Advanced Research on Information Systems Security
An International Journal · ISSN 2795-4609 | 2795-4560
Vol. 6, No. 2 (2026)
pp. 3–16
aris-journal.com

REVIEW ARTICLE

Cybersecurity Resilience in IoT-Enabled Critical Infrastructures: A PRISMA Systematic Review and Bibliometric Analysis

Luis Miguel Pires [a,b]

[a] School of Communication, Arts and Information (ECATI), Lusofona University, 1749-024 Lisbon

[b] Technologies and Engineering School (EET), Polytechnic University of Lusofonia (IPLuso), 1700-098 Lisbon, Portugal

Received: 2026-01-26 · Accepted: 2026-07-02 · Published: 2026-11-05 · DOI: https://doi.org/10.56394/aris2.v6i2.68

ABSTRACT

The increasing integration of IoT technologies into critical infrastructures has brought significant benefits in terms of automation, monitoring, and operational efficiency across sectors such as energy, healthcare, transportation, and industrial systems. At the same time, this transformation has substantially increased exposure to cyber threats, particularly in environments where cyber and physical processes are tightly coupled and service availability is critical. Conventional cybersecurity approaches, largely focused on prevention and perimeter defense, have shown limited effectiveness in highly distributed, heterogeneous, and dynamic IoT-based infrastructures. In this context, the notion of cybersecurity resilience has emerged as a key paradigm, emphasizing the ability of systems to withstand attacks, adapt to adverse conditions, and recover essential functions rather than relying solely on intrusion prevention. This paper presents a systematic literature review conducted in accordance with the PRISMA 2020 guidelines, focusing on cybersecurity resilience in IoT-enabled critical infrastructures. An initial set of 244 publications was identified through major scientific databases, from which nine primary studies were selected following a rigorous screening and eligibility process. The review is complemented by a bibliometric analysis that examines publication trends, research focus, and the evolution of resilience-oriented security approaches over time. The findings indicate a distinct transformation in the direction of unified security frameworks, from having separate intrusion detection mechanisms. Nevertheless, current integration efforts still reveal substantial differences in maturity and validation, particularly in operational environments.

KEYWORDS

cybersecurity resilience; Internet of Things (IoT); critical infrastructures; anomaly detection; machine learning; federated learning; cloud–edge security; PRISMA systematic review

1. Introduction

The rapid adoption of Internet of Things (IoT) technologies has fundamentally transformed the operation of critical infrastructures, including energy systems, healthcare services, transportation networks, and industrial environments. By enabling large-scale sensing, real-time monitoring, and remote control, IoT has become a core component of modern Cyber-Physical Systems (CPS) and Industrial Internet of Things (IIoT) architectures. While these technologies significantly enhance efficiency and operational awareness, they also introduce complex cybersecurity challenges that directly affect the safety, reliability, and continuity of critical services [1]. Unlike traditional Information Technology (IT) systems, IoT-enabled critical infrastructures integrate heterogeneous and resource-constrained devices, legacy industrial protocols, and tightly coupled cyber–physical processes. This convergence substantially enlarges the attack surface and creates new opportunities for adversaries to exploit vulnerabilities across both cyber and physical domains [2], [31], [34]. Surveys on CPS and IIoT security consistently demonstrate that attacks targeting industrial control systems, smart grids, and healthcare infrastructures can result in cascading failures, with consequences extending far beyond data loss to include physical damage, service disruption, and risks to human safety [3].

* Corresponding author: luis.pires@ipluso.pt
© 2026 The Author(s). Published by LAPI2S.
Cite as: L. M. Pires, “Cybersecurity Resilience in IoT-Enabled Critical Infrastructures: A PRISMA Systematic Review and Bibliometric Analysis,” *Adv. Res. Inf. Syst. Secur.*, vol. 6, no. 2, pp. 3–16, 2026, doi: 10.56394/aris2.v6i2.68.

Recent threat analyses further indicate that IoT devices are increasingly exploited as initial entry points for attacks against critical infrastructures. Weak authentication mechanisms, limited patching capabilities, and insufficient monitoring at the edge make IoT components particularly attractive targets for large-scale exploitation [4]. Reports from European and international cybersecurity agencies confirm a steady increase in attacks leveraging IoT deployments to compromise or disrupt essential services [5]. Recent incident reports from operational environments show that even highly secured infrastructures remain exposed to lateral movement and undetected activities, highlighting the limitations of security strategies that rely solely on prevention [6]. In response to these limitations, the concept of cybersecurity resilience has gained prominence in both research and standardization efforts. Rather than focusing solely on protection, resilience emphasizes the ability of systems to continue operating under attack, adapt to adverse conditions, and recover essential functions in a timely manner [7]. This perspective is formalized by National Institute of Standards and Technology (NIST), which characterizes cyber-resilient systems as those designed to anticipate, withstand, recover from, and adapt to cyber-related disruptions throughout their lifecycle [8]. This approach is aligned with internationally recognized cybersecurity best practices, namely those promoted by the NIST Cybersecurity Framework. From an operational standpoint, this transition mirrors the increasing acknowledgment that keeping the services running and allowing controlled degradation are usually more practical goals than complete protection in IoT-supported vital infrastructures.

Achieving cybersecurity resilience in IoT-enabled critical infrastructures remains particularly challenging due to inherent system characteristics, including real-time operational constraints, decentralized architectures, and tight coupling between cyber components and physical processes. As a result, cyber incidents may directly affect physical safety, service availability, and public trust [9]. To address these challenges, recent research has explored resilience-oriented security mechanisms such as machine-learning-based anomaly detection, federated learning for distributed intrusion detection, blockchain-enabled trust frameworks, and cloud–edge security architectures grounded in Zero Trust principles [10]-[13]. Despite the growing body of literature, existing contributions remain fragmented across application domains and often differ significantly in validation methodology, performance metrics, and real-world applicability. There is a lack of consolidated evidence focusing specifically on cybersecurity resilience in IoT-enabled critical infrastructures supported by experimental validation, objective evaluation metrics, or realistic deployment scenarios. This fragmentation makes it difficult to assess the maturity of current approaches and to identify consistent research trends and open challenges. The fragmentation of knowledge in this field motivated the present work to conduct a systematic review, adhering to PRISMA 2020 guidelines [14], to bring together the latest evidence on cybersecurity resilience in IoT-enabled critical infrastructures.

