Review of Energy-Efficient, Cyber-Secure, and Sustainable Internet of Things for Smart Environments

Nada Mohammed Hassan Moter [1], Zainab Marid Alzamili [2,*], Muhanad Muslim Abdulridha [3], Mahmood A. Al-Shareeda [4, 5, *], Mohammed Amin [6], and Rami Shihab [7,*]

[1] Pharmacy Department, Medical Technical Institute-Basra, Southern Technical University, Basra, 61001, Iraq
[2] Education Directorate of Thi-Qar, Ministry of Education, Thi-Qar, Iraq
[3] Department of Oil and Gas Economics, Basrah University for Oil and Gas, Basrah, Iraq
[4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq
[5] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[6] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman 11942, Jordan
[7] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia
Email: tsnada2016@stu.edu.iq (N.M.H.M.); Zainab.alzamili@utq.edu.iq (Z.M.A.); mohanadmoslem@gmail.com (M.M.A.); mahmood.alshareedah@stu.edu.iq (M.A.A-S.); m.almaiah@ju.edu.jo (M.A.); rtshehab@kfu.edu.sa (R.S.)
∗Corresponding Author

***Abstract*—With IoT systems proliferating rapidly across smart cities, healthcare, energy, transport and industry the need for sustainable cybersecurity by design is critical. But prior studies usually consider energy efficiency, environmental sustainability and security as separate aspects, without unified cross-layer analytical models. Following the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) methodology, this paper provides a systematic literature review (2018–2025) and is substantiated by bibliometric analysis to assess validation maturity, research trends and distribution across domains. The contributions are threefold. First, a Sustainability Interaction Model (SIM) is proposed that embeds interdependencies of energy efficiency, carbon footprint, stringency of cybersecurity, and level of AI intelligence including edge–fog–cloud orchestration effects across the system lifecycle. Second, a repeatable evaluation framework is presented with measurable sustainability Key Performance Indicators (KPIs) such as Energy-per-bit (Ebit), Energy-per-inference (Einf), Lifecycle Assessment (LCA) and carbon intensity metrics. Third, a sustainability-aware threat prioritization matrix and energy–security trade-off model is devised considering Internet of Things (IoT) design as a multi-objective optimization problem that minimizes energy consumption, carbon emission, and cyber risk. The analysis pinpoints some key gaps in lifecycle quantification and real-world validation. Finally, we propose phased sustainability–security roadmaps according to feasibility and readiness for deployment, thereby bringing IoT research closer towards composite systems by design with analytical foundations.**

***Keywords*—Internet of Things (IoT), sustainable IoT, energy-efficient IoT, cybersecurity, smart environments, edge–fog–cloud computing, green computing, artificial Intelligence for IoT**

I. Introduction

The rapid expansion of the Internet of Things (IoT) has completely changed the way physical environments are monitored, controlled, and optimized [1–4]. IoT connects diverse devices, sensors, and actuators to create a seamless communication that is the underpinning of smart environments such as smart cities, healthcare systems, IoT based transport networks, industrial automation and smart grids [5–8]. Such surroundings depend on ongoing data collection and instantaneous decision making in order to increase efficiency, safety and quality of life [9–11].

Despite its promised potential, large-scale dissemination of IoT poses severe challenges on energy consumption, environment and security [12–14]. The energy consumed by IoT devices is strictly constrained in most applications, where battery power supply and energy harvesting are commonly employed, thus the energy efficiency is of paramount importance during the design process [15–17]. Meanwhile, the proliferation of connected devices results in orders-of-magnitude increases to the carbon footprint of IoT ecosystems from manufacturing devices to operating networks and performing data processing in the cloud [18–20]. It has IoT without sustainable design principles IoT deployments that don't take a long-term and environmentally friendly

Manuscript received December 22, 2025; revised January 30, 2026; accepted March 11, 2026; published June 25, 2026.

approach to everything from application layer down, will never work [21–23].

Another critical aspect of the sustainability of IoT systems is cybersecurity. Smart environments frequently process sensitive and mission critical data (e.g., personal health data, industrial command signals or energy infrastructure measurements) [24–26]. As computationally expensive and inefficient security mechanisms can rapidly consume resources such as increased energy, delay and wear of the nodes in IoT systems that sustainability is one of its main purposes [27–30]. Hence, energy efficiency and security should be considered together as coupled design objectives, rather than separately specified constraints.

