

IoT Security Frameworks for Protecting Connected Devices

José M. del Álamo

Associate Professor, Polytechnic University of Madrid, Spain

Abstract

The rapid expansion of Internet of Things (IoT) technologies has created interconnected environments in which sensors, smart appliances, industrial devices, medical equipment, vehicles, and digital platforms continuously exchange information. While connected devices provide significant opportunities for automation, monitoring, and intelligent services, their distributed architecture also introduces substantial cybersecurity risks. This study examines IoT security frameworks for protecting connected devices, with emphasis on device authentication, authorization, secure communication, data protection, access control, vulnerability management, network security, threat detection, and security lifecycle management.

A qualitative descriptive and conceptual research design was adopted using secondary academic literature. The analysis indicates that effective IoT security requires a multilayered framework extending from device hardware and firmware to communication networks, gateways, cloud platforms, and applications. Authentication and authorization mechanisms can restrict unauthorized access, while encryption can protect information during transmission and storage. Secure software updates and vulnerability management can reduce risks associated with outdated device components.

Network monitoring and intelligent threat detection can provide additional protection against emerging attacks. However, resource constraints, heterogeneous devices, interoperability limitations, inadequate security standards, privacy concerns, and large-scale deployment complexity continue to challenge IoT security. Recent research also emphasizes the absence of comprehensive security approaches covering all IoT layers and the need for stronger assessment and benchmarking mechanisms. The study concludes that secure-by-design architectures, lifecycle-based protection, standardized security requirements, adaptive monitoring, and risk-based security management are essential for protecting future connected-device ecosystems.

Keywords: Internet of Things, IoT Security, Connected Devices, Cybersecurity, Authentication, Authorization, Encryption, Access Control, Network Security, Security Frameworks, Vulnerability Management.

1. Introduction

The Internet of Things has transformed traditional computing environments by connecting physical objects to digital networks and enabling them to collect, process, and exchange information. Connected devices now operate across smart homes, healthcare, transportation, manufacturing, energy systems, agriculture, and public infrastructure. The increasing number and diversity of IoT devices have created

new opportunities for automation and intelligent services. At the same time, interconnected devices expand the potential attack surface and create security requirements that differ from those of conventional computing systems. IoT security has therefore become an important area of technological and academic research.

IoT environments typically involve multiple layers, including sensing devices, communication networks, gateways, edge platforms, cloud infrastructures, and application services. Each layer can introduce different security vulnerabilities. Resource-constrained devices may have limited processing power, memory, and energy for implementing sophisticated security mechanisms. Communication channels may be exposed to interception or manipulation, while gateways can become important targets because they connect large groups of devices with broader networks. Consequently, protecting an IoT ecosystem requires coordinated security controls across multiple architectural layers rather than relying on a single defensive mechanism.

Device authentication and authorization represent fundamental components of IoT security frameworks. Connected devices should be able to establish trusted identities and communicate only with authorized systems. Cryptographic techniques can protect information from unauthorized disclosure and manipulation, while access-control mechanisms can restrict device and application privileges. Secure software development, firmware protection, vulnerability assessment, and controlled software updates are also essential because vulnerabilities can remain active throughout the operational life of connected devices. NIST guidance specifically emphasizes establishing cybersecurity requirements for IoT products and identifying device capabilities needed to support security controls.

The increasing heterogeneity of IoT ecosystems creates additional security challenges. Devices from different manufacturers may use different operating systems, communication protocols, security mechanisms, and data formats. This diversity can make it difficult to establish consistent security policies across complete IoT environments. Research on IoT frameworks has identified differences in security architectures and approaches across major platforms, while systematic reviews have emphasized security threats and countermeasures across multiple IoT layers.

Modern IoT security frameworks increasingly incorporate intelligent monitoring, risk assessment, and adaptive security mechanisms. Security analytics can examine network behavior and device activity to identify unusual patterns, while machine-learning approaches can support threat detection and classification. Risk assessment frameworks can help organizations identify vulnerabilities, evaluate potential impacts, and prioritize security controls. Recent research has emphasized the importance of structured IoT risk management and assessment because connected systems increasingly operate in critical domains such as healthcare, transportation, and energy.