The rest of the article is structured as follows. Section 2 provides background and related work, summarizing recent developments in cybersecurity, resilience, and the deployment of smart protective mechanisms for IoT-enabled critical infrastructures. The methodology adopted, including the process of systematic review and bibliometric analysis framework, is explained in Section 3. Section 4 presents and argues the main findings, bringing to the fore the emerging trends, technological approaches, and research gaps that have been identified. Finally, Section 5 wraps up the paper by outlining the main contributions and offering directions for future research.

2. Methodology

This section describes the methodology adopted for systematic review and bibliometric analysis, detailing the review design, information sources, and study selection process.

2.1 Review Design and Research Scope

This study adopts a systematic literature review methodology to analyze the current state of research on cybersecurity resilience in IoT-enabled critical infrastructures. In line with the resilience-oriented perspective introduced in Section 1, the review focuses on studies that explicitly address capabilities such as anomaly detection, adaptation, recovery, and continuity of operation, rather than solely preventive or perimeter-based

security mechanisms. The scope of the review encompasses IoT-enabled critical infrastructure domains, including energy systems, industrial control systems, healthcare infrastructures, and large-scale urban or smart-city deployments. These domains are characterized by tight coupling between cyber and physical processes and by the integration of heterogeneous, resource-constrained IoT devices, which significantly increase system complexity and exposure to cyber threats.

Only peer-reviewed journal articles and conference papers published between 2015 and 2025 were considered. This time window reflects both the widespread adoption of IoT technologies in critical infrastructures and the increasing recognition of cybersecurity resilience as a distinct and necessary research focus.

2.2 Information Sources and Search Strategy

The literature search was conducted across five major scientific databases: IEEE Xplore, ScienceDirect, SpringerLink, MDPI, and Scopus. These databases were selected due to their comprehensive coverage of high-impact research in cybersecurity, Internet of Things, cyber-physical systems, and critical infrastructure protection.

A structured search strategy was applied using combinations of keywords related to *Internet of Things*, *critical infrastructures*, *cybersecurity*, and *resilience*. To capture recent resilience-oriented approaches, additional terms such as *anomaly detection*, *machine learning*, *federated learning*, *blockchain*, *cloud–edge security*, and *Zero Trust* were included. Boolean operators were used to maximize coverage while maintaining relevance, and searches were applied to titles, abstracts, and author keywords.

2.3 Study Selection Process

The study selection process was conducted in accordance with the PRISMA 2020 guidelines to ensure transparency, traceability, and reproducibility [14]. The selection followed four phases: identification, screening, eligibility, and inclusion.

A total of 244 records were initially identified across the selected databases. Duplicate detection and removal were performed using the Rayyan.ai platform, resulting in the removal of three duplicate records prior to screening. During the screening phase, titles and abstracts were analyzed to exclude studies that were out of scope, non-technical, or not related to IoT-enabled critical infrastructures. This step led to the exclusion of 204 records, leaving 37 studies for full-text assessment. Among the studies selected for retrieval, 12 reports could not be accessed, primarily due to publisher access limitations. The remaining 25 studies were assessed for eligibility based on predefined inclusion and exclusion criteria. Studies were excluded if they lacked a clear cybersecurity or resilience focus, did not involve IoT-enabled environments, or failed to provide sufficient technical or experimental detail. Following this process, nine primary studies were included in the final review. Figure 1 shows PRISMA 2020 flow diagram illustrating the identification, screening, eligibility, and inclusion of studies.

