

IoT Security: Threat Detection, Analysis, and Defense

Olivier Markowitch ^{1,*}  and Jean-Michel Dricot ^{2,*} 

¹ Computer Science Department and Cybersecurity Research Center, Faculty of Sciences, Université Libre de Bruxelles, Boulevard du Triomphe CP 212, 1050 Brussels, Belgium

² Cybersecurity Research Center, Ecole Polytechnique de Bruxelles, Université Libre de Bruxelles, 50 Avenue Franklin Roosevelt CP 165/56, 1050 Brussels, Belgium

* Correspondence: olivier.markowitch@ulb.be (O.M.); jean-michel.dricot@ulb.be (J.-M.D.)

In recent years, the rapid growth of Internet of Things (IoT) technologies has created numerous opportunities across fields such as smart cities, transportation, energy, and healthcare. However, the growth of IoT technology also introduces significant security and privacy challenges, leading to research on intrusion detection in IoT environments, privacy-preserving data analysis, firmware vulnerability analysis, and secure communication protocols. The complexity and diversity of IoT ecosystems necessitate new techniques, architectures, and frameworks to detect, analyze, and counter emerging threats. This Special Issue of *Future Internet*, titled “IoT Security: Threat Detection, Analysis and Defense”, highlights papers and research reviews that explore the current state of the art in IoT system security.

After a thorough screening and peer-review process, ten papers were accepted for publication. These papers are categorized into two groups: (1) papers presenting emerging techniques and frameworks for intrusion detection, privacy preservation, and further securing operations in IoT, and (2) surveys and systematic analyses that aggregate knowledge and discuss future directions.

The first group focuses on innovative architectures and algorithms that aim to detect and mitigate attacks within IoT environments.

Lazea et al. [1] present a methodology for constructing “equi-width” histograms directly on homomorphically encrypted IoT data, thereby facilitating privacy-preserving analytics without the need to expose raw data. Their approach, based on the TFHE scheme, is optimized for secure computation. This approach is evaluated through the lens of an encrypted outlier detection use case.

Fatema et al. [2] introduce Federated XAI IDS, which integrates federated learning to develop an explainable intrusion detection system that safeguards privacy. Trained collaboratively across multiple decentralized devices on the CIC-IoT-2023 dataset, the framework achieves high accuracy while ensuring that sensitive network data remain local and interpretable.

Cibrario Bertolotti et al. [3] examine SlowROS attacks targeting the ROS Master component in industrial automation systems. They demonstrate how prolonged idle connection timeouts can be exploited to disrupt system-wide operations, bypassing built-in kernel protections.

In the domain of vehicular cybersecurity, Althunayyan et al. [4] propose a Hierarchical Federated Learning framework for intrusion detection in in-vehicle networks. The system’s incorporation of multiple edge aggregators mitigates the risk of single points of failure and enhances scalability.



Received: 26 August 2025

Accepted: 29 August 2025

Published: 30 August 2025

Citation: Markowitch, O.; Dricot, J.-M. IoT Security: Threat Detection, Analysis, and Defense. *Future Internet* **2025**, *17*, 399. <https://doi.org/10.3390/fi17090399>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Tseng et al. [5] explore multi-class intrusion detection using Transformer models on the CIC-IoT-2023 dataset. Their Transformer-based approach performs well in binary classification, particularly in multi-class scenarios.

For resource-constrained environments such as smart homes, Javed et al. [6] implement a lightweight, two-layered IDS that operates both on-device and in the cloud. Their XGBoost-based solution efficiently detects MITM and DoS attacks on microcontroller-powered devices, making it suitable for real-time deployment.

The second group provides broader perspectives and foundational insights.

He et al. [7] surveyed energy-aware security mechanisms for IoT technologies, identifying the interplay between energy efficiency and security, reviewing current privacy-preserving approaches, and outlining future directions for sustainable IoT protection.

Bagheri et al. [8] address the issue of smart grid security through a PUF-based authentication and key agreement protocol that combines physical unclonable functions with elliptic curve cryptography.

Zhou et al. [9] provide a critical revisit of IoT firmware emulation and its application to fuzzing. By examining recent works, they identify fundamental challenges, systematically classify solutions according to the issues they address, and perform a comparative analysis of emulation fidelity and bug detection capabilities. They also highlight key research gaps for future exploration.

Finally, Papadopoulos et al. [10] provide a comprehensive review of recent advancements in federated learning. Their analysis emphasizes FL's role in privacy preservation and data decentralization while identifying existing challenges in securing models against adversarial attacks.

We sincerely thank all authors for their contributions and the reviewers for their efforts in ensuring the Special Issue was of the highest quality. Together, the papers represent the dynamic and changing field of IoT security research, providing implementation strategies, theoretical advances, and recommendations for addressing the security and privacy challenges of these connected systems.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lazea, D.; Hangan, A.; Cioara, T. Building Equi-Width Histograms on Homomorphically Encrypted Data. *Future Internet* **2025**, *17*, 256. [\[CrossRef\]](#)
2. Fatema, K.; Dey, S.K.; Anannya, M.; Khan, R.T.; Rashid, M.M.; Su, C.; Mazumder, R. Federated XAI IDS: An Explainable and Safeguarding Privacy Approach to Detect Intrusion Combining Federated Learning and SHAP. *Future Internet* **2025**, *17*, 234. [\[CrossRef\]](#)
3. Cibrario Bertolotti, I.; Durante, L.; Cambiaso, E. Analyzing Impact and Systemwide Effects of the SlowROS Attack in an Industrial Automation Scenario. *Future Internet* **2025**, *17*, 167. [\[CrossRef\]](#)
4. Althunayyan, M.; Javed, A.; Rana, O.; Spyridopoulos, T. Hierarchical Federated Learning-Based Intrusion Detection for In-Vehicle Networks. *Future Internet* **2024**, *16*, 451. [\[CrossRef\]](#)
5. Tseng, S.-M.; Wang, Y.-Q.; Wang, Y.-C. Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset. *Future Internet* **2024**, *16*, 284. [\[CrossRef\]](#)
6. Javed, A.; Ehtsham, A.; Jawad, M.; Awais, M.N.; Qureshi, A.-u.-H.; Larijani, H. Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes. *Future Internet* **2024**, *16*, 200. [\[CrossRef\]](#)
7. He, P.; Zhou, Y.; Qin, X. A Survey on Energy-Aware Security Mechanisms for the Internet of Things. *Future Internet* **2024**, *16*, 128. [\[CrossRef\]](#)
8. Bagheri, N.; Bendavid, Y.; Safkhani, M.; Rostampour, S. Smart Grid Security: A PUF-Based Authentication and Key Agreement Protocol. *Future Internet* **2024**, *16*, 9. [\[CrossRef\]](#)

9. Zhou, W.; Shen, S.; Liu, P. IoT Firmware Emulation and Its Security Application in Fuzzing: A Critical Revisit. *Future Internet* **2025**, *17*, 19. [[CrossRef](#)]
10. Papadopoulos, C.; Kollias, K.-F.; Fragulis, G.F. Recent Advancements in Federated Learning: State of the Art, Fundamentals, Principles, IoT Applications and Future Trends. *Future Internet* **2024**, *16*, 415. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.