Science Archives (ISSN:2582-6697)

Journal homepage: www.sciencearchives.org

Original Research Article

https://doi.org/10.47587/SA.2021.2416

Exploring Interoperability and Security Standards in the Internet of Things: An In-Depth Survey

Neetu Singh✉ and Ankur Rohilla

Department of Computer Application, Department of Computer Science
Shri Ram College, Muzaffarnagar, India

Received: Oct 13, 2021/ Revised: Nov 04, 2021/Accepted: Nov 05, 2021

Abstract

Recent advancements in Internet of Things (IoT) research underscore the significance of interoperability and security across diverse sectors like smart cities, homes, factories, and healthcare, highlighting the intricate interconnection among users, devices, and information resources. While existing studies tend to address specific challenges in IoT implementation, a comprehensive solution encompassing interoperability and security remains elusive. International standards serve as a crucial framework for achieving these goals, facilitating streamlined system development and management. Despite ongoing efforts by standard organizations to develop IoT-related standards, there exists a gap in the consolidated examination of interoperability- and security-related standards. This paper fills that gap by conducting a systematic literature review, analyzing international standards relevant to IoT interoperability and security, and identifying remaining challenges in this domain. Consequently, the adoption of international standards becomes imperative to surmount the hurdles in IoT. Moreover, international standard organizations are actively formulating IoT-related standards, potentially offering solutions to interoperability and security challenges. Nevertheless, there remains a gap in research focusing on standards pertaining to interoperability and security. Thus, this paper directs its attention to international standards concerning interoperability and security within IoT environments. Additionally, we examine standard organizations engaged in developing IoT standards. Through a systematic literature review, we analyze international standards and address any lingering challenges associated with interoperability and security in IoT standards.

Keywords: Internet of Things (IoT), interoperability, standards, protocols, compatibility, integration

Introduction

The Internet of Things (IoT) has emerged as a transformative paradigm, connecting a myriad of devices, sensors, and systems to enable unprecedented levels of automation, efficiency, and convenience across diverse domains such as smart cities, healthcare, manufacturing, and transportation. This interconnected network of devices holds immense potential to revolutionize how we interact with the physical world, but it also presents unique challenges, particularly concerning interoperability and security. Interoperability, the ability of diverse devices and systems to communicate and work together seamlessly, is essential for realizing the full potential of IoT deployments. Without interoperability, devices from different manufacturers may struggle to exchange (Atzori et al., 2010) data or execute tasks, leading to fragmented ecosystems and limited functionality. Moreover, the proliferation of IoT devices introduces new security vulnerabilities, as these devices often collect and transmit sensitive data over networks, making them potential targets for cyberattacks. In response to these challenges, various standards and protocols have been developed to promote interoperability and enhance the security of IoT deployments. These standards govern communication protocols, data formats, authentication mechanisms, encryption techniques, and access control policies, among other aspects. However, navigating this complex landscape of standards can be daunting for researchers, practitioners, and policymakers alike.

This paper presents an in-depth survey aimed at exploring the interoperability and security standards landscape in the Internet of Things. By systematically reviewing existing literature, analyzing international standards, and synthesizing key findings, we aim to provide a comprehensive overview of the current state-of-the-art in IoT standards. Through this survey, we seek to elucidate the challenges, trends, and emerging best practices in interoperability and security standards for IoT deployments. By shedding light on the existing standards and identifying areas for improvement, this research contributes to the ongoing efforts to enhance the interoperability, security, and resilience of IoT ecosystems. Furthermore, it aims to inform future research directions, policy initiatives, and industry practices to foster a more robust and trustworthy IoT infrastructure. In the subsequent sections of this paper, we will delve into the methodology used for conducting the survey, discuss the key findings and insights derived from our analysis, and conclude with recommendations for advancing the state of IoT standards to meet the evolving needs of the interconnected world (Gershenfeld et al., 2004).