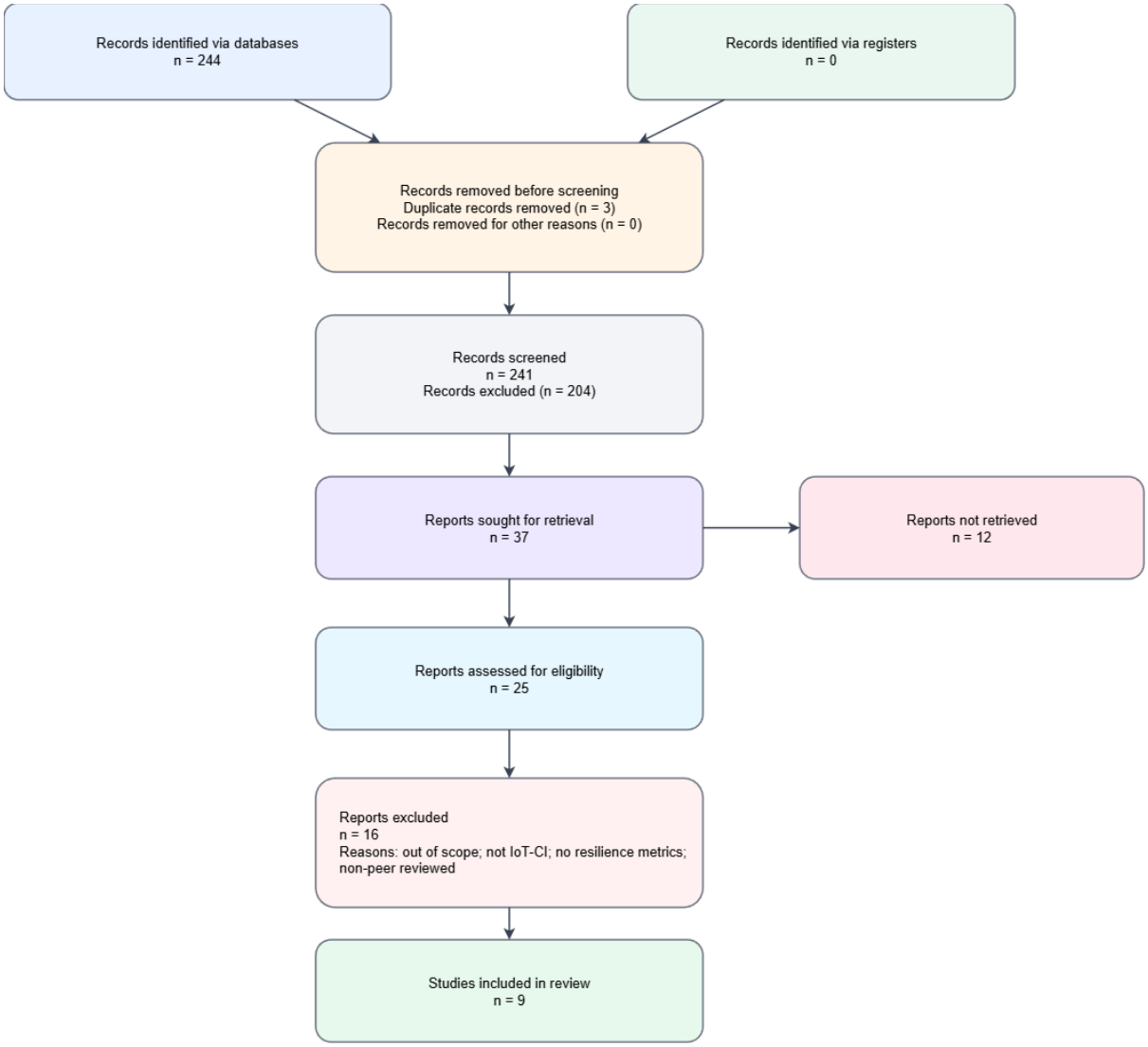


Figure 1. PRISMA 2020 flow diagram illustrating the identification, screening, eligibility, and inclusion of studies.

2.4 Data Extraction and Study Classification

For each of the nine included studies, structured data extraction was performed to ensure consistency and comparability. Extracted information included publication year, application domain, type of critical infrastructure, security objectives, employed technologies, evaluation methodology, and reported outcomes.

Special attention was given to mechanisms explicitly supporting cybersecurity resilience, such as adaptive anomaly detection, machine-learning-based intrusion detection, federated and distributed learning architectures, blockchain-enabled trust mechanisms, and cloud-edge security frameworks. Based on these characteristics, the studies were classified into thematic groups to support a structured qualitative synthesis in the subsequent analysis.

2.5 Bibliometric Analysis Procedure

In addition to qualitative synthesis, a bibliometric analysis was conducted to explore publication trends and thematic evolution in cybersecurity resilience research for IoT-enabled critical infrastructures. Bibliographic metadata was exported from Scopus and analyzed using VOSviewer [15], a widely adopted tool for constructing and visualizing bibliometric networks.

The bibliometric analysis focused on publication trends over time and author keyword co-occurrence networks, enabling the identification of dominant research themes and emerging topics. Co-occurrence analysis was

applied to highlight conceptual relationships between keywords, while density and temporal overlay visualizations were used to capture both the intensity and the evolution of research topics over time. Figure 2 shows temporal distribution of publications on cybersecurity in IoT-enabled critical infrastructures between 2015 and 2025.

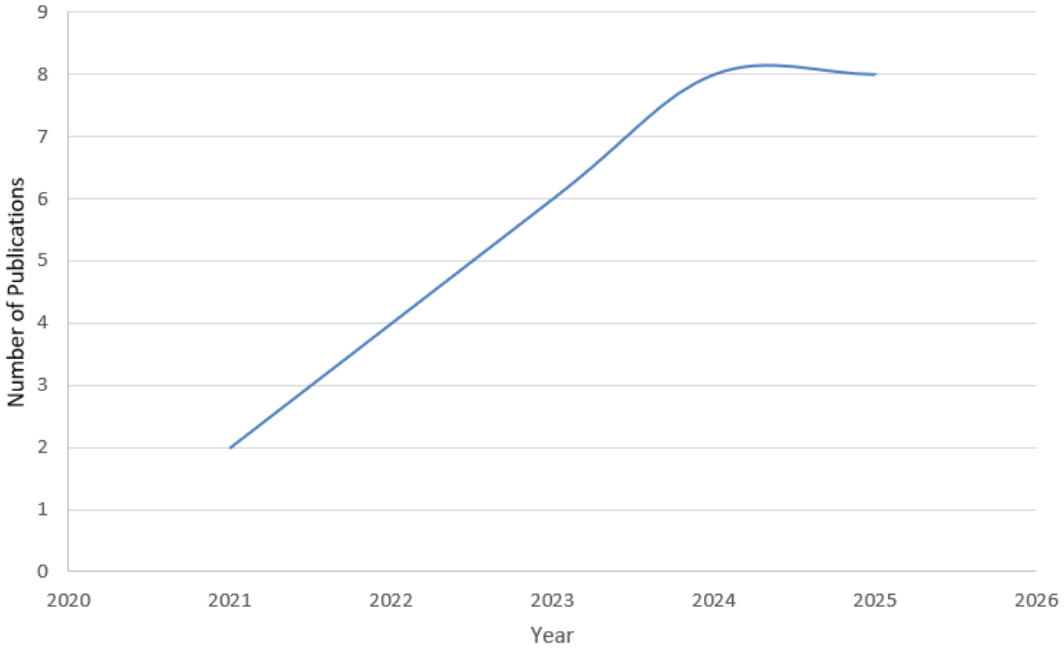


Figure 2. Temporal distribution of publications on cybersecurity in IoT-enabled critical infrastructures (2015 to 2025).

Figure 3 show publication trend of the final PRISMA-selected studies between 2021 and 2025.

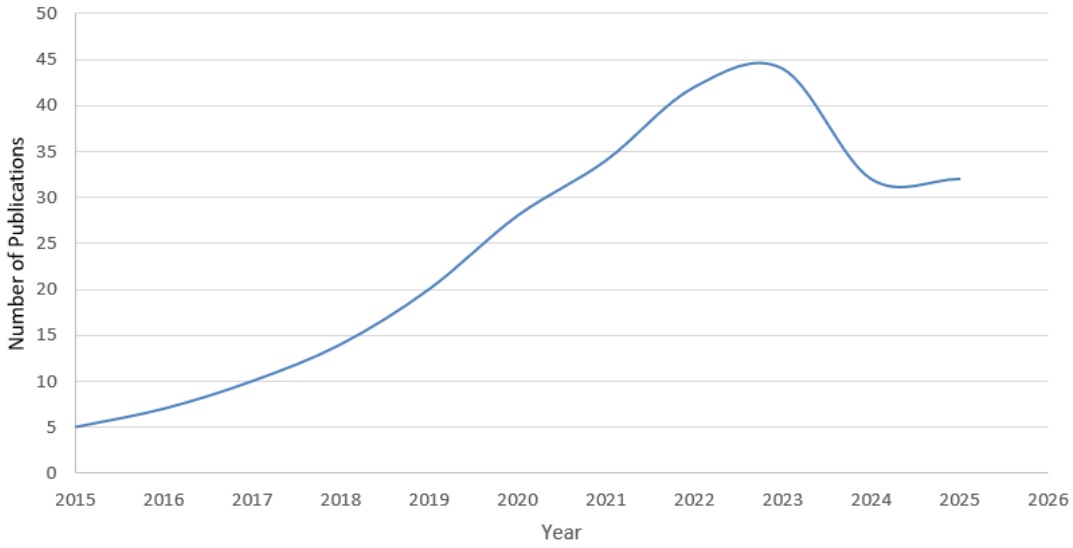


Figure 3. Publication trend of the final PRISMA-selected studies (2021 to 2025).