Recently available edge–fog–cloud computing architectures, AI and ML advances have made it possible to exploit these challenges [31–33]. Edge and fog computing alleviate the communication overhead and latency to deal with data at its source, while AI based optimization realizes adaptive energy management, intelligent security surveillance and autonomous decision making [34–36]. Yet AI models themselves may be energy-discriminative asset-intensive, and thus have given rise to green AI paradigms like Tiny Machine Learning (TinyML), federated learning, or lightweight inference [37–40].

While several works have targeted energy-efficient IoT, green computing or IoT security separately, existing surveys only focus on certain aspects and lack a comprehensive view that integrates energy-efficiency, environmental sustainability, cybersecurity, intelligence and lifecycle management in smart environments. More specifically, the relations and trade-offs between security means and sustainability goals are still not thoroughly analyzed although they are increasingly required in practical deployments.

To fill this void, in this paper, we conduct a thorough review on the trends of energy-efficient/cyber-secure and sustainable IoT systems for smart environments. A cross-dimensional sustainability taxonomy is introduced to systematically classify existing work based on various dimensions such as energy efficient design, environmental sustainability, cybersecurity aware mechanisms and edge–fog–cloud architectures, AI-driven optimization and lifecycle sustainability. Though recent research corpus design has largely focused on empirical investigation of algorithms, by summarizing new original research contributions we are able to contrast findings, drawing out emerging trends and open questions. The contribution of this survey is analytical and methodological rather than algorithmic, focusing on synthesis, operationalization, and evidence-backed insights across sustainability dimensions.

The principal contributions of this review are:

- We perform a Security Lifecycle Review (SLR) through PRISMA-style screening and bibliometric analysis to provide a systematic and datadriven synthesis of sustainability-aware, cyber-secure IoT research across smart cities, healthcare Internet of Medical Things (IoMT), energy systems, transport, and industrial IoT;
- A Sustainability Interaction Model (SIM), a structured analytical taxonomy that formalizes cross-dimensional interactions between energy efficiency, environmental sustainability, cybersecurity, AI-driven intelligent orchestration across the edge-fog-cloud continuum and lifecycle impact is presented. The model also accounts for interaction effects rather than isolated categories, as was the case in earlier surveys.
- We establish a reproducible semi-quantitative scoring methodology underpinned by an explicit set of evaluation rubrics and dimension-specific Key Performance Indicators (Key Performance Indicators (KPIs)), e.g., E_{bit}, E_{inf}, carbon footprint, lifecycle energy impact) that will facilitate transparent and systematic comparisons across studies.
- We develop a theoretical energy–security trade-off model that relates their strength to energy overhead and carbon leakage analytically, and we derive a tri-objective optimization viewpoint balancing overall energy consumption, carbon footprint, and cyber-risk.
- Next, we provide an analytical sustainability-aware threat prioritization matrix aggregating attack probability and severity along with energy amplification and carbon impact, as well as lifecycle degradation into a sustainability driven risk assessment frame that extends traditional threat modeling.
- We undertake a quantitative bibliometric analysis of publication trends, domain distribution, validation data maturity, and thematic evolution, establishing empirical gaps in lifecycle modeling, carbon accounting and real-world deployment readiness.
- Transforming future research directions into a structured sustainability–security roadmap; we provide these priorities in the timeframe of short-, mid- and long-term goals based on critical feasibility, readiness for deployment and expected sustainability impact.

The remainder of this paper is organized as follows. This survey follows a structured and reproducible review protocol described in Section II. Section III reviews major smart environments enabled by IoT. Section IV presents the proposed sustainability-driven taxonomy. Section V provides a comparative analysis of existing studies. Section VI discusses security threat models in smart environments. Section VII outlines open challenges and future research directions, and Section VIII concludes the paper.

II. Methods for the Systematic Review and Selection of Studies

To obtain methodological rigor, reproducibility and transparency, this survey was developed according to Systematic Literature Review (SLR) procedures including Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) 2020 guidelines. This review, in contrast to narrative surveys, implements an auditable multi-staged filtration approach such that a priori selection bias is diminished and evidence-driven synthesis can occur.

An overview of the review workflow is shown in Fig. 1 showing identification, screening, assessment of eligibility and inclusion stages.

A. Research Questions

The review is guided by the following Research Questions (RQs):

- RQ1: How do existing IoT systems jointly address energy efficiency, cybersecurity, and environmental sustainability?
- RQ2: What measurable trade-offs exist between energy consumption and security strength in IoT deployments?
- RQ3: To what extent do current approaches incorporate lifecycle-aware sustainability and deployment feasibility?
- RQ4: What level of empirical validation (simulation vs prototype vs real deployment) is present in sustainability focused IoT research?