Interoperability Standards in IoT

Interoperability standards in IoT encompass a set of guidelines, protocols, and specifications that enable different devices, systems, and applications to communicate and work together seamlessly within the Internet of Things ecosystem. These standards are crucial because IoT environments often consist of a diverse range of devices from various manufacturers, running on different platforms, and utilizing different communication protocols. The purpose of interoperability standards is to ensure that these heterogeneous devices can exchange data and interact with each other effectively, regardless of their differences. This allows for the creation of cohesive IoT solutions where devices can collaborate to perform complex tasks, share information, and respond to changing conditions in real-time.

Interoperability standards in IoT cover various aspects of communication, data exchange, security, and device management. They define common protocols and data formats that devices must adhere to, specify methods for authentication and access control, and provide guidelines for device discovery, configuration, and interoperability testing. By adhering to interoperability standards, IoT devices can seamlessly integrate into larger (Kamilaris et al., 2016) IoT ecosystems, enabling the creation of scalable, flexible, and interoperable solutions. This interoperability fosters innovation, promotes competition, and accelerates the adoption of IoT technology across industries such as smart cities, healthcare, manufacturing, agriculture, and transportation.

Security Standards in IoT

Security standards in IoT refer to the established protocols, frameworks, and guidelines designed to safeguard IoT devices, networks, and data from unauthorized access, malicious attacks, and data breaches. With the proliferation of interconnected devices in IoT ecosystems, security standards are essential to mitigate the inherent risks and vulnerabilities associated with IoT deployments (Yu et al., 2016). The primary goals of security standards in IoT are to protect the confidentiality, integrity, and availability of data, as well as ensure the privacy and trustworthiness of IoT systems. These standards address various aspects of security, including authentication, encryption, access control, device management, and secure communication protocols. Authentication standards in IoT establish mechanisms for verifying the identity of devices, users, and applications within the IoT ecosystem. This helps prevent unauthorized access and ensures that only legitimate entities can interact with IoT devices and access sensitive data. Encryption standards specify methods for encrypting data transmitted between IoT devices and networks, as well as for storing data securely on IoT devices. By encrypting data, security standards help prevent eavesdropping, tampering, and data theft, ensuring the confidentiality and integrity of information exchanged in IoT environments.

Access control standards define policies and procedures for controlling access to IoT devices, networks, and data based on user roles, privileges, and permissions. This helps enforce least privilege principles and restricts access to authorized entities, reducing the risk of unauthorized actions and insider threats. Device management standards outline best practices for securely provisioning, configuring, updating, and decommissioning IoT devices throughout their lifecycle. This ensures that devices are properly managed and maintained, minimizing the risk of security vulnerabilities and ensuring the overall security posture of IoT deployments. Secure communication protocols, such as Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Message Queuing Telemetry Transport (MQTT) with Secure Sockets Layer (SSL), establish secure channels for transmitting data between IoT devices and networks. These protocols encrypt data in transit, authenticate communicating parties, and provide integrity protection, thereby ensuring the secure exchange of information in IoT environments. Overall, security standards in IoT are essential for addressing the diverse security challenges and risks associated with interconnected devices. By adhering to these standards, IoT stakeholders can implement robust security measures to protect against cyber threats, safeguard sensitive data, and build trust in IoT systems (Hatcher et al., 2018).

Security Standards in IoT

Security standards in IoT refer to the established protocols, frameworks, and guidelines designed to safeguard IoT devices, networks, and data from unauthorized access, malicious attacks, and data breaches. With the proliferation of interconnected devices in IoT ecosystems, security standards are essential to mitigate the inherent risks and vulnerabilities associated with IoT deployments.

The primary goals of security standards in IoT are to protect the confidentiality, integrity, and availability of data, as well as ensure the privacy and trustworthiness of IoT systems. These standards address various aspects of security, including authentication, encryption, access control, device management, and secure communication protocols. Authentication standards in IoT establish mechanisms for verifying the identity of devices, users, and applications within the IoT ecosystem. This helps prevent unauthorized access and ensures that only legitimate entities can interact with IoT devices and access sensitive data.