2.6 Methodological Overview

To provide a concise overview of the adopted methodology, a conceptual workflow diagram summarizes the interaction between the PRISMA-based systematic review process, the bibliometric analysis using VOSviewer [15], and the subsequent thematic synthesis. Figure 4 show methodological workflow illustrating the PRISMA-based study selection, bibliometric analysis, and thematic synthesis.

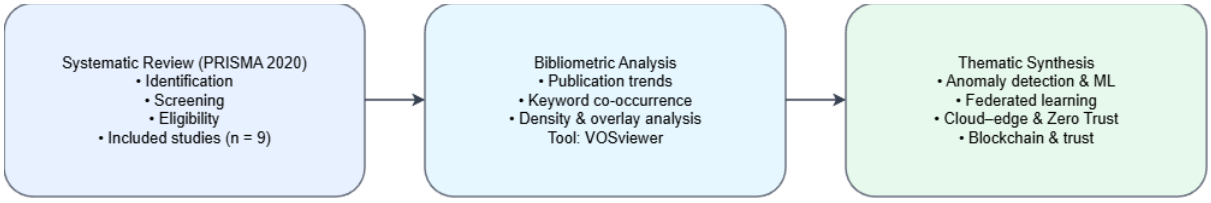


Figure 4. Methodological workflow illustrating the PRISMA-based study selection, bibliometric analysis, and thematic synthesis.

3. Bibliometric Results and Keyword Analysis

This section presents the results of the bibliometric analysis conducted on the final set of studies included after the PRISMA-based selection process. The objective is to characterize the thematic structure of literature and to analyze the evolution of research topics related to cybersecurity resilience in IoT-enabled critical infrastructures. Bibliometric mapping and visualization were performed using the VOSviewer software tool [15].

3.1 Keyword Co-occurrence Analysis

The keyword co-occurrence network generated using VOSviewer is shown in Figure 5. This network provides an overview of the conceptual relationships between the most relevant author keywords extracted from the selected studies.

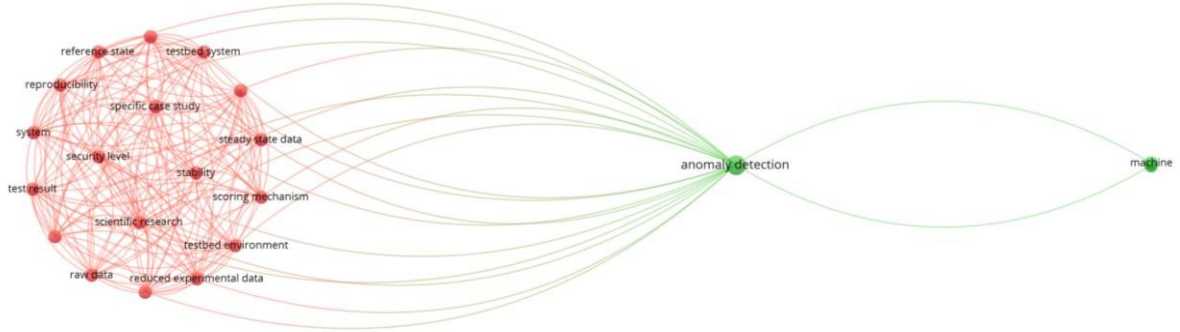


Figure 5. Keyword co-occurrence network of cybersecurity resilience research in IoT-enabled critical infrastructures, generated using VOSviewer.

The network reveals a dense cluster of keywords associated with system-level evaluation and operational performance, including terms such as reliability, security level, stability, raw data, and testbed environment. The prominence of these terms highlights the strong emphasis placed on experimental validation and measurable performance metrics within the analyzed literature. A second, highly connected cluster is centered on anomaly detection, which emerges as a pivotal concept linking traditional system evaluation practices with more advanced, data-driven security mechanisms. The centrality of anomaly detection reflects its importance as an enabling capability for early threat identification and adaptive response in dynamic and heterogeneous IoT environments.

3.2 Keyword Density Analysis

To complement the network-based interpretation, a keyword density visualization was generated, as illustrated in Figure 6. This visualization highlights the most frequently occurring keywords in the analyzed studies, allowing the identification of dominant research focus areas.

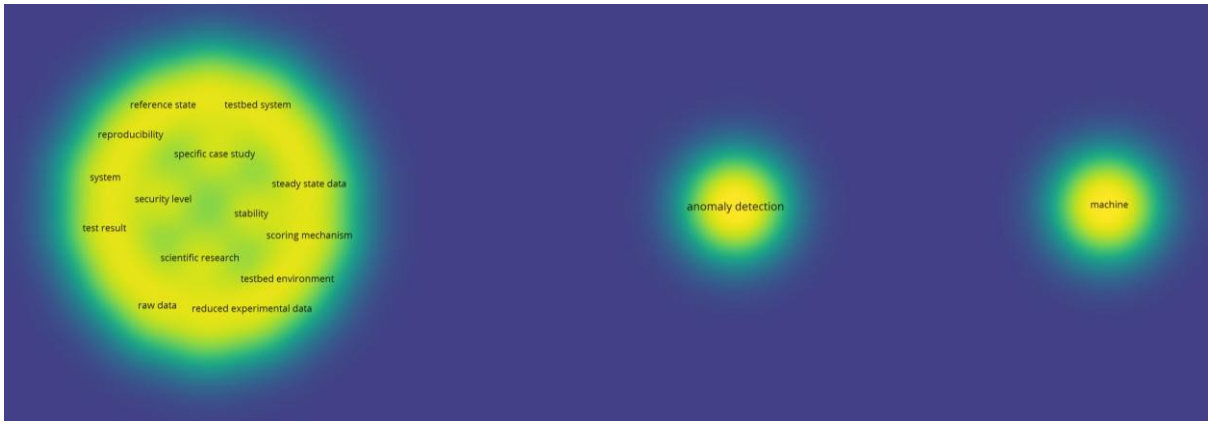


Figure 6. Keyword density visualization of cybersecurity resilience research in IoT-enabled critical infrastructures generated using VOSviewer.