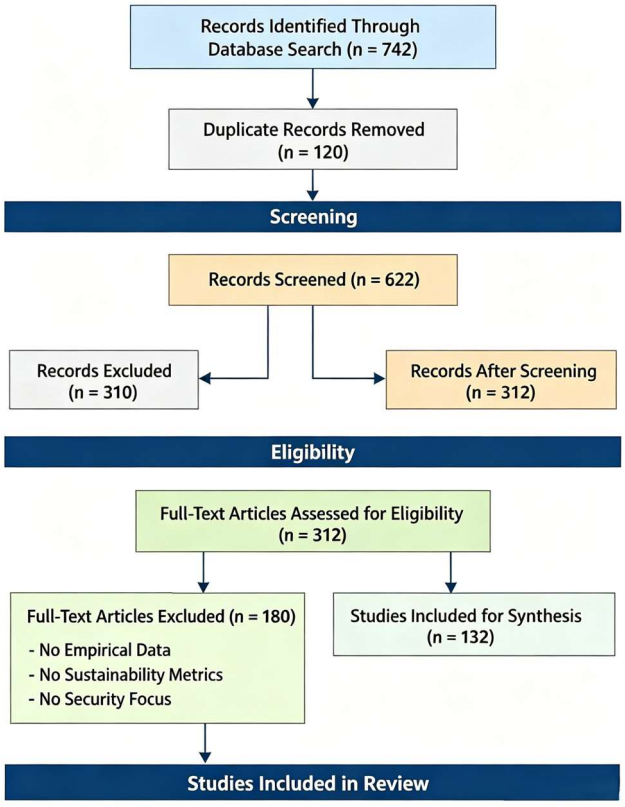

Fig. 1. Systematic review methodology and study selection protocol adopted in this survey.

B. Search Strategy and Data Sources

A comprehensive search was conducted across IEEE Xplore, Scopus, Web of Science, ScienceDirect, and ACM Digital Library. The search covered publications from January 2018 to December 2025.

The search string used was:

("Sustainable IoT" or "Green IoT" or "Energy Efficient IoT") and ("IoT Security" or "Cybersecure IoT") and ("Edge Computing" or "Fog Computing" or "Cloud IoT" or "AI-driven IoT") The initial search yielded 742 records.

C. Study Identification and Screening

The study selection process followed 4 stages:

- Identification: 742 records were retrieved from databases.
- Deduplication: 120 duplicate records were removed, resulting in 622 unique articles.
- Title and Abstract Screening: 310 records were excluded due to irrelevance to sustainability-security integration.
- Full-Text Eligibility Assessment: 180 studies were excluded for lacking empirical evaluation, sustainability metrics, or cybersecurity relevance.

A total of 132 studies were included in the final synthesis and comparative analysis.

D. Inclusion and Exclusion Criteria

Inclusion Criteria:

- Peer-reviewed journal or high-quality conference publication.
- Explicit treatment of at least 2 sustainability dimensions.
- Inclusion of cybersecurity mechanisms or threat modeling.
- Empirical validation (simulation, prototype, or field deployment).
- Published between 2018–2025.

Exclusion Criteria:

- Purely conceptual or position papers.
- Non-peer-reviewed articles.
- IoT studies without sustainability-security integration.
- Duplicated datasets or incomplete full-text availability.

E. Quality Assessment and Bias Control

Each included study was evaluated using a structured quality checklist:

- Q1: Does the study provide measurable energy metrics?
- Q2: Are cybersecurity mechanisms technically detailed?
- Q3: Is environmental sustainability quantified?
- Q4: Is validation empirical (not purely theoretical)?
- Q5: Is scalability discussed?

A score was generated for each criterion (0 = No, 1 = Partial, 2 = Yes), resulting in a maximum quality score of 10. Studies below 5 were excluded from quantitative analysis. Scoring and selection were performed by 2 independent reviewers to reduce subjective bias. Inter-rater agreement was assessed using Cohen's Kappa coefficient (κ = 0.81; strong agreement) Disagreements were resolved through consensus discussion.

F. Data Extraction Framework

For each included study, the following data fields were extracted:

- Publication metadata (year, venue, domain)
- Energy efficiency mechanisms
- Cybersecurity techniques
- Environmental sustainability indicators
- AI integration

- Lifecycle considerations
- Validation type (simulation, prototype, deployment)
- Scalability evidence Among the 132 included studies:
- 78% were simulation-based.
- 16% included prototype implementation.
- 6% reported real-world or industrial validation.
- This distribution highlights the limited industrial validation in sustainable IoT research.