Encryption standards specify methods for encrypting data transmitted between IoT devices and networks, as well as for storing data securely on IoT devices. By encrypting data, security standards help prevent eavesdropping, tampering, and data theft, ensuring the confidentiality and integrity of information exchanged in IoT environments. Access control standards define policies and procedures for controlling access to IoT devices, networks, and data based on user roles, privileges, and permissions. This helps enforce least privilege principles and restricts access to authorized entities, reducing the risk of unauthorized actions and insider threats. Device management standards outline best practices for securely provisioning, configuring, updating, and decommissioning IoT devices throughout their lifecycle. This ensures that devices are properly managed and maintained, minimizing the risk of security vulnerabilities and ensuring the overall security posture of IoT deployments. Secure communication protocols, such as Transport Layer Security (TLS) [Dehghantanha @ 2016], Datagram Transport Layer Security (DTLS), and Message Queuing Telemetry Transport (MQTT) with Secure Sockets Layer (SSL), establish secure channels for transmitting data between IoT devices and networks. These protocols encrypt data in transit, authenticate communicating parties, and provide integrity protection, thereby ensuring the secure exchange of information in IoT environments.

Methodology

Literature Review

Conducted a comprehensive review of existing literature, including academic papers, industry reports, technical specifications, and standardization documents related to IoT interoperability and security standards. Identified relevant research articles, surveys, case studies, and white papers that provided insights into the current state-of-the-art in IoT standards.

Standardization Bodies and Organizations

Identified and reviewed the activities of major standardization bodies and organizations involved in developing IoT interoperability and security standards, such as IEEE, ISO, IETF, ITU-T, and industry consortia. Explored the standards development processes, participation requirements, and collaboration initiatives within these organizations.

Standard Identification and Classification

Compiled a comprehensive list of interoperability and security standards relevant to the IoT domain, including communication protocols, data formats, authentication mechanisms, encryption techniques, and access control policies. Classified the identified standards based on their functionality, applicability, and domain-specific requirements.

Data Collection

Gathered relevant data and documentation for each identified standard, including specifications, technical reports, implementation guides, and case studies. Collected information on the features, capabilities, limitations, and adoption status of each standard from authoritative sources.

Data Analysis and Synthesis

Analyzed the collected data to identify common themes, trends, and patterns across different interoperability and security standards. Compared and contrasted the features, strengths, and weaknesses of various standards, highlighting their implications for IoT deployments. Synthesized key findings and insights from the analysis, providing a coherent narrative that contextualized the landscape of IoT interoperability and security standards (Noura et al., 2016).

Evaluation and Validation

Evaluated the effectiveness and suitability of identified standards in addressing interoperability and security challenges in real-world IoT scenarios. Validated the survey findings through expert reviews, stakeholder consultations, and peer feedback to ensure accuracy, relevance, and credibility.

Recommendations and Future Directions

Provided recommendations for stakeholders, including IoT developers, system integrators, policymakers, and standardization bodies, on selecting and implementing interoperability and security standards. Identified gaps, challenges, and emerging trends in the field of IoT standards and suggested potential areas for future research, development, and standardization efforts.

Report Writing

Documented the survey methodology, findings, analysis, and recommendations in a comprehensive research paper format. Clearly presented the methodology steps, data sources, analysis techniques, and validation procedures to enhance the transparency and reproducibility of the survey results.

