy; Standard

Introduction

The Internet of Things (IoT) has developed as an innovative technological paradigm, created into the fabric of modern life by a web of interconnected devices, sensors, and systems. This connectivity extends beyond typical computing devices to daily objects [1], vehicles [2], industrial equipment [3], and even municipal infrastructure [4]. The IoT promises to revolutionize industries, improve convenience, and boost efficiency in previously imagined ways by facilitating the seamless flow of data and information among various entities.

The emergence of Industrial IoT (IIoT), where the convergence of industrial processes and digital connection is transforming manufacturing [5], logistics [6], and supply chain management, is one notable aspect of the IoT revolution. The IoT envisions a world in which manufacturing floors, logistics hubs, and essential infrastructure are linked by networks of sensors and actuators, allowing for real-time monitoring [7], predictive maintenance [8], and data-driven decision-making [9]. This convergence not only improves operational efficiency but also creates opportunities for new business models and revenue sources, ushering in the industry 4.0 era.

The importance of the IoT rests in its ability to instill intelligence and connectedness into previously inanimate items, so transcending traditional human-machine interactions [10]. IoT devices in smart homes regulate lighting and temperature based on resident preferences, and wearable health trackers monitor vital indicators and provide information for wellness optimization [11]. IoT-powered sensors in agriculture provide precision irrigation and soil analysis, maximizing resource utilization and crop output

* Correspondence:
reza.shahbazian@unical.it

[12]. IoT has the ability to transform society and economies on a global scale, with applications ranging from urban planning to transportation to energy management [13].

This incredible development, however, brings with it a number of security and privacy issues that must not be overlooked [14]. As billions of devices join the IoT ecosystem, they represent possible entry points for hostile actors looking to undermine data integrity, breach sensitive data, or disrupt key systems. The impacts of such breaches range from compromising personal privacy to economic espionage, and in the most extreme cases, manipulation of vital infrastructure with far-reaching societal consequences [15].

Addressing IoT security and privacy concerns is a critical component of establishing trust in the IoT ecosystem's continued growth and acceptance [16]. A disjointed approach to security can lead to vulnerabilities that spread across interconnected networks, emphasizing the importance of robust and standardized security solutions. Furthermore, IoT systems frequently collect large amounts of personal and sensitive data, necessitating the deployment of strict privacy controls to ensure that individuals' rights are honored and their data is responsibly handled. The IoT landscape's spreading complexity and variety highlight the crucial role that standards play in establishing effective security and privacy protections. Standards serve as a common language that supports interoperability and harmonizes security procedures in a world where varied devices, protocols, and applications converge. Without clear rules, the outcome is a fragmented ecosystem with discrepancies in security implementation, creating weaknesses that malevolent actors can exploit. Strong standards enable a uniform approach to security, allowing devices and systems from multiple vendors to communicate securely and seamlessly, improving the overall resilience of the IoT ecosystem. Furthermore, standards serve as a platform for rigorous security assessments, audits, and certifications. IoT manufacturers and developers can mitigate risks while also demonstrating their commitment to providing trustworthy products and services by complying to well-defined security standards. This builds consumer trust and fosters wider adoption of IoT technologies, eventually forcing the industry toward safer and privacy-conscious practices. Standards can assist regulators and politicians in developing frameworks that support responsible IoT adoption, finding a balance between innovation and individual rights protection [17]. Standards are important benchmarks for ethical data processing and consent-driven procedures in the context of IoT privacy [17]. Privacy standards lead the development of transparent data collecting processes, safe data storage, and mechanisms for informed user consent as IoT devices continuously acquire and exchange personal and sensitive data. These standards provide people more control over their data, lowering the danger of illegal access and exploitation. As the digital and physical worlds grow more integrated, standards provide a light of clarity, advocating responsible data management and safeguarding privacy values in an interconnected age [18].

This paper contributes to understanding and advancement of IoT security standards. We provide a review of the numerous tactics and frameworks available to improve the security posture of IoT ecosystems by examining a wide range of IoT security standards. The classification and explanation of standards in important areas of IoT security, such as communication, authentication, data privacy, device management, risk assessment, and interoperability, provide readers with a sophisticated understanding of the varied nature of IoT security concerns. Furthermore, exploring larger issues such as privacy adds dimension to the conversation by recognizing that effective IoT implementation demands a holistic strategy that goes beyond technical features.