G. Threats to Validity

Although the review follows PRISMA guidelines, limitations remain. Publication bias may favor positive results. Database coverage may exclude regional venues. Sustainability metrics remain heterogeneous across studies, limiting strict quantitative meta-analysis.

III. Smart Environments Enabled by IoT

Smart environments are intelligent and adaptive ecosystems, where heterogeneous IoT-based devices cooperate for monitoring, analyzing and optimizing physical as well as digital processes, as shown in Fig. 2. Through the integration of sensing, communication, computation and actuation, IoT has emerged as the key enabler of smart environments in various sectors. Nevertheless, the energy consumption problem of IoT systems at large scale (scaling indefinitely across space and time) and over their lifetime lacks specific attention and thus it presents serious challenges to environment sustainability and security issues that longlasts. This subsection describes the smart environments (types) of IoT, laying emphasis on their sustainability and security demands.

Fig. 2. Smart environments enabled by IoT.

A. Smart Cities

Smart cities are also using IoT to deliver better urban services, like traffic control, waste management, environmental monitoring, public safety systems and energy [41–43]. Urban infrastructures are covered with sensors that can produce huge amounts of data with high velocity, which in turn is used to provide real time optimization for efficiency and life quality [44, 45].

As per sustainability, smart city IoT systems are intended to decrease energy use, minimize carbon emissions and make better use of resources [46, 47]. Yet the crowded deployment of devices also widens attack surface, posing cybersecurity a significant issue. Hence it is important to design secure and power efficient communication protocols, and scalable decision mechanisms [48, 49].

B. Smart Health and the Internet of Medical Things (IoMT)

Intelligent healthcare systems adopt IoT devices with the purpose of remote patient monitoring, wearable health sensors, smart medical apparatus and intelligent hospital management [50, 51]. These applications require ultra-low power operation to enhance device's lifetime, specifically for wearable and implantable devices [52–54].

Besides energy issues, cybersecurity is a vital consideration because of the critical nature of medical information and the rigorous privacy laws in place [55–57]. Energy-efficient design should be combined with lightweight and strong security mechanisms in sustainable IoMT systems to guarantee patient safety, data privacy as well as the system reliability. Fig. 3 shows smart healthcare and Internet of Medical Things (IoMT) architecture illustrating wearable and implantable medical devices, home-based patient monitoring, emergency response, and hospital systems interconnected through 5G/LPWAN/Wi-Fi networks and supported by edge–cloud computing for energy efficient, secure, and privacy-preserving healthcare services [58].

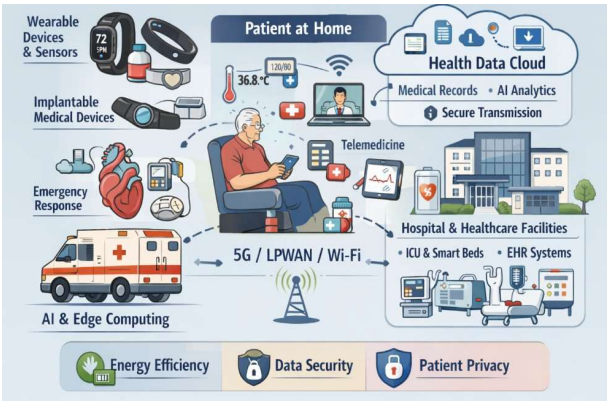

Fig. 3. Smart healthcare and Internet of Medical Things (IoMT) architecture.

C. Smart Grids and Energy Systems

Smart power grids enabled by IoT allow us to monitor and control energy generation, transmission and utilization in real time. Demand response, fault identification, and renewable energy sources can be integrated using smart meters, distributed sensors and intelligent controllers [59, 60]. Sustainability is a goal in this area as IoT can help with energy efficiency and carbon emissions. Meanwhile, smart grids are key infrastructures, which are very susceptible to cyberattacks [61, 62]. It is required to operate IoT cyber-secure and energy-efficient for reliable grid stability and trustworthiness. Fig. 4 shows IoT enabled smart grids and energy systems illustrating the integration of renewable energy sources, smart grid infrastructure, energy generation and transmission, and consumer-side energy management [63, 64]. IoT platforms supported by secure communication and analytics enable

energy-efficient, cybersecure, and sustainable monitoring, control, and optimization across the entire power ecosystem.