Despite technological progress, IoT security remains affected by device constraints, inconsistent security practices, weak authentication, outdated software, privacy risks, inadequate monitoring, and limited security benchmarking. Recent systematic research indicates that IoT systems still lack comprehensive security assessment approaches covering all layers and that standardized benchmarks for evaluating IoT security solutions remain limited. These concerns demonstrate the need for security frameworks that integrate preventive, detective, and responsive mechanisms throughout the device lifecycle.

This study examines IoT security frameworks for protecting connected devices by analyzing authentication, authorization, encryption, access control, secure communication, vulnerability management, software updates, network monitoring, threat detection, and lifecycle security. The study also evaluates implementation challenges and future research directions. The central focus is the development of a multilayered security perspective in which device-level protection is integrated with network, gateway, edge, cloud, and application security. Such an approach can contribute to more resilient and trustworthy IoT ecosystems.

2. Objectives of the Study

Primary Objective

The primary objective of this study is to examine IoT security frameworks for protecting connected devices by analyzing authentication, authorization, encryption, access control, secure communication, vulnerability management, network monitoring, threat detection, and lifecycle security.

The study seeks to understand how integrated security mechanisms can reduce vulnerabilities and strengthen the confidentiality, integrity, availability, privacy, reliability, and resilience of connected-device ecosystems.

2.1 Examination of IoT Security Framework Components

The first objective is to examine the principal components of IoT security frameworks, including device authentication, authorization, encryption, access control, secure communication, firmware protection, vulnerability management, and security monitoring.

The study evaluates how these mechanisms operate across device, network, gateway, edge, cloud, and application layers. Understanding these components can support the development of comprehensive security architectures capable of addressing diverse IoT threats.

2.2 Assessment of Connected-Device Protection Mechanisms

The second objective is to assess mechanisms used to protect connected devices throughout their operational lifecycle. The study examines secure device configuration, identity management, software updates, access policies, cryptographic protection, network monitoring, and threat detection.

Particular attention is given to how these mechanisms can address unauthorized access, data interception, malicious manipulation, software vulnerabilities, and abnormal device behavior across heterogeneous IoT environments.

2.3 Identification of IoT Security Challenges

The third objective is to identify challenges associated with implementing IoT security frameworks, including resource constraints, device heterogeneity, scalability, interoperability, privacy, outdated firmware, weak security practices, and limited security benchmarking.

The study evaluates how these challenges affect security effectiveness and operational reliability. Identifying these limitations can support future development of adaptive, standardized, scalable, and lifecycle-oriented security frameworks for connected devices.

3. Review of Literature

3.1 IoT Security Architecture and Frameworks

Roman et al. (2013) emphasized that distributed IoT environments introduce security and privacy challenges because devices operate across interconnected and heterogeneous infrastructures. Their work highlighted the importance of security mechanisms capable of addressing distributed architectures rather than treating IoT as a conventional network. Similarly, Sicari et al. (2015) examined security, privacy, and trust as interconnected requirements for IoT systems. These studies establish the importance of integrated security frameworks that address multiple technological and organizational dimensions.

Noor and Hassan (2019) reviewed IoT security research and emphasized the importance of protecting hardware, networks, data, infrastructure, and users. Their analysis demonstrates that IoT security encompasses confidentiality, privacy, integrity, authentication, and availability. Later framework-focused research compared multiple IoT platforms and identified differences in their security architectures and mechanisms. Such findings indicate that security frameworks must accommodate different device capabilities, communication technologies, application requirements, and operational environments rather than depending on a universal security mechanism.