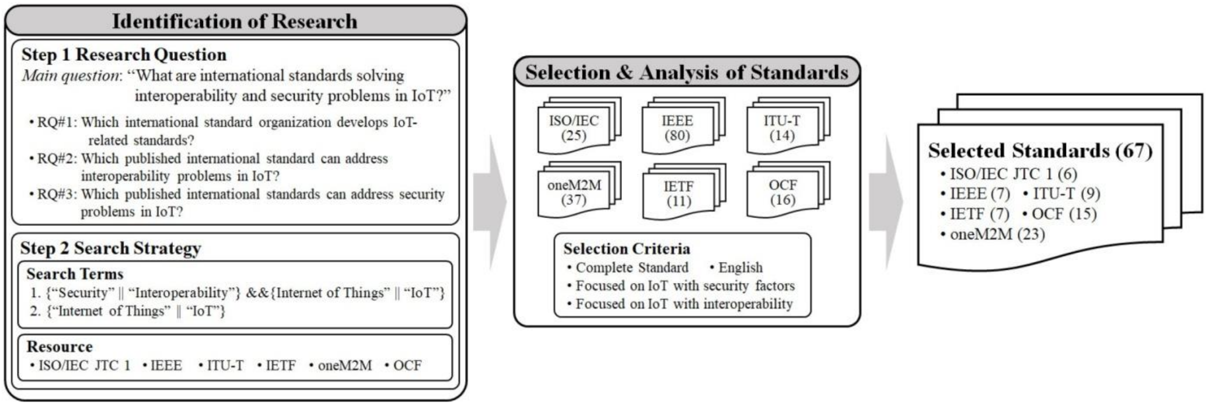
Identification of Research
Step 1 Research Question
Main question: "What are international standards solving interoperability and security problems in IoT?"
• RQ#1: Which international standard organization develops IoT-related standards?
• RQ#2: Which published international standard can address interoperability problems in IoT?
• RQ#3: Which published international standards can address security problems in IoT?
Step 2 Search Strategy
Search Terms
1. {"Security" ‖ "Interoperability"} &&{Internet of Things" ‖ "IoT"}
2. {"Internet of Things" ‖ "IoT"}
Resource
• ISO/IEC JTC 1 • IEEE • ITU-T • IETF • oneM2M • OCF
Selection & Analysis of Standards
ISO/IEC (25)
IEEE (80)
ITU-T (14)
oneM2M (37)
IETF (11)
OCF (16)
Selection Criteria
• Complete Standard • English
• Focused on IoT with security factors
• Focused on IoT with interoperability
Selected Standards (67)
• ISO/IEC JTC 1 (6)
• IEEE (7) • ITU-T (9)
• IETF (7) • OCF (15)
• oneM2M (23)

Fig. 1 Summary of procedure used for the literature review to select relevant internal standards.