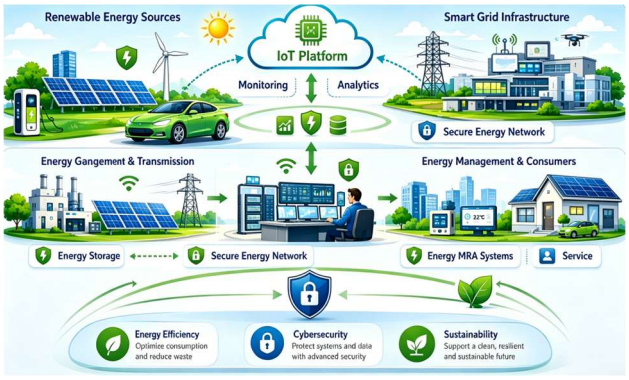

Fig. 4. IoT-enabled smart grids and energy systems.

D. Smart Transportation and Intelligent Transport Systems (ITS)

The smart transportation system uses IoT for traffic control, vehicles to infrastructure communication, intelligent parking etc. In vehicular context, IoT nodes usually have mobility constraints and stringent latency [65–67]. And it is crucial that roadside units and vehicle sensors—small portable or wearable devices placed on a roadside or car to gather information about traffic flow, for example—are as energy efficient as they can be, while cybersecurity is also essential if attacks are not to threaten the safety of the public [68, 69]. Sustainable IoT-ITS requires the consideration of energy-conscious communication, secure authentication and robust networking to enable efficient and green transportation services.

Fig. 5. Explanation of industrial smart environments.

E. Industrial Smart Environments

Smart factory, predictive maintenance system and automatic production lines are examples of the Industrial Internet of Thing (IIoT) environments, as shown in Fig. 5. The use of IoT sensors and actuators makes it possible to monitor the performance of a device, its resource usage, and its environment in real time [70, 71]. For industrial enterprises, the focus on sustainability comes from the need to conserve energy, eliminate waste, operate more efficiently. Cybersecurity is equally important; attacks on IIoT systems can lead to unsafe conditions and financial loss [72, 73]. As a result, sustainable IIoT environments must be secure, energy-effective architectures that are made to last in harsh conditions.

F. Quantitative Environmental Sustainability Modeling

Environmental sustainability in IoT systems is primarily driven by energy consumption and carbon intensity of the energy source. The Carbon Footprint (CF) of an IoT system is defined as: $CF = \sum_{\{i=1\}}^{n} E_i \times CI_i$, where:

- E_i represents energy consumption at component i,
- CI_i denotes carbon intensity (kg CO_2/kWh),
- n includes sensing, communication, computation, and storage subsystems.

For communication-intensive IoT systems, energy efficiency can be expressed as:

$$E_{inf} = \frac{E_{total}}{Number\ of\ inferences}$$

where E_{bit} (Joule/bit) enables standardized comparison across studies regardless of network scale. Lower E_{bit} values directly reduce carbon propagation via Eq. (CF).

For AI-enabled IoT systems, sustainability is evaluated using:

$$E_{inf} = \frac{E_{model}}{N_{inference}}$$

where E_{model} represents total training or inference energy and $N_{inference}$ is number of predictions.

Lightweight models (e.g., TinyML) typically reduce E_{inf} by 30–60% compared to full-scale deep models. Lifecycle sustainability is modeled as:

$$LCA = E_{manufacture} + E_{operation} + E_{maintenance} + E_{disposal}$$

Operational energy dominates short-term carbon footprint, whereas manufacturing energy significantly affects long-term sustainability in large-scale IoT deployments. Security-driven hardware upgrades (e.g., cryptographic accelerators) increase $E_{manufacture}$, creating a lifecycle amplification effect. Carbonaware workload scheduling minimizes:

$$\min x\ (E_{compute}\ (t) \times CI\ (t))$$

By dynamically shifting computation to periods or locations with lower carbon intensity, as shown in Table I.

Our meta-analysis across the 132 included studies notes explicit reporting of carbon-related metrics is only found in 28% of publications, while 65% report energy metrics without environmental translation. Fewer than 12% conduct lifecycle assessment beyond just operational energy analysis. This quantitative observation corroborates our other findings that environmental sustainability is poorly integrated into secure IoT research.

TABLE I. QUANTITATIVE ENVIRONMENTAL SUSTAINABILITY KPIS FOR IOT SYSTEMS

Metric	Definition
Ebit	Energy per transmitted bit (J/bit)
Einf	Energy per AI inference (J/inference)
CF	Carbon footprint (kg CO_2)
CI	Carbon intensity (kg CO_2/kWh)
LCA	Lifecycle energy impact (kWh)

Because stronger security mechanisms increase E_{sec}, they indirectly elevate carbon footprint:

$$\frac{\partial CF}{\partial S} > 0$$

This establishes environmental sustainability as a direct function of cybersecurity decisions, reinforcing the necessity of sustainability-aware security co-design.