3.2 Authentication, Encryption, and Access Control

Authentication is a fundamental mechanism for establishing trust between IoT devices, users, gateways, and services. Recent systematic research on IoT authentication has examined different authentication and key-agreement approaches according to security strength, computational requirements, communication costs, and energy consumption. This is particularly important because many IoT devices operate with limited resources. Effective authentication mechanisms must therefore provide strong protection without imposing excessive computational or energy requirements on constrained devices.

Encryption and access control provide complementary protection by securing information and limiting authorized operations. Encryption can protect data while it is transmitted across potentially exposed communication networks, while access-control policies can determine which devices or users may access particular resources.

However, IoT environments require lightweight and adaptable mechanisms because device capabilities vary substantially. Security frameworks should therefore balance protection requirements with device limitations, network performance, interoperability, and application-specific security needs.

3.3 Risk Management and Security Assessment

Risk assessment has become increasingly important as IoT technologies expand into critical application domains. Recent research has developed taxonomies for IoT security risk management, analysis, and evaluation, emphasizing systematic identification and prioritization of security risks. Risk-based approaches can help organizations determine which devices, interfaces, data flows, and services require stronger protection. They can also support the selection of appropriate controls according to potential threats and operational consequences.

Security assessment research further indicates that IoT environments require comprehensive evaluation mechanisms covering multiple architectural layers. A 2026 systematic review identified limitations in existing IoT security assessment practices, including the lack of comprehensive

frameworks, standardized benchmarks, and sufficient attention to gateway security. These findings indicate that security should not be evaluated only at the individual-device level. Instead, assessment should consider interactions among devices, gateways, networks, applications, and cloud or edge services.

4. Research Methodology

4.1 Research Design

This study adopted a qualitative descriptive and conceptual research design to examine IoT security frameworks for protecting connected devices. The study relied on secondary academic literature addressing IoT security, authentication, encryption, access control, network protection, risk assessment, vulnerability management, security monitoring, and device lifecycle management. The design was selected to synthesize established knowledge and identify relationships among security mechanisms applicable to heterogeneous IoT environments.

The conceptual framework was organized around six dimensions: device security, identity and access management, communication security, network and gateway protection, data and application security, and lifecycle management. These dimensions were examined in relation to confidentiality, integrity, availability, privacy, reliability, and resilience. Risk assessment and security monitoring were considered cross-cutting elements because they can support continuous identification and management of vulnerabilities across connected-device ecosystems.

4.2 Data Collection

Secondary information was collected from peer-reviewed journal articles, academic publications, systematic reviews, and authoritative cybersecurity guidance concerning IoT security. The literature included research on IoT security architectures, authentication mechanisms, cryptographic approaches, network security, security frameworks, risk assessment, device cybersecurity requirements, and security assessment methodologies. Sources were selected according to their relevance to the study objectives and their contribution to understanding connected-device protection.

The collected literature was categorized according to security functions and IoT architectural layers. Device-level security research was examined separately from communication, gateway, cloud, and application protection. Studies concerning authentication, encryption, access control, vulnerability management, and threat detection were also grouped according to their primary security function. This categorization provided a structured basis for comparing security mechanisms and identifying recurring challenges affecting IoT protection.

4.3 Data Analysis

The collected literature was analyzed using thematic analysis. Major themes included device identity, authentication, authorization, encryption, access control, secure communication, firmware protection, vulnerability management, network monitoring, threat detection, risk assessment, privacy, and lifecycle security. Each theme was examined according to its contribution to protecting connected devices and maintaining secure communication and information exchange.

A comparative synthesis was subsequently conducted to identify relationships among security layers. Device security was considered the foundation, while authentication and authorization established trusted access.

Communication security protected information exchanges, and gateway and network security addressed broader infrastructure risks. Cloud and application security were considered higher-level protection mechanisms. Lifecycle management was evaluated as an overarching process supporting secure configuration, updates, monitoring, assessment, and retirement of connected devices.

5. Analysis

5.1 Core Components of IoT Security Frameworks

A comprehensive IoT security framework should integrate multiple protection mechanisms across connected-device architectures.