The remainder of this paper is organized as follows. Section 2 introduces and categorizes IoT security standards depending on their applicability. Each category is presented briefly, followed by the standards that correspond to it. Section 3 analyzes various related standards that do not directly address IoT security, and Section 4 closes the article and suggests potential future efforts.

2. IoT Security Standards

As illustrated in Figure 1, we divide IoT security standards into seven major areas in this section. The rest of this section explains each category and its accompanying standards in detail.

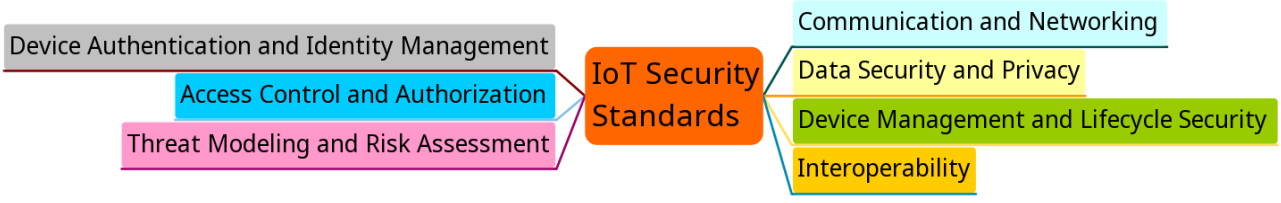

Fig 1. The categorization of IoT Security Standards

2.1. Communication and Networking Standards

Communication and networking standards play an important role in guaranteeing secure and dependable connectivity among Internet of Things devices, laying the groundwork for a thriving IoT ecosystem. These standards include protocols, technologies, and procedures that regulate how devices exchange data, connect to networks, and communicate with one another. In the networked IoT world, a secure communication framework is critical for protecting sensitive information, maintaining data integrity, and preventing unauthorized access or tampering as addressed in the following.

- Secure Communication Protocols: IEEE 802.15.4 and ISO/IEC 8802-15-4 standards establish protocols for efficient and secure communication between IoT devices, especially in resource-constrained contexts. These protocols ensure that data is sent in a way that reduces the possibility of eavesdropping, tampering, or unwanted access.
- Encryption: Encryption standards, such as those supported by Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), maintain the confidentiality of data transported via networks. Encryption turns data into a safe format that only authorized recipients can decipher, preventing unlawful interception.
- Authentication Mechanisms: IEEE 802.1AR and ISO/IEC 29115 define protocols for authenticating devices and establishing their network identity. Strong authentication systems aid in preventing unauthorized devices from getting network access and ensuring that only trusted organizations engage in IoT communications.
- Device Identity Management: These standards cover how devices in the network are uniquely identified and controlled. Impersonation and unlawful access are prevented by proper device identity management, which contributes to the overall security of the IoT ecosystem.
- Network Access Control: IEEE 802.1X standards offer network access control techniques to ensure that only authorized devices can connect to the network. This prevents rogue or compromised devices from obtaining access to the network and potentially compromising it.
- Constrained Environments: Communication and networking standards like "RFC 7228: Terminology for Constrained-Node Networks" are especially important in IoT device contexts with limited resources. These standards solve the issues posed by devices' limited processing power and memory while yet providing safe connection.

Communication and networking standards are the foundation of IoT security, allowing for the development of safe and interoperable IoT ecosystems. These standards ensure that IoT devices may securely interact with one another and with external systems, reducing the danger of data breaches, illegal access, and other security flaws. By adhering to these standards, IoT manufacturers, developers, and stakeholders can lay a solid security foundation that fosters user trust, promotes widespread adoption, and enables the full potential of the IoT in a variety of domains. Among the addressed standards, we breifly expalin three main standards as the following:

1. ISO/IEC 8802-15-4 (IEEE 802.15.4): The ISO/IEC 8802-15-4 standard, often known as IEEE 802.15.4, provides the physical and Medium Access Control (MAC) layers for low-rate wireless personal area networks (LR-WPANs). LR-WPANs are intended to allow communication between devices that have limited power, processing capabilities, and data rates, which are common characteristics of many IoT devices. This standard is suited for applications such as smart homes, industrial automation, and healthcare monitoring since it offers the foundation for developing dependable and energy-efficient communication lines. IEEE 802.15.4 contributes to the development of secure and resilient IoT networks by establishing efficient communication protocols and resolving energy restrictions.
2. NIST SP 800-183: The National Institute of Standards and Technology (NIST) Special Publication 800-183 is a comprehensive resource that provides information on Network of Things (NoT) communication security. It explores into the security concerns that surround IoT device communication, such as encryption techniques and safe protocols. The issues of safeguarding data sharing and communication channels in the context of IoT are addressed in this paper. NIST 800-183 aids companies in implementing effective security measures to protect IoT communications from potential threats and vulnerabilities by providing practical guidelines and best practices.
3. "RFC 7228: Terminology for Constrained-Node Networks" by IETF: The Internet Engineering Task Force (IETF) is critical in creating the architecture of the internet, and RFC 7228 makes an important contribution to the IoT security landscape. This RFC focuses on defining language particular to constrained-node networks, which are commonly used by IoT devices. Memory, computing power, and energy usage are all limited at constrained nodes. RFC 7228 enables clear communication among IoT stakeholders by introducing standardized vocabulary, assisting them in understanding the particular problems and requirements of IoT devices operating in resource-constrained contexts.

2.2. Device Authentication and Identity Management Standards

Device authentication and identity management standards are critical to maintaining the security and trustworthiness of IoT ecosystems. These standards define

means for authenticating IoT devices, guaranteeing that only authorized and valid devices can access and interact with the network. These standards reduce the dangers of unwanted access, device spoofing, and data breaches in the linked IoT landscape by securely managing device identifications and authentication processes. Key aspects these standards are presented in the following.

1. IEEE 802.1AR: This standard also known as "Secure Device Identity," is a framework for developing and managing secure identities for network devices. This standard specifies procedures for securely provisioning and authenticating device identities in order to ensure that devices are correctly represented and trusted inside the network.
2. ISO/IEC 27034-6: This standard is concerned with application security and contains concerns for device authentication and identity management in IoT applications. It discusses authentication mechanisms and best practices for ensuring secure device interaction with applications, databases, and other IoT system components.

Standards for device authentication and identity management are crucial for establishing a secure basis in IoT deployments. The following aspects are addressed by these standards:

- Preventing Unauthorized Access: These standards prohibit unauthorized or malicious devices from getting network access by establishing strong authentication procedures. This is necessary in order to avoid unwanted data access, tampering, and the possible compromise of vital systems.
- Mitigating Device Spoofing: Secure device identity management assures that devices cannot impersonate other network devices or entities. This prevents attackers from impersonating legitimate devices in order to obtain unwanted access.
- Establishing Trust: Device identity management establishes a foundation for trust between devices and networks. Verified device IDs enable network components to interact confidently, lowering the risk of data breaches or malicious activity.
- Enhancing Accountability: Accountability is established by uniquely identifying each device. If a security incident happens, the device can be traced back to it, assisting in incident response and resolution.
- Supporting Regulatory Compliance: Compliance mandates strong device authentication and identity management in many sectors. These guidelines assist firms in meeting their regulatory duties.

2.3. Data Security and Privacy Standards

Data security and privacy standards are critical components of IoT security, concentrating on ensuring the confidentiality, integrity, and availability of data generated, communicated, and stored inside the IoT ecosystem. These standards set recommendations for safeguarding sensitive data, preventing unwanted access, and ensuring compliance with privacy laws, addressing important concerns about the handling of IoT-generated data. The main standards in this category are explained in the following.

1. ISO/IEC 27001: The ISO/IEC 27001 standard provides a comprehensive foundation for Information Security Management Systems (ISMS). This standard, while not IoT-specific, provides an organized approach to detecting, assessing, and mitigating information security risks. Organizations can customize ISO/IEC 27001 principles to include IoT-specific security and privacy concerns, ensuring that data generated and processed by IoT devices is suitably safeguarded.
2. NIST SP 800-183: NIST SP 800-183 provides useful information about safeguarding data in transit and at rest in IoT systems. It focuses on encryption, access controls, and secure communication protocols, emphasizing the special issues of data protection in the context of IoT devices and networks.
3. Practical Internet of Things Security [19]: The work goes into practical IoT security aspects, such as data security and privacy. It explains how to properly deploy security measures, including encryption, access control, and data lifecycle management. The book helps practitioners grasp the complexities of safeguarding IoT-generated data by presenting real-world difficulties and solutions.