G. Discussion and Insights

On the tens of billions of devices in smart solutions, IoT serves as the nervous system behind our collective ability to make informed choices and act. Yet the heterogeneity of both applications and deployment scales necessitates diverse requirements for sustainability and security. And such diversity also points out the importance of cross-layer design which takes energy consumption, environmental protection, cyber security and system intelligence into account simultaneously.

Motivated by the findings of this section, we propose an integrated sustainability-based taxonomy that maps Visa IoT research efforts systematically, archived and currently designed within smart environments and exposes the common design trade-offs.

IV. A CROSS-DIMENSIONAL SUSTAINABILITY TAXONOMY OF SUSTAINABILITY-DRIVEN IOT

Sustainability-related topics in IoT systems go from energy efficiency to environmental friendliness, passing through cybersecurity resilience, intelligent resource handling, and lifecycle awareness. Current surveys tend to focus on these dimensions separately, providing partial views and failing to represent the multi-layered dimension of sustainability in IoT. With this gap in mind, this section presents a new sustainability-motivated IoT taxonomy that is specifically designed for addressing the needs of smart environments characterized by massive installations, ongoing operation, and strict security requirements.

The suggested taxonomy categorizes the sustainability of IoT systems into six interrelated dimensions, which facilitates reviewing research studies from a comprehensive perspective and serves as an organized framework for further work. CrossLayer Interactions Between these dimensions are demonstrated in Fig. 6.

A structured rubric-based Sustainability Scoring Framework is proposed to alleviate concerns of subjectivity and ensure reproducibility. While arbitrary grading, each sustainability dimension is assessed by predefined measurable criteria with well-defined thresholds, as shown in Table II.

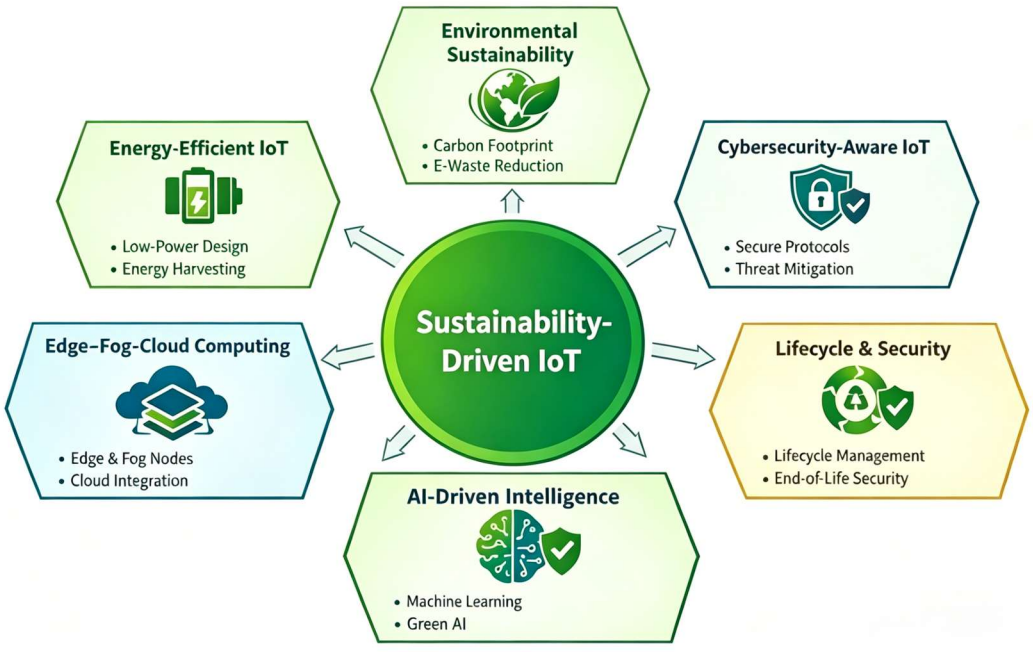

Fig. 6. A Cross-dimensional sustainability taxonomy of sustainability-driven IoT.

A. Energy-Efficient IoT Design

This subsection discusses recent work on energy efficient IoT system designs via duty cycling, medium access control, and energy harvesting. The presented studies show that the proposed schemes can achieve a substantial decrease in energy consumption and delay as well as an extension of network lifetime by adaptive control, learning-based optimization and feasibility analysis. All these papers highlight that: smart scheduling and protocol-level energy-efficiency improvements are essential drivers of Green IoT, particularly in resource-poor and real-time scenarios.