High-density regions are primarily associated with concepts related to system reliability, security evaluation, and stability, confirming that resilience-oriented research remains strongly grounded in system-level assessment. Anomaly detection also appears as a high-density term, reinforcing its role as a core operational mechanism for achieving cybersecurity resilience in IoT-enabled critical infrastructures.

3.3 Temporal Overlay Analysis

To analyze the temporal evolution of research themes, a keyword overlay visualization was produced using VOSviewer, as shown in Figure 7. This visualization maps keywords according to their average publication year, enabling the identification of emerging and maturing research topics.

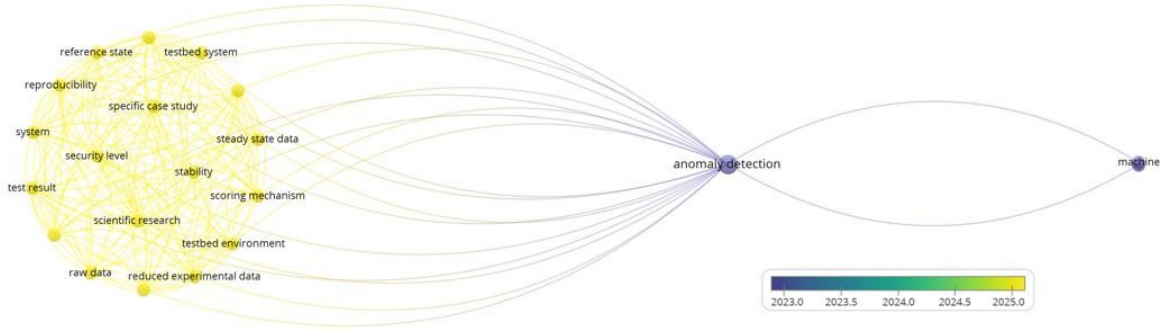


Figure 7. Temporal overlay visualization of keyword co-occurrence by average publication year, generated using VOSviewer.

The overlay analysis indicates that keywords related to system evaluation, testing environments, and performance assessment tend to appear earlier in the analysis period. In contrast, terms associated with machine learning, anomaly detection, and adaptive security mechanisms are more prominent in recent years. This shift reflects a gradual transition towards data-driven and adaptive approaches aimed at addressing the limitations of static, prevention-based cybersecurity solutions in IoT-enabled critical infrastructures.

3.4 Summary of Bibliometric Insights

Overall, the bibliometric analysis highlights a clear evolution of cybersecurity research in IoT-enabled critical infrastructures towards resilience-oriented, experimentally validated, and data-driven approaches. Anomaly detection emerges as a central concept connecting system-level evaluation practices with modern machine-learning-based security mechanisms. These findings provide a structured foundation for the subsequent discussion, where the selected studies are critically analyzed with respect to architectural choices, validation strategies, and open research challenges.

4. Discussion

This section discusses the main findings of systematic review and bibliometric analysis, focusing on the implications for cybersecurity resilience in IoT-enabled critical infrastructures. The discussion is structured around the dominant technical approaches identified, their maturity, validation practices, and the gaps that remain in current research.

4.1 From Preventive Security to Cybersecurity Resilience

The analyzed literature confirms a clear transition from prevention-centric cybersecurity models towards resilience-oriented approaches in IoT-enabled critical infrastructures. Traditional mechanisms such as static access control, perimeter defenses, and signature-based intrusion detection systems remain widely referenced but are increasingly recognized as insufficient in highly distributed and dynamic IoT environments [1], [2], [4], [32], [33].

Resilience-oriented approaches, aligned with the NIST definition of cyber resilience [5], emphasize the ability of systems to detect, withstand, adapt to, and recover from cyber incidents rather than assuming complete prevention. This shift is particularly relevant in critical infrastructures, where IoT devices often operate under resource constraints, rely on legacy protocols, and interact directly with physical processes, amplifying the potential impact of cyber incidents [10], [11].

To synthesize the relationships between the identified cybersecurity mechanisms and the operational requirements of critical infrastructures, Figure 8 presents a conceptual mapping derived from the comparative analysis of the included studies. The mapping highlights how different mechanisms contribute to specific resilience phases and system requirements.

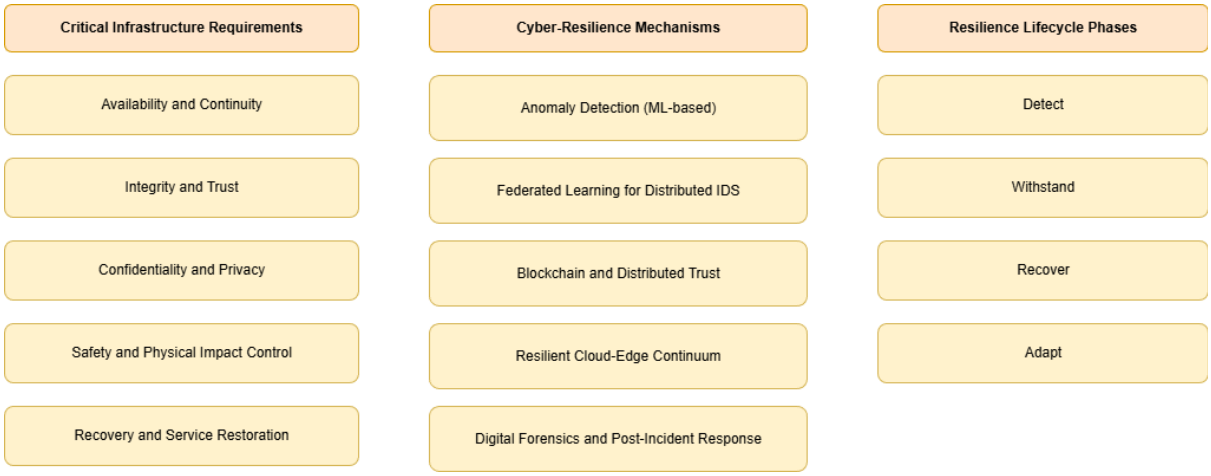


Figure 8. Conceptual mapping between cybersecurity resilience mechanisms identified in the reviewed studies and core critical infrastructure requirements across the detect, withstand, recover and adapt resilience lifecycle.