Data security and privacy standards have a profound impact on IoT ecosystems:

- Confidentiality and Privacy: ensures that sensitive data is kept private and personal information is kept safe from unauthorized access, lowering the risk of data breaches and privacy violations.
- Integrity and Trustworthiness: These standards protect data integrity by providing encryption and secure data transfer, preventing tampering or alteration during transit.
- Regulatory Compliance: Many industries are governed by data privacy laws (for example, GDPR and HIPAA). Following these guidelines assists companies in meeting legal requirements and avoiding penalties.
- Consumer Trust: Adherence to data security and privacy standards boosts consumer trust in IoT devices and services, hence driving widespread adoption.
- Responsible Data Handling: These standards aid organizations in implementing responsible data handling practices such as data minimization, appropriate consent processes, and secure data disposal.
- Mitigating Risks: Proactively addressing data security and privacy concerns decreases the probability of data breaches, reputational harm, and financial losses.

2.4. Access Control and Authorization Standards

Standards for access control and authorization are critical components of IoT security because they govern the procedures that determine which organizations have access to IoT resources and services. These standards provide protocols and policies that ensure only authorized devices, users, or applications interact with IoT networks, preventing unauthorized access and potential security breaches. Key Aspects of these standards are presented in the following:

1. ISO/IEC 29115: ISO/IEC 29115 focuses on ensuring entity authentication in IoT contexts. It sets criteria for various levels of authentication assurance, ensuring that the level of trust built between organizations fits with the IoT use case needs. This standard aids in the selection of appropriate authentication mechanisms to reduce the risks of illegal access.
2. IEEE 802.1X: IEEE 802.1X defines a network access control architecture based on ports that is applicable to IoT devices requesting network connectivity. It ensures that only authorized devices can connect to a network port. This standard is frequently used to prevent unwanted devices from connecting to networks, improving the security of IoT deployments.
3. NIST SP 800-183: The NIST SP 800-183 discusses access control considerations for IoT systems. It explains how to put in place access restrictions that limit which devices or users can access IoT resources and services. This paper underlines the significance of enforcing the principle of least privilege—granting entities just the permissions they require to reduce potential security threats.

2.5. Device Management and Lifecycle Security Standards

Device management and lifecycle security standards are critical for assuring the secure deployment, operation, and maintenance of IoT across their entire lifecycle. These standards provide an organized way for managing IoT devices successfully, from initial provisioning to retirement, while addressing security concerns at each stage of the device's existence. Key aspects of these standards are as follows:

1. ISO/IEC 30141: This standard provides a complete standard architecture for the Internet of Things ecosystem. This standard offers advice on different elements of IoT adoption, such as device management and security concerns. It explains how IoT devices should be managed, monitored, updated, and secured from the time they are integrated into the network until they are decommissioned.
2. IEEE 802.1Qbz: IEEE 802.1Qbz covers time-sensitive networking needs, which are critical for real-time communication and administration of IoT devices. This standard assures that devices can meet severe timing requirements, making it especially important for applications that demand exact device synchronization and coordination.

These standards for device management and lifecycle security contribute considerably to the overall security and endurance of IoT deployments aspects:

- Secure Onboarding: These standards govern the safe provisioning and onboarding of network devices, ensuring that devices are properly verified and permitted.
- Remote Device Updates: Over-the-air (OTA) upgrades of IoT devices are made possible by standards. This is critical for addressing vulnerabilities, installing fixes, and maintaining device security over the course of their operating life.
- Continuous Monitoring: Devices are regularly monitored for irregularities, unauthorized access, and potential security breaches as part of lifecycle security standards.
- Risk Mitigation: Organizations can limit the danger of devices being infiltrated or hijacked for harmful reasons by following to these standards, protecting both the device and the wider network.
- Sustainability: Secure device management and lifecycle procedures allow IoT devices to be successfully upgraded and maintained, extending their operational life. This helps to ensure the long-term viability of IoT investments.
- Compliance: Standards help enterprises satisfy regulatory compliance requirements for data security and device security.