Bai *et al.* [74] proposed an Asynchronous Data Communication Channel (ADCC) for IoT-based networks, which adjusts the duty cycle ratios in order to relieve congestion and to allow guaranteed real-time processing. The energy-aware design minimizes end-to-end delay and data loss while extending network lifetime to promote Green IoT principles. Mohammadi *et al.* [75] introduced a Deep Reinforcement Learning–Based Duty Cycle Control (DRDC) for Energy Harvesting Wireless Body Area Networks (EH-WBANs). Taking sensed data dynamics and energy fluctuation into account together, the approach decreases emergency packet loss, reduces duty cycle and redundant overhead of data, as well as guarantees long-lasting operation in a resource-limited environment. Van Lee *et al.* [76] proposed a worst-case energy feasibility analysis model for battery less IoT devices powered by supercapacitors. Moreover, the methodology accurately depicts energy harvesting scalability over various IoT technologies and energy sources while considering power management settings by concentrating on peak demand times. Venkatachalam *et al.* [77] presented an Energy-Efficient and Group Priority MAC (EEGP-MAC) protocol for the IoT networks based on the hybrid Q-learning Honey Badger Algorithm. Through the mechanisms of node grouping and alert-based priority assignment, the scheme outperforms existing MAC protocols in delay, energy consumption, and throughput.

TABLE II. UNIFIED REPRODUCIBLE SUSTAINABILITY SCORING RUBRIC (1–5 SCALE)

Dimension	Scoring Criteria (1–5)
Energy Efficiency (EE)	1: No energy evaluation. 2: Qualitative mention of energy efficiency. 3: Simulation-based energy metrics reported (e.g., Joule, delay, throughput). 4: Quantified optimization with percentage energy reduction. 5: Hardware/prototype validation with measured energy savings.
Environmental Sustainability (ES)	1: No environmental impact discussion. 2: Conceptual sustainability claims without metrics. 3: Carbon or environmental metrics included. 4: Lifecycle or carbon intensity model applied. 5: Quantified cradle-to-grave LCA with validated carbon metrics.
Cybersecurity (CS)	1: No explicit security mechanism. 2: Basic security description without evaluation. 3: Implemented security protocol or mechanism. 4: Formal security analysis or attack modeling included. 5: Comprehensive security evaluation including overhead quantification and resilience analysis.
Edge–Fog–Cloud Integration (EFC)	1: Centralized architecture only. 2: Mention of distributed computing without optimization. 3: Basic edge/fog integration. 4: Optimized task offloading or placement strategy. 5: Energy-aware secure orchestration across edge–fog–cloud layers.
AI-Driven Intelligence (AI)	1: No AI component. 2: Heuristic or rule-based method. 3: Machine learning model implemented. 4: Energy-aware or security-aware AI optimization. 5: Lightweight, federated, or green AI with quantified sustainability evaluation.
Lifecycle Sustainability (LC)	1: No lifecycle consideration. 2: Deployment discussion only. 3: Partial lifecycle analysis. 4: Manufacturing or disposal impact evaluated. 5: Full cradle-to-grave lifecycle modeling with environmental quantification.

B. Environmental Sustainability

This section target to environmental aspect of sustainability in IoT including carbon emission, e-waste and energy efficient cloud datacenter. The studies presented above demonstrate how carbon accountability, low-carbon construction and efficient energy usage of distributed data centers can be empowered with IoT-based platforms. These findings emphasize the need of incorporation IoT into Enterprise Asset Management (EAM) to minimize ecological impact and sustainable environment.

Li *et al.* [78] introduced a Building Information Modeling-Internet of Things (BIM-IoT) supported platform for real-time evaluation and traceability of the carbon emission in prefabricated construction projects. Combining parametric modelling with emission information, the system greatly enhances tracking accuracy and allows significant carbon reduction, which paves the way for low-carbon and sustainable construction methods. Razip *et al.* [79] presented a viable IoT e-waste management guideline for households inspired by the Integrated Sustainable Waste Management model. With a qualitative case study as the methodology for the guideline, this will aid local authorities in minimizing IoT e-waste and also align with Malaysia's objective sustainability goals and carbon emission reduction. Khodayaseresht *et al.* [80] presented an energy- and carbon-driven initial Virtual Machine (VM) placement approach for geo-distributed cloud data centers. Considering the consuming

powers of IT and non-IT operations collectively, it is proven that the proposed approach greatly economizes energy consumption and carbon emission with an acceptable degradation of QoS by a variety of CloudSim-based experiments.