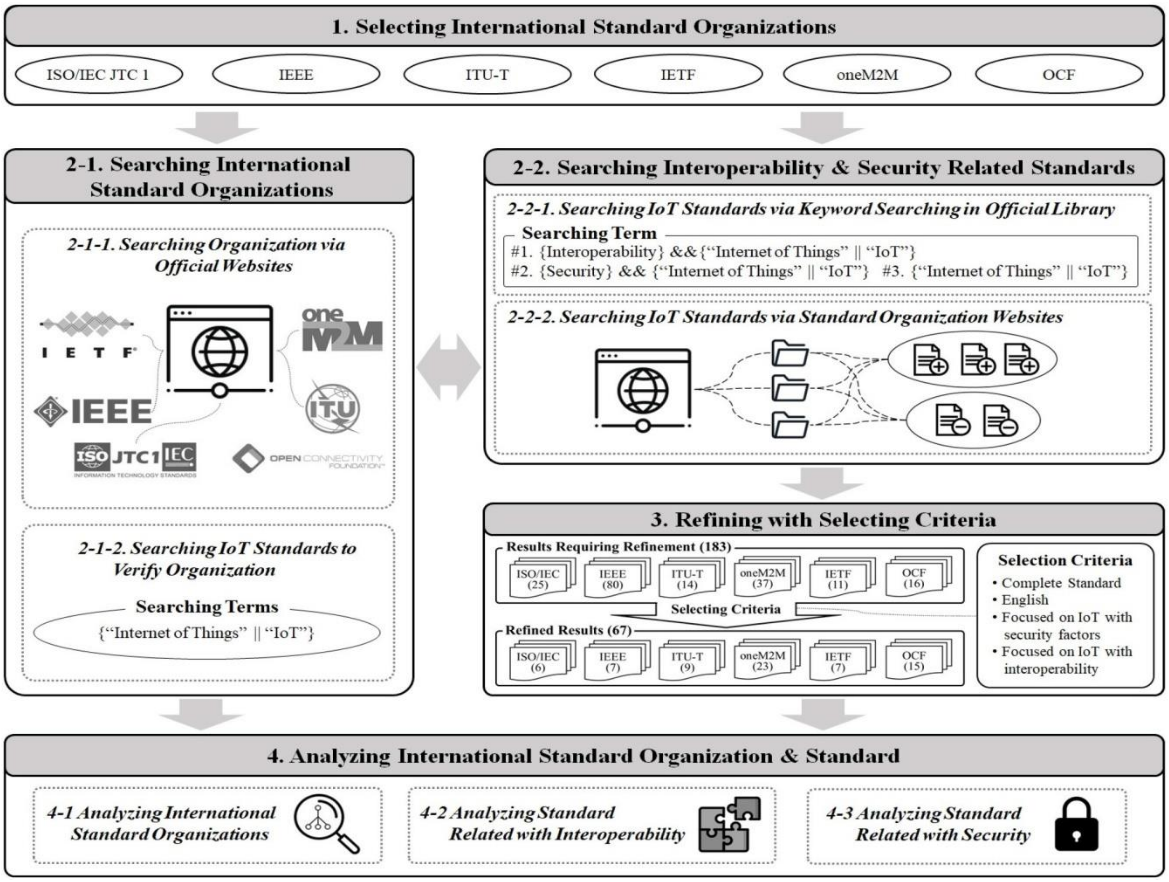
1. Selecting International Standard Organizations
ISO/IEC JTC 1
IEEE
ITU-T
IETF
oneM2M
OCF
2-1. Searching International Standard Organizations
2-1-1. Searching Organization via Official Websites
IETF
IEEE
ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS
one M2M
ITU
OPEN CONNECTIVITY FOUNDATION
2-1-2. Searching IoT Standards to Verify Organization
Searching Terms
{"Internet of Things" ‖ "IoT"}
2-2. Searching Interoperability & Security Related Standards
2-2-1. Searching IoT Standards via Keyword Searching in Official Library
Searching Term
#1. {Interoperability} &&{"Internet of Things" ‖ "IoT"}
#2. {Security} && {"Internet of Things" ‖ "IoT"} #3. {"Internet of Things" ‖ "IoT"}
2-2-2. Searching IoT Standards via Standard Organization Websites
3. Refining with Selecting Criteria
Results Requiring Refinement (183)
ISO/IEC (25)
IEEE (80)
ITU-T (14)
oneM2M (37)
IETF (11)
OCF (16)
Selecting Criteria
Refined Results (67)
ISO/IEC (6)
IEEE (7)
ITU-T (9)
oneM2M (23)
IETF (7)
OCF (15)
Selection Criteria
• Complete Standard
• English
• Focused on IoT with security factors
• Focused on IoT with interoperability
4. Analyzing International Standard Organization & Standard
4-1 Analyzing International Standard Organizations
4-2 Analyzing Standard Related with Interoperability
4-3 Analyzing Standard Related with Security

Fig. 2 Detailed process of survey

Identification of Interoperability Standards

The survey identified a comprehensive range of interoperability standards relevant to the Internet of Things (IoT) ecosystem. These standards encompassed communication protocols, data formats, interoperability frameworks, and device management protocols. Commonly identified interoperability standards included MQTT, CoAP, OPC UA, oneM2M, and Thread. Each of these standards addressed different aspects of IoT interoperability, such as device communication, data exchange, and service integration.

Analysis of Security Standards

Security standards play a crucial role in ensuring the confidentiality, integrity, and availability of IoT systems and data. The survey analyzed various security standards applicable to IoT deployments, including authentication protocols, encryption algorithms, access control mechanisms, and secure communication protocols. Notable security standards identified in the survey included TLS/SSL, OAuth, JWT, AES, and RBAC. These standards provide robust mechanisms for securing IoT communication, authenticating users and devices, and protecting against cyber threats.

Evaluation of Standard Effectiveness

The effectiveness of interoperability and security standards was assessed based on their ability to address key challenges and requirements in IoT deployments. Interoperability standards were evaluated based on their compatibility with different devices and systems, ease of implementation, scalability, and support for interoperability testing and certification. Security standards were evaluated based on their strength of encryption, resistance to attacks, usability, and compatibility with existing IoT infrastructure (Ashton et al., 2009).

Discussion on Challenges and Future Directions

Despite the availability of interoperability and security standards, several challenges remain in their implementation and adoption in IoT deployments. Challenges include device heterogeneity, interoperability testing, resource constraints in IoT devices, evolving security threats, and compliance with regulatory requirements. Future research directions include the development of standardized interoperability testing frameworks, the integration of blockchain technology for enhanced security, the adoption of AI-driven security solutions, and the establishment of industry-wide best practices for IoT security.