2.6. Threat Modeling and Risk Assessment Standards

In the IoT ecosystem, threat modeling and risk assessment standards are critical for identifying potential vulnerabilities, analyzing risks, and implementing effective security solutions. These standards provide methodology and procedures for completely assessing security threats, comprehending their potential impact, and developing proactive mitigation solutions.

1. NIST SP 800-183: The NIST SP 800-183 provides a thorough overview of IoT device and system security aspects. It highlights the significance of threat modeling and risk assessment in the context of IoT. This article helps enterprises understand the security landscape and make informed risk management decisions by giving insights into potential threats and vulnerabilities related to IoT deployments.
2. Internet of Things: Principles and Paradigms [20]: This publication lays out the essential ideas and para-

Table 1. The Categorization of IoT security standards reviewed in Section 2.

Standard	Category	Focus Areas	Relevance
ISO/IEC 8802-15 (IEEE 802.15.4)	Communication and Networking	Low-rate wireless communication	Device communication
NIST SP 800-183*	Communication and Networking	IoT communication security	Encryption, secure protocols
RFC 7228	Communication and Networking	Constrained-node network terminology	Resource-constrained environments
IEEE 802.1AR	Device Authentication	Secure device identity	Authentication assurance
ISO/IEC 27034-6	Device Authentication	Application security, authentication	IoT application security
IEEE 802.1X	Access Control	Port-based network access control	Device network access
ISO/IEC 29115	Access Control	Entity authentication assurance	IoT entity authentication
ISO/IEC 27001	Data Security and Privacy	Information security management systems	IoT-specific security
NIST SP 800-183*	Data Security and Privacy	IoT data security	Data security in IoT
ISO/IEC 30141	Device Management and Lifecycle	IoT reference architecture	Device management, security
IEEE 802.1Qbz	Device Management and Lifecycle	Time-sensitive networking	Real-time communication
NIST SP 800-183*	Threat Modeling and Risk Assess.	IoT device and system security	Threat modeling, risk assessment
RFC 7452	Interoperability.	Architectural considerations	Smart object networking

* NIST SP 800-183 is repeated in several categories.

digms of the IoT. While it does not directly address threat modeling and risk assessment, it does provide a deeper knowledge of the complexities of IoT. This fundamental understanding helps to understand the potential security difficulties and dangers that threat modeling and risk assessment seek to address.

Threat modeling and risk assessment standards serve as cornerstones for IoT security:

- Vulnerability Identification: These standards aid in identifying potential security flaws and vulnerabilities in IoT ecosystems.
- Risk Evaluation: Organizations can analyze the possible impact of discovered threats and vulnerabilities on their IoT deployments by conducting detailed risk assessments.
- Mitigation Strategies: Threat modeling assists organizations in developing strategies to reduce identified threats, thereby improving the overall security posture of IoT systems.
- Resource Allocation: Risk assessment guides resource allocation decisions, ensuring that security measures are prioritized appropriately based on the severity of identified risks.
- Informed Decision-Making: Standards in this field give a standardized method to evaluating and managing IoT security threats, enabling organizations to make informed decisions to safeguard their IoT assets.

2.7. Interoperability Standards

Interoperability standards are essential for guaranteeing seamless communication, cooperation, and integration among various devices, systems, and platforms in the IoT ecosystem. These standards lay the groundwork for various IoT devices and components to work in concert, independent of their origins or makers. Interoperability standards improve the overall functioning and security of IoT deployments by addressing issues such as data sharing, communication methods, and device compatibility.

1. RFC 7452: Architectural Considerations in Smart Object Networking: The Internet Engineering Task Force (IETF) published this document, which examines architectural issues for smart item networking, a core part of IoT. It discusses different design ideas and technical concerns needed to ensure that smart things can communicate, collaborate, and interoperate efficiently within IoT networks.