The conceptual mapping reveals a strong emphasis on detection and resistance capabilities, mainly supported by anomaly detection, federated learning, and blockchain-based trust mechanisms. In contrast, explicit recovery and adaptation strategies remain less explored, reinforcing the need for integrated end-to-end resilience frameworks.

4.2 Central Role of Anomaly Detection

One of the most consistent findings across both the qualitative review and the bibliometric analysis is the central role of anomaly detection in enabling cybersecurity resilience. As highlighted in Section 3, anomaly detection appears as a highly connected keyword bridging system-level evaluation metrics and advanced data-driven security mechanisms. Machine-learning-based anomaly detection techniques are widely adopted to identify deviations from normal operational behavior, particularly in scenarios where labelled attack data are scarce or

unavailable [7], [17], [18], [30]. In IoT-enabled critical infrastructures, anomaly detection supports early threat identification, enabling timely mitigation actions before cyber incidents propagate to physical processes.

However, the review also reveals that many proposed anomaly detection approaches remain highly context-dependent, often tuned to specific datasets, infrastructures, or attack models. This limits their generalizability and raises concerns regarding robustness under real-world operational variability.

After utilizing the PRISMA-based research selection technique, there were nine primary studies that were kept for thorough examination. A brief synopsis of these studies, including their application areas, the cybersecurity resilience mechanisms used, and the kind of validation disclosed is given in Table 1. This synthesis makes it possible to compare directly the methodological approaches and shows the different levels of maturity that exist in IoT-enabled critical infrastructure sectors.

Table 1. Summary of the nine primary studies included in the systematic review, highlighting the critical infrastructure domain, main cybersecurity resilience mechanisms, and validation approach.

Study	CI Domain/IoT Context	Main Resilience Mechanism	Validation & Key Outcomes
[21]	Smart Home Energy / HEMS	Cybersecurity framework (governance + controls)	Framework/conceptual; good holistic view; limitation: lack of quantitative resilience metrics
[17]	Smart Grid	ML-based anomaly detection	Experimental/simulation; focus on detection; limitation: generalization and dataset dependency
[20]	Smart Grid Communications	Lightweight authentication	Technical assessment (classic in communications security); limitation: does not cover resilience metrics
[19]	SCADA / Energy Management	DDoS context + verificação/avaliação	Simulation/study; good focus on availability; limitation: limited adversarial model and real scale
[7]	IoHT / Healthcare IoT	AI-based anomaly detection + blockchain trust	Experimental evaluation; integrity and traceability; limitation: overhead/complexity and privacy trade-offs
[8]	Public Networks / Distributed IDS	Federated Learning (IDS)	Testbed/experimental; reduces data sharing; limitation: communication overhead and robustness to poisoning
[6]	Cloud–Edge IoT	Resilient cloud–edge continuum	Architecture + validation; improved fault tolerance; limitation: complexity of orchestration and implementation
[18]	CPS / Security evaluation	Anomaly detection + objective evaluation	Experimental; focus on objective evaluation; limitation: transferability between infrastructures
[16]	Industry 4.0/5.0	Digital forensic framework	Case/architectural; strong for recovery and post-incident; limitation: little real-time operational validation

Table 1 illustrates that most studies concentrate on detection-oriented mechanisms, especially anomaly detection and intrusion detection systems, whereas only a small portion of the works discuss cyber resilience in terms of recovery and adaptation phases. In addition, experimental validation is still quite variable, with several contributions depending on simulation or theoretical frameworks.

In Appendix A (Table 2), a comprehensive data extraction matrix consisting of threat focus, resilience phases, validation strategies, metrics, and identified limitations for each study is presented. This extensive analysis not only aids comparative discussion but also makes it easier to reproduce the review.

4.3 Distributed and Federated Security Architectures

Another prominent research direction concerns the adoption of distributed and federated learning architectures for intrusion detection and security monitoring. Federated learning-based approaches aim to overcome data-sharing constraints by enabling collaborative model training across distributed IoT nodes without centralizing raw data [8], [24], [29].

These approaches align well with the decentralized nature of IoT-enabled critical infrastructures and support privacy preservation and scalability [34]. Nevertheless, the review indicates that federated security solutions often assume ideal communication conditions and may overlook practical challenges such as model poisoning, heterogeneous device capabilities, and communication overheads, which can significantly affect resilience in operational deployments.

4.4 Cloud–Edge Continuum and Zero Trust Perspectives

Several studies emphasize the importance of cloud–edge security architectures as a foundation for resilient IoT systems [6], [13]. By distributing security functions across edge, fog, and cloud layers, these architectures aim to balance latency, scalability, and computational constraints while improving fault tolerance.

In parallel, Zero Trust Architecture (ZTA) principles are increasingly referenced as a conceptual framework for securing IoT-enabled critical infrastructures [22], [23], [27]. Zero Trust shifts the focus from network perimeter protection to continuous verification of entities and contexts. While conceptually appealing, the review highlights that practical implementations of Zero Trust in resource-constrained IoT environments remain limited, with few studies providing comprehensive experimental validation.

4.5 Validation Practices and Research Gaps

Despite the growing body of work on cybersecurity resilience, the review reveals significant gaps in experimental validation and evaluation consistency. Many studies relieve simulations, synthetic datasets, or small-scale testbeds, with limited assessment of long-term behavior, adversarial adaptation, or cascading failure scenarios.

Furthermore, evaluation metrics vary widely across studies, making cross-comparison difficult. While metrics such as detection accuracy and false-positive rates are commonly reported, fewer studies evaluate resilience-specific metrics, such as recovery time, service continuity, or degradation under sustained attack conditions [12].

These gaps indicate a need for standardized evaluation frameworks, shared datasets, and reproducible experimental setups tailored to IoT-enabled critical infrastructures.