Table 1: Core Components of IoT Security Frameworks

Security Component	Primary Function	Protection Contribution
Device Identity	Establish device trust	Prevents unauthorized devices
Authentication	Verify identity	Restricts illegitimate access
Authorization	Define permissions	Controls resource usage
Encryption	Protect information	Supports confidentiality
Access Control	Regulate activities	Limits unauthorized operations
Secure Communication	Protect data exchange	Reduces interception risks
Vulnerability Management	Identify weaknesses	Reduces exploitable flaws
Security Monitoring	Observe activities	Supports threat detection
Firmware Updates	Maintain software security	Addresses known vulnerabilities
Incident Response	Manage security events	Supports recovery and resilience

The analysis demonstrates that effective IoT protection requires multiple security controls operating together. Device identity and authentication establish trust, while authorization and access control restrict activities. Encryption and secure communication protect information exchanges. Vulnerability management and firmware updates address weaknesses over the device lifecycle. Security monitoring provides visibility into abnormal behavior, while incident-response mechanisms support recovery. NIST

guidance similarly emphasizes device cybersecurity capabilities and organizational supporting capabilities as components of IoT security requirements.

5.2 IoT Security Protection Across Architectural Layers

IoT security controls must operate across different layers of the connected-device ecosystem.

Table 2: Layer-Based IoT Security Protection

IoT Layer	Major Security Requirement	Example Protection
Device Layer	Device integrity	Secure boot and firmware protection
Connectivity Layer	Communication security	Encryption and secure protocols
Gateway Layer	Traffic and device control	Authentication and monitoring
Edge Layer	Local processing protection	Access control and isolation
Cloud Layer	Data and service security	Encryption and identity management
Application Layer	User and service protection	Authorization and secure interfaces
Management Layer	Lifecycle security	Updates and vulnerability management

The layer-based analysis indicates that IoT security cannot depend exclusively on device-level controls. Connected devices communicate through gateways, networks, edge systems, cloud services, and applications, each of which can introduce security risks.

Systematic literature has emphasized the need to examine security threats and countermeasures across IoT architecture layers. Recent assessment research also identifies the need for broader security evaluation and stronger attention to gateway security.

6. Discussion

IoT security frameworks must address the distributed and heterogeneous nature of connected-device environments. A device may be physically constrained while simultaneously communicating with gateways, cloud services, and other devices. Consequently, a weakness in one component can influence the broader ecosystem. Security should therefore be implemented as a multilayered architecture rather than as an isolated device function. Authentication, encryption, access control, monitoring, and vulnerability management should operate together to establish a stronger security posture.

Device identity and authentication represent essential foundations for protecting connected environments. Unauthorized devices should not be permitted to join trusted networks or access sensitive services. Similarly, authorization mechanisms should ensure that legitimate devices receive only the

permissions required for their functions. Recent authentication research highlights the need to balance security strength with computational and communication requirements because IoT devices can have limited resources. Lightweight but robust security mechanisms are therefore particularly important for large-scale IoT deployments.

Lifecycle-oriented security is equally important because connected devices may remain operational for extended periods. Security weaknesses can emerge after deployment as vulnerabilities are discovered or attack techniques evolve. Secure firmware updates, vulnerability assessment, configuration management, continuous monitoring, and appropriate device retirement procedures can help maintain protection over time. NIST guidance emphasizes establishing cybersecurity requirements for IoT products and considering them within broader risk-management processes.

7. Challenges

7.1 Resource Constraints and Device Limitations

Many IoT devices operate with limited processing capacity, memory, storage, bandwidth, and battery power. These limitations can restrict the use of computationally intensive encryption, authentication, monitoring, and threat-detection mechanisms. Security solutions designed for conventional computers may therefore create excessive overhead when applied directly to constrained devices. Research has repeatedly identified resource limitations as an important challenge for implementing strong security mechanisms across large and diverse IoT environments.