Interoperability standards significantly impact the effectiveness and security of IoT ecosystems:

- Seamless Communication: These standards permit the flow of data and information among various IoT devices and components, allowing them to coexist peacefully.
- Scalability and Flexibility: Interoperability means that IoT deployments may be scaled up or extended without major changes, decreasing implementation complexity.
- Reduced Vendor Lock-In: Organizations can avoid vendor lock-in by adhering to interoperability standards and selecting solutions that meet their individual needs and criteria.
- Innovation and Collaboration: Standards promote collaboration and creativity by allowing devices and systems from many manufacturers to communicate with one another, resulting in a thriving and diverse IoT ecosystem.
- Security Considerations: Interoperability standards cover the security elements of data sharing and communication between devices, assisting in the prevention of security flaws caused by incompatible or poorly built interfaces.
- Ecosystem Integration: IoT interoperability standards enable IoT to be integrated with other technologies and systems, such as cloud services and data analytics platforms, hence increasing the value and utility of IoT deployments.

3. Privacy Related Standards

Some IoT standards that are not solely concerned with technological security but are concerned with larger security issues such as privacy, law, regulation, and ethical factors are as the following:

- ISO/IEC 27550: This standard specifies how to resolve privacy problems in IoT implementations. It presents a framework for recognizing and mitigating privacy issues related with personal data collection, processing, and sharing in IoT devices. The need of including privacy considerations into the design, development, and operation of IoT solutions is emphasized by ISO/IEC 27550.
- ISO/IEC 30182: While security and privacy are addressed, this standard focuses on the larger concept of trustworthiness in IoT devices. It offers recommendations for assessing and improving the trustworthiness of IoT devices and services, taking into account characteristics such as security, privacy, resilience, and transparency. ISO/IEC 30182 assists enterprises in developing more dependable and trustworthy IoT solutions.
- ISO/IEC 29134: This standard, while not particular to IoT, gives guidance for conducting privacy impact assessments (PIAs). PIAs assist firms in identifying and mitigating potential privacy concerns related to data processing activities. ISO/IEC 29134 helps guide the assessment of the privacy implications of IoT installations and ensure compliance with data protection requirements in the context of IoT.
- ISO/IEC 30107-1:This standard focuses on the detection of biometric presentation attacks (PAD). While it is not directly related to IoT, it does have ramifications for IoT systems that use biometric authentication. It establishes a paradigm for assessing biometric systems' susceptibility to presentation attacks (spoofing). Adherence to this standard can improve security and prevent unwanted access in IoT applications that rely on biometric data.
- ISO/IEC 20248: The protocol for providing audit and integrity services in information systems is outlined in this standard. While not unique to IoT, it can be useful in guaranteeing the integrity and accountability of data and transactions within IoT systems. Implementing audit and integrity services can aid in the detection of unlawful actions and the preservation of data accuracy.
- ISO/IEC 30141: While this standard is primarily concerned with architecture, it also covers ethical issues in IoT installations. It underlines the importance of taking ethical, sociological, and cultural factors into account while creating IoT systems. ISO/IEC 30141 encourages enterprises to integrate their Internet of Things deployments with ethical principles and values, ensuring that technology improvements are in line with social well-being.

These guidelines emphasize the need of including security, privacy, legal compliance, and ethical issues into IoT implementations. Organizations may establish IoT ecosystems that are not just technically secure, but also respectful of user privacy, compliant with regulations, and aligned with ethical standards by considering these larger features.

4. Conclusions and Future Works

The rapid growth of IoT devices has given unparalleled connectivity and ease to a wide range of areas, transforming companies and improving user experiences. This transformative potential, however, is accompanied by complex security issues that necessitate comprehensive answers [21-25]. This study delves into the varied landscape of IoT security, investigating a wide range of standards that cover essential aspects of protecting IoT ecosystems. Standards, best practices, and frameworks for designing, implementing, and operating secure IoT systems have been classified and explained in terms of communication and networking, device authentication, data security and privacy, device management, threat modeling and risk assessment, and interoperability. Notable standards such as ISO/IEC, NIST, IEEE, and others were investigated, each of which contributed to a more comprehensive IoT security posture.