4.6 Discussion Summary and Implications

Overall, the findings suggest that cybersecurity resilience in IoT-enabled critical infrastructures is an emerging but still maturing research field. Anomaly detection and machine-learning-based approaches dominate current research, supported by distributed architectures and cloud–edge integration. However, the lack of unified validation methodologies and real-world deployments limits the assessment of true operational resilience.

These insights motivate the need for future research focusing on holistic resilience evaluation, integration of security mechanisms with operational control systems, and long-term experimental validation in realistic critical infrastructure scenarios. Based on the extracted data and thematic analysis, Figure 9 proposes a taxonomy that organises the reviewed studies according to their primary cybersecurity resilience dimensions. This taxonomy provides a structured overview of how resilience is addressed across architectural, intelligence-driven, and trust-oriented approaches.

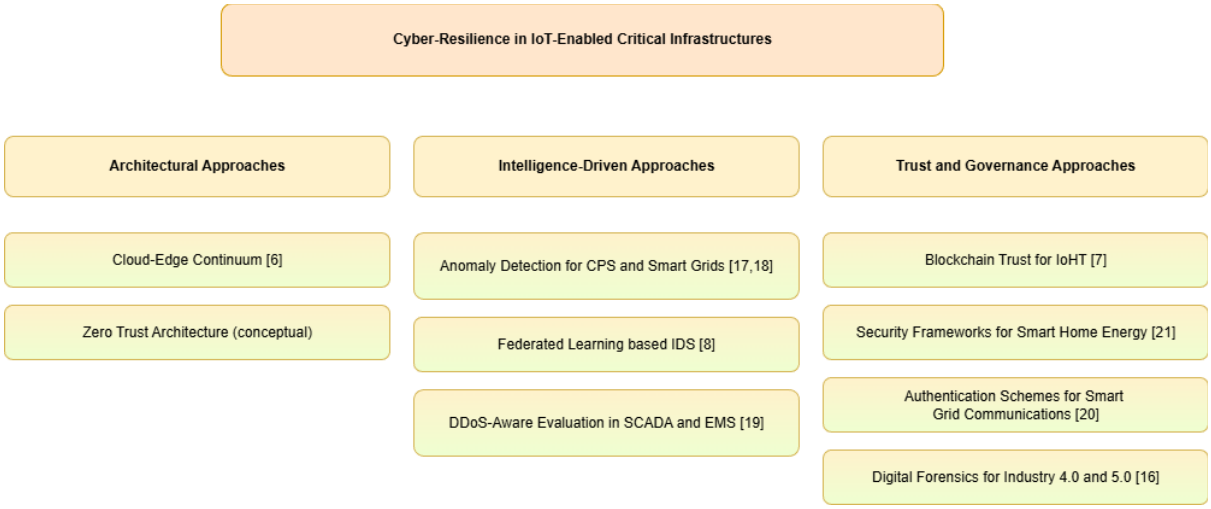


Figure 9. Taxonomy of cybersecurity resilience approaches for IoT-enabled critical infrastructures, organizing the reviewed literature into architectural, intelligence-driven, and trust and governance dimensions.

The taxonomy illustrates that most contributions focus on intelligence-driven mechanisms, particularly anomaly detection and intrusion detection, while fewer works address architectural resilience and post-incident governance aspects, such as digital forensics and coordinated recovery.

5. Conclusions

This paper presented a systematic literature review on cybersecurity resilience in IoT-enabled critical infrastructures, complemented by a bibliometric analysis to identify dominant research themes and their evolution over time. By following the PRISMA 2020 guidelines, the review ensured transparency, methodological rigor, and reproducibility in the study selection process. When considered as a whole, the evidence points to the notion that existing resilience-oriented approaches are still very much scattered and not validated enough for operational critical infrastructures.

The outcomes support the claim that cybersecurity resilience has been recognized as a separate and more researchable paradigm in the IoT-based critical infrastructure domain. Traditional security mechanisms that focus on prevention are nowadays complemented or even replaced by approaches which stress detection, adaptation, and recovery, thereby reflecting the very nature of the practical limitations of assuming that complete attack prevention can be achieved in extremely distributed and heterogeneous IoT environments.

The bibliometric analysis shows that anomaly detection has become the central enabling mechanism for cybersecurity resilience, acting as a bridge between system-level evaluation methods and data-driven security practices. The utilization of machine-learning-based anomaly detection approaches is quite extensive owing to their ability to detect novel threats and, consequently, facilitate the mechanism of early response. Yet, the study found out that most of the suggested solutions are limited to specific contexts and will therefore have difficulty being applied to other areas and different operational conditions. One of the outstanding features of distributed and federated learning was that they were pointed out as the best possible means for the large-scale and privacy-preserving security monitoring of IoT-enabled critical infrastructures. Although these methods align well with decentralized system architectures, their real-life application is still hindered by the communication overheads, the need for adversarial robustness, and the varying device capabilities.

In addition, it was determined that the pairing of cloud–edge security architectures and Zero Trust principles is becoming more frequent as the conceptual basis for resilient IoT systems. Even so, the testing of these architectures in actual critical infrastructure is still very limited, indicating that there is a significant gap between theoretical frameworks and practical implementations.

The evaluation reveals that the resilience of cybersecurity in critical infrastructures which are supported by IoT technology is an active but still developing research area. The researchers in future should give priority to the establishment of the standard evaluation methods, the long-term experiment validation, and the very realistic deployment scenarios that would reflect the complicated relationship between cyber and physical processes. It will be crucial to deal with these challenges to convert the present research breakthroughs into strong and practical solutions that will be able to protect critical services in environments that are getting more connected and dynamic all the time.

Appendix A

Table 2. Detailed data extraction matrix of the nine included studies, reporting threat focus, resilience phase coverage, core techniques, validation methodology, metrics, strengths, and limitations.