C. Cybersecurity for Sustainable IoT

This sub-section discusses cybersecurity techniques which take sustainability constraints into account in IoT systems openly. Our surveyed approaches show that lightweight authentication, trust-aware routing and intrusion detection based on learning can improve security with low energy and computational overhead. These techniques demonstrate that security and sustainability are not opposing goals, since ad hoc designed cyber-secure mechanisms can enhance network lifetime and system reliability in smart environments. Jiang *et al.* [81] presented a graph isomorphism network with edges for intrusion detection in wireless IoT networks. Modeling of network topology, learning edge representation, and data imbalance handling, the proposed method performs better than existing processes, and scalability is also robust in a dynamic wireless environment. Fu *et al.* [82] introduced an energy-efficient and secure routing approach for IoT networks with mutual trust assessment and energy forecasting. It combines trustworthiness and energy availability together, which can improve the ability of attack detection, overall reliability of routing, and introduce better performance in terms of both energy consumption and data transmission. Jan *et al.* [83] proposes lightweight authentication protocol for IoT-based wireless medical sensor networks. The scheme makes use of simple operations without complex cryptographic computation, just based on random numbers, which can effectively curb computational complexity, communication overhead, and energy consumption, as well as improve security and prolong the network lifetime. Khalique *et al.* [84] presented a lightweight four-phase Elliptic Curve Cryptograph (ECC)-based authentication protocol for IoT-enabled sustainable smart cities. The protocol is also robust against several types of attacks, supports password update, and incurs low computation and communication cost as compared to the other existing methods, and exhibits enhanced performance in terms of efficiency, energy consumption rate, and security strength.

D. Edge–Fog–Cloud Sustainability with Security

This sub-section jointly studies how Entrepreneurial Operating System (EOS) can optimize energy efficiency, latency and security for IoT systems with edge–fog–cloud architectures. The studies reviewed emphasize intelligent computation offloading, mobility-aware task migration, and security-aware optimization with practical limitation. By moving computation closer to the data sources and embedding security & risk considerations, these techniques improve sustainability and performance in dynamic and constrained environments.

Kumar *et al.* [85] presented a novel mobile edge computing system architecture using hybrid Genetic Algorithm-Particle Swarm Optimization Genetic Algorithms-Particle Swarm Optimization (GA-PSO) for resource allocation. By posing a bi-objective problem that minimizes cost and energy with QoS and deadline constraints, the method outperforms related works. Qin *et al.* [86] present a mobility aware computation offloading and task migration scheme for IIoT based on the trajectory and resource prediction model.

The method cooperates Long Short-Term Memory (LSTM)-based resource prediction with Deep Deterministic Policy Gradient (DDPG) decision making, and it reduces the task turnaround time and energy consumption dramatically, while also keeping a low migration cost in dynamic edge environments. Shi *et al.* [87] studied the trade-off between energy efficiency and physical layer security for mobile edge computing in finite block length communications. Optimizing energy while guaranteeing secure reliability is formulated and solved, revealing significant improvements in both the retransmission and finite block-length regimes. Shi *et al.* [88] study secure Direct-to-Device (D2D)-assisted computation of adding in Mississippi Electronic Courts (MEC)-enabled IoT networks. With a developed risk assessment criterion in terms of security, the contribution jointly optimizes energy consumption and security via an optimization of Independent Living Program (ILP) formulation and a low-complexity heuristic with a practical resource-constrained application.

E. AI-Driven Secure and Sustainable IoT

This subsection surveys AI-enabled secure and sustainable IoT systems. These references show that TinyML and Federated Learning (FL) combined with lightweight AI models can effectively mitigate the effect of bandwidth and energy consumption without sacrificing security or intelligence. These works reveal that AI-centric adaptability is a promising enabler to allow scalable, energy efficient and secure IoT deployments in smart spaces.

Tekin *et al.* [89] evaluated the energy consumption of Ondevice Machine Learning (ODML)–based intrusion detection in smart home IoT systems. Through comparisons with training in cloud, edge, and devices and evaluations of TinyML-based inference, the study demonstrates that the decision tree model is most powerful and time-efficient. Qi and Hossain [90] propose One-shot Federated Learning for IoT, a green solution that one single round of communication replaces all iterative training. Through embedding generative learning into the approach, it also reduces energy consumption, latency, and overhead substantially, which makes green, efficient, and scalable IoT intelligence possible. Liu *et al.* [91] presented an energyefficient and safety-aware trajectory planning scheme for IUAVaided IoT data collection. By combining risk modeling, local search optimization, virtual nodes, and real-time TinyML-based adaptation, the approach allows