Device limitations also affect the ability to maintain security throughout the operational lifecycle. Some devices may have limited mechanisms for secure software updates, vulnerability scanning, logging, or local security monitoring. Battery-powered devices may reduce security activities to preserve operational lifetime. Consequently, IoT security frameworks must balance protection requirements with device capabilities. Lightweight cryptographic mechanisms, efficient authentication, adaptive monitoring, and hardware-supported security can help provide stronger protection without creating excessive computational or energy requirements.

7.2 Device Heterogeneity and Interoperability

IoT ecosystems contain devices manufactured by different organizations and designed for different applications. These devices may use different operating systems, communication protocols, security mechanisms, and data formats. Such heterogeneity can make it difficult to apply consistent security policies across the entire environment. Research on IoT frameworks has shown that different platforms can adopt different security architectures and approaches, demonstrating the complexity of achieving consistent protection.

Interoperability problems can also affect security monitoring and incident response. A security platform may not receive standardized information from every device, making it difficult to identify threats consistently. Different authentication and communication mechanisms can further complicate centralized security management. Standardized interfaces, common security requirements, interoperable protocols, and clearly defined device-security capabilities can improve integration. However, security frameworks must remain flexible enough to accommodate different device types, application requirements, and technological constraints.

7.3 Scalability and Security Management

Large IoT deployments may contain thousands or millions of connected devices, making manual security management impractical. Organizations must manage device identities, credentials, access permissions, firmware versions, vulnerabilities, security policies, and network behavior across extensive infrastructures. As device populations increase, centralized approaches may experience processing and management limitations. Scalable identity management, automated configuration, distributed monitoring, and risk-based prioritization are therefore necessary for maintaining effective protection.

Security assessment also becomes more difficult as IoT ecosystems expand. Recent research indicates that comprehensive assessment frameworks and standardized security benchmarks remain limited, making it difficult to compare security solutions consistently. Large-scale IoT security management should therefore incorporate automated assessment, continuous monitoring, standardized metrics, and lifecycle-based evaluation. Such approaches can help organizations identify high-risk devices and prioritize security resources according to potential threats and operational impact.

7.4 Privacy and Emerging Threats

IoT devices can collect information about physical environments, user activities, locations, behaviors, and operational processes. Improper access or processing of such information can create significant privacy concerns. Security frameworks must therefore consider not only protection from unauthorized access but also appropriate data collection, storage, processing, and sharing. Privacy-preserving approaches, data minimization, encryption, access controls, and transparent information-management policies can reduce privacy risks.

The threat environment also continues to evolve as attackers develop new techniques for targeting connected systems. Emerging risks may involve compromised firmware, supply-chain vulnerabilities, gateway attacks, credential theft, malicious updates, and coordinated attacks across multiple devices. Recent research emphasizes the need for continuous IoT security assessment because existing controls may not adequately address emerging vulnerabilities. Adaptive security monitoring and regular reassessment are therefore necessary to maintain protection against changing threats.

8. Future Research

Future research should focus on developing comprehensive IoT security frameworks that integrate device, network, gateway, edge, cloud, and application protection. Research should investigate lightweight authentication, efficient cryptography, secure boot mechanisms, automated vulnerability management, and adaptive access control for resource-constrained devices. Greater attention should also be given to standardized security benchmarks that allow organizations to evaluate and compare IoT security solutions consistently. Recent research indicates that standardized assessment remains an important gap.

Further research should examine artificial intelligence for adaptive threat detection and automated security management. Machine-learning systems could analyze device behavior, network traffic, and security events to identify abnormal activities. Research should also investigate privacy-preserving security analytics, decentralized security architectures, zero-trust approaches, secure device lifecycle management, and resilient gateway protection. Future frameworks should be evaluated under

realistic large-scale conditions and should measure security effectiveness alongside computational overhead, energy consumption, interoperability, scalability, and operational reliability.