Implications for Stakeholders

The survey findings have implications for various stakeholders involved in IoT development, deployment, and management. IoT developers can leverage the identified standards to design interoperable and secure IoT solutions, thereby reducing development time and costs. System integrators can use the survey findings to select appropriate standards for integrating IoT devices and systems into existing infrastructure. Policymakers and regulators can use the survey findings to develop policies and regulations that promote the adoption of interoperability and security standards in IoT deployments. Overall, the survey provides valuable insights into the landscape of interoperability and security standards in the Internet of Things. By addressing key challenges and identifying future research directions, the survey aims to contribute to the advancement of interoperable and secure IoT ecosystems (Zorzi et al., 2010).

Conclusion

In conclusion, the exploration of interoperability and security standards in the Internet of Things (IoT) through this in-depth survey has provided valuable insights into the current state-of-the-art, challenges, and future directions in IoT standardization. The survey identified a diverse range of interoperability and security standards, including communication protocols, data formats, authentication mechanisms, encryption techniques, and access control policies, which play a crucial role in enabling seamless communication and secure interaction among IoT devices and systems.

Through the analysis of these standards, several key findings have emerged:

- The importance of interoperability standards in facilitating seamless communication and integration among heterogeneous IoT devices and systems.
- The critical role of security standards in safeguarding IoT deployments against cyber threats and ensuring the confidentiality, integrity, and availability of IoT data and services.
- The challenges associated with implementing and adopting interoperability and security standards in real-world IoT deployments, including device heterogeneity, interoperability testing, resource constraints, and evolving security threats.
- The need for continued research and standardization efforts to address these challenges and drive innovation in IoT standardization.

In conclusion, the exploration of interoperability and security standards in the Internet of Things has shed light on the importance of standardized approaches to address the complex challenges of IoT deployments. By embracing interoperability and security standards, stakeholders can build more robust, scalable, and secure IoT ecosystems that drive innovation, enhance efficiency, and improve quality of life. Continued collaboration and research efforts are essential to advancing the state-of-the-art in IoT standardization and realizing the full potential of the Internet of Things.

.

References

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

Cass, S. (2014). The age of the zettabyte Cisco: the future of internet traffic is video [Dataflow]. *IEEE Spectrum*, *51*(3), 68–68. https://doi.org/10.1109/mspec.2014.6745894

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Dhamdhere, A., & Dovrolis, C. (2011). Twelve Years in the Evolution of the Internet Ecosystem. *IEEE/ACM Transactions on Networking*, *19*(5), 1420–1433. https://doi.org/10.1109/tnet.2011.2119327

Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. *Scientific American*, *291*(4), 76–81. https://doi.org/10.1038/scientificamerican1004-76

Kamilaris, A., & Pitsillides, A. (2016). Mobile Phone Computing and the Internet of Things: A Survey. *IEEE Internet of Things Journal*, *3*(6), 885–898. https://doi.org/10.1109/jiot.2016.2600569

Li, S., Xu, L. D., & Zhao, S. (2014). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Noura, M., Atiquzzaman, M., & Gaedke, M. (2018). Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mobile Networks and Applications*, *24*(3), 796–809. https://doi.org/10.1007/s11036-018-1089-9

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., . . . Borriello, G. (2009). Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *IEEE Internet Computing*, *13*(3), 48–55. https://doi.org/10.1109/mic.2009.52

Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A Survey on the Edge Computing for the Internet of Things. *IEEE Access*, *6*, 6900–6919. https://doi.org/10.1109/access.2017.2778504

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view. *IEEE Wireless Communications*, *17*(6), 44–51. https://doi.org/10.1109/mwc.2010.5675777

How to cite this article

Singh, N. and Rohilla, A. (2021). Exploring Interoperability and Security Standards in the Internet of Things: An In-Depth Survey. *Science Archives,* Vol. 2(4), 362-367. https://doi.org/10.47587/SA.2021.2416.

Publisher's Note: MD International Publishing stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.