The joint efforts of researchers, industry stakeholders, and standardization bodies will drive the evolution of IoT security standards in the future works. As the IoT landscape evolves, it is critical to address evolving risks, cross-industry collaboration, and user education to build a secure and trusted IoT ecosystem that harnesses IoT's revolutionary potential while protecting data, privacy, and user experiences. The promise of IoT can be fully fulfilled in a secure and robust manner by concentrated efforts in adopting and improving these standards.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Received: Jul. 2023 Accepted: Aug. 2023
Published online: Sep. 2023

DOI: 10.22034/ASAS.2023.411968.1032

5. References

[1] Khalid, Lawchak Fadhil, and Siddeeq Y. Ameen. "Secure Iot integration in daily lives: A review." Journal of Information Technology and Informatics 1.1 (2021): 6-12.

[2] Boursianis, Achilles D., et al. "Internet of things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: A comprehensive review." Internet of Things 18 (2022): 100187.

[3] Yang, Xing, et al. "Physical security and safety of iot equipment: A survey of recent advances and opportunities." IEEE Transactions on Industrial Informatics 18.7 (2022): 4319-4330.

[4] Nesse, Per J., and Olai Bendik Erdal. "Smart Digitalization in Nordic Cities and Municipalities Through Internet of Things." Economics and Finance Readings: Selected Papers from Asia-Pacific Conference on Economics & Finance, 2021. Singapore: Springer Nature Singapore, 2022.

[5] Ghosh, Swapan, et al. "Digital transformation of industrial businesses: A dynamic capability approach." Technovation 113 (2022): 102414.

[6] SHUKLA, VINOD KUMAR, et al. "Leveraging IIoT in Reverse Logistics: A WSN Approach." Internet of Things: Technological Advances and New Applications (2023): 119.

[7] Xu, Hansong, et al. "A Survey on Digital Twin for Industrial Internet of Things: Applications, Technologies and Tools." IEEE Communications Surveys & Tutorials (2023).

[8] Compare, Michele, Piero Baraldi, and Enrico Zio. "Challenges to IoT-enabled predictive maintenance for industry 4.0." IEEE Internet of Things Journal 7.5 (2019): 4585-4597.

[9] Bousdekis, Alexandros, et al. "A review of data-driven decision-making methods for industry 4.0 maintenance applications." Electronics 10.7 (2021): 828.

[10] Ding, Wenbo, et al. "Human–machine interfacing enabled by triboelectric nanogenerators and tribotronics." Advanced Materials Technologies 4.1 (2019): 1800487.

[11] Wickramasinghe, Nilmini, and Freimut Bodendorf, eds. Delivering superior health and wellness management with IoT and analytics. Springer Nature, 2019.

[12] Kumar, Khushi, et al. "IoT Enabled Crop Detection System using Soil Analysis." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.

[13] Radanliev, Petar, et al. "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance." (2018): 3-9.

[14] Schiller, Eryk, et al. "Landscape of IoT security." Computer Science Review 44 (2022): 100467.

[15] Shen, Yun, and Pierre-Antoine Vervier. "Iot security and privacy labels." Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7. Springer International Publishing, 2019.

[16] Voas, Jeffrey, et al. "Internet of Things (IoT) trust concerns." NIST Tech. Rep 1 (2018): 1-50.

[17] Lee, Euijong, et al. "A Survey on Standards for Interoperability and Security in the Internet of Things." IEEE Communications Surveys & Tutorials 23.2 (2021): 1020-1047.

[18] Ahad, Mohd Abdul, et al. "IoT data management—Security aspects of information linkage in IoT systems." Princi-

ples of internet of things (IoT) ecosystem: Insight paradigm (2020): 439-464.
[19] Russell, Brian, and Drew Van Duren. Practical internet of things security. Packt Publishing Ltd, 2016.
[20] Buyya, Rajkumar, and Amir Vahid Dastjerdi, eds. Internet of Things: Principles and paradigms. Elsevier, 2016.
[21] Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014.
[22] Xiao, Liang, et al. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?." IEEE Signal Processing Magazine 35.5 (2018): 41-49.
[23] Rizvi, Syed, et al. "Securing the internet of things (IoT): A security taxonomy for IoT." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.
[24] Uprety, Aashma, and Danda B. Rawat. "Reinforcement learning for iot security: A comprehensive survey." IEEE Internet of Things Journal 8.11 (2020): 8693-8706.
[25] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.