9. Conclusion

IoT security frameworks are essential for protecting the rapidly expanding ecosystem of connected devices. IoT environments contain sensors, smart devices, gateways, networks, edge platforms, cloud systems, and applications that continuously exchange information. This interconnected structure creates significant benefits but also introduces multiple security vulnerabilities. Effective protection therefore requires coordinated mechanisms across architectural layers rather than relying on isolated security controls.

The analysis demonstrates that authentication, authorization, encryption, access control, secure communication, vulnerability management, firmware protection, monitoring, and incident response are important components of comprehensive IoT security. These mechanisms perform different but interconnected functions. Authentication establishes trusted identities, authorization controls permissions, encryption protects information, and monitoring provides visibility into suspicious activities. Lifecycle security ensures that protection continues from device deployment through maintenance and eventual retirement.

However, resource constraints, device heterogeneity, interoperability problems, scalability requirements, privacy concerns, and evolving threats continue to limit IoT security effectiveness. Recent research indicates that comprehensive assessment frameworks and standardized security benchmarks remain insufficient, particularly across complex IoT environments. Addressing these limitations requires stronger standardization, automated security management, risk-based assessment, and adaptive protection mechanisms.

Overall, IoT security should be approached as a continuous and multilayered process. Future connected-device ecosystems require security-by-design principles, lifecycle-based management, strong identity protection, secure communication, intelligent monitoring, and standardized evaluation. NIST guidance and contemporary research emphasize the importance of establishing explicit cybersecurity requirements and incorporating IoT products into broader risk-management processes. Such approaches can improve the confidentiality, integrity, availability, privacy, reliability, and resilience of increasingly interconnected IoT environments.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
2. Weber, R. H. (2010). Internet of Things—New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23–30. <https://doi.org/10.1016/j.clsr.2009.11.008>
3. Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *Computer*, 44(9), 51–58. <https://doi.org/10.1109/MC.2011.291>
4. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497–1516. <https://doi.org/10.1016/j.adhoc.2012.02.016>

5. Heer, T., Garcia-Morchon, O., Seitz, L., Sturek, D., & Schmitt, C. (2011). Security challenges in the IP-based Internet of Things. *Wireless Personal Communications*, 61, 527–542. <https://doi.org/10.1007/s11277-011-0383-7>
6. Garcia-Morchon, O., Kumar, S., Sethi, M., Keoh, S. L., & Hummen, R. (2014). *Security considerations in the IP-based Internet of Things*. Internet Engineering Task Force.
7. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>
8. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, 17(3), 1294–1312. <https://doi.org/10.1109/COMST.2015.2388550>
9. Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, 17–31. <https://doi.org/10.1016/j.adhoc.2015.01.006>
10. Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. In *Proceedings of the 52nd Annual Design Automation Conference* (pp. 1–6). ACM. <https://doi.org/10.1145/2744769.2747942>
11. Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. *Internet Research*, 26(2), 337–359. <https://doi.org/10.1108/IntR-07-2014-0173>
12. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), 269–284. <https://doi.org/10.1109/JIOT.2015.2460333>
13. Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, 112, 237–262. <https://doi.org/10.1016/j.comnet.2016.11.007>
14. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for Internet of Things: A comprehensive survey. *Security and Communication Networks*, 2017, Article 6562953. <https://doi.org/10.1155/2017/6562953>
15. Atwady, Y., & Hammoudeh, M. (2017). A survey on authentication techniques for the Internet of Things. In *Proceedings of the International Conference on Future Networks and Distributed Systems*. ACM. <https://doi.org/10.1145/3102304.3102312>
16. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10–28. <https://doi.org/10.1016/j.jnca.2017.04.002>
17. Abomhara, M., & Køien, G. M. (2014). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 4(1), 65–88.
18. Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, 4(2), 118–137. <https://doi.org/10.1016/j.dcan.2017.04.003>
19. Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A survey of cybersecurity certification for the Internet of Things. *ACM Computing Surveys*, 53(6), Article 115, 1–36. <https://doi.org/10.1145/3410160>