Ref.	Focus	Core tech	Dataset Testbed	Metrics	Type of Val	key	Limitations
[21]	Multi-threat	Framework	N/A	Qualitat.	Conceptual	Holisttic	No quantitative metrics
[17]	Anomalies Intrusions	ML	Dataset Simul.	Acc, FPR/FNR	Simul	Detection	Context dependency
[20]	Spoofing MITM	Auth scheme	Models	Overhead, delay	Analitic Simul	Low cost	Resilience
[19]	DDoS	Security eval	Simul	Availability/ impact	Simul	Avalability	forward model
[7]	Data tamper	AI Blockchain	Prototype	Overhead	Experim	Integrity	Overhead and privacy
[8]	Intrusions	Federated Learning	Testebed	F1	Experim	Scala privacy	Latency and poisoning
[6]	Failures attacks	Cloud–edge resilience	Testebed	Availability/ latency	Experim	Fault tolerance	Operational complexity
[18]	Anomalies	AD objective eval	Experim	“object. metrics”	Experim	Structured assessment	transferability
[16]	Incidents	Digital forensics	Case study	Qualitat	Case study	Recovery	Little real-time defense

References

[1] Ahmed, A.A.; Farhan, K.; Jabbar, W.A.; Al-Othmani, A.; Abdulrahman, A.G. IoT Forensics: Current Perspectives and Future Directions. *Sensors* 2024, 24, 5210. https://doi.org/10.3390/s24165210

[2] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security - A Survey,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[3] European Union Agency for Cybersecurity (ENISA), *Threat Landscape for IoT*, ENISA, Athens, Greece, 2022.

[4] Dritsas, E.; Trigka, M. A Survey on Cybersecurity in IoT. *Future Internet* 2025, 17, 30. https://doi.org/10.3390/fi17010030

[5] National Institute of Standards and Technology (NIST), *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, vol. 2, 2021.

[6] E. Zeydan *et al.*, “Securing IoT with resilient cloud–edge continuum,” in *Proc. IEEE Int. Conf. on Cyber Security and Network Systems (ICCNS)*, 2024.

[7] O. P. Olawale and S. Ebadinezhad, “Cybersecurity anomaly detection: AI and Ethereum blockchain for a secure and tamperproof IoHT data management,” *IEEE Access*, vol. 12, pp. 1–18, 2024.

[8] A. Mahmoodi *et al.*, “Autonomous federated learning for distributed intrusion detection systems,” *IEEE Access*, vol. 11, pp. 1–16, 2023.

[9] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, n71, 2021.

[10] K. Kim, S. Park, and H. Choi, "Cybersecurity for industrial control systems: A survey," *IEEE Access*, vol. 9, pp. 142618–142643, 2021.

[11] J. Lin *et al.*, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[12] F. Pinheiro *et al.*, "Resilience in cyber-physical systems: State-of-the-art and research challenges," *Journal of Systems and Software*, vol. 190, 2022.

[13] E. Zeydan *et al.*, "Securing IoT with resilient cloud–edge continuum," *IEEE ICCNS*, 2024.

[14] O. P. Olawale and S. Ebadinezhad, "Cybersecurity anomaly detection: AI and Ethereum blockchain for secure IoHT data management," *IEEE Access*, vol. 12, 2024.

[15] N. J. van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[16] N. Nelufule *et al.*, "An adaptive digital forensic framework for the evolving digital landscape in Industry 4.0 and 5.0," in *Proc. IEEE Int. Conf. on Digital Industry and IoT (IDCIoT)*, 2024.

[17] R. Shabad *et al.*, "Anomaly detection in smart grids using machine learning," in *Proc. IEEE IECON*, 2021.

[18] H. Zhang and H. Zhang, "Anomaly detection and objective security evaluation in cyber-physical systems," *Sensors*, vol. 25, no. 3, 2025.

[19] K. Sivakumar *et al.*, "SCADA energy management system under distributed denial-of-service attack using verification techniques," in *Proc. IEEE ICSES*, 2023.

[20] M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen,

"A Lightweight Message Authentication Scheme for Smart Grid Communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp.

675–685, Dec. 2011.

[21] M. S. Alkatheiri et al., "Cyber security framework for smart home energy systems," Sustainable Energy, Grids and Networks, vol. 26, pp. 100424, 2021.

[22] National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, NIST Special Publication 800-207, 2020.

[23] H. Zhang *et al.*, "Anomaly detection and objective security evaluation for industrial cyber-physical systems," *Sensors*, 2025.

[24] Y. Zhao *et al.*, "Federated learning for edge computing: Principles and applications," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 450–473, 2022.

[25] A. Sgambelluri *et al.*, "AI-enhanced home energy management systems: Security and resilience perspectives," *IEEE Internet of Things Journal*, 2024.

[26] S. Shin *et al.*, "Blockchain-based lightweight security framework for IoT," *IEEE Access*, vol. 11, pp. 1–14, 2023.

[27] J. Li *et al.*, "Zero-trust architecture for edge-enabled critical infrastructures," *IEEE Transactions on Network and Service Management*, 2024.

[28] T. Park and Y. Won, "Energy-efficient cryptography for IoT devices," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9876–9888, 2022.

[29] D. R. Leitão *et al.*, "Federated learning for secure IoT: Challenges and opportunities," *ACM Computing Surveys*, vol. 56, no. 2, 2024.

[30] G. Zhang and W. Lee, "Anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 3456–3468, 2023.

[31] A. F. Costa and N. M. Coelho, "Evolving cybersecurity challenges in the age of AI-powered chatbots: A comprehensive review," in *Technological Innovation for Human-Centric Systems*, L. M. Camarinha-Matos and F. Ferrada, Eds., vol. 716. Cham, Switzerland: Springer, 2024, pp. 217–228, doi: 10.1007/978-3-031-63851-0_15.

[32] N. Mateus-Coelho, "A new methodology for the development of secure and paranoid operating systems," *Procedia Computer Science*, vol. 181, pp. 1207–1215, 2021, doi: 10.1016/j.procs.2021.01.318.

[33] N. R. Mateus-Coelho, B. R. Fonseca, and A. V. Castro, "POSMASWEB: Paranoid operating system methodology for anonymous and secure web browsing," in *Handbook of Research on Cyber Crime and Information Privacy*, M. M. Cruz-Cunha and N. Mateus-Coelho, Eds. Hershey, PA, USA: IGI Global, 2021, pp. 466–497, doi: 10.4018/978-1-7998-5728-0.ch023.

[34] N. Mateus-Coelho and M. Cruz-Cunha, Eds., *Exploring Cyber Criminals and Data Privacy Measures*. Hershey, PA, USA: IGI Global, 2023, doi: 10.4018/978-1-6684-8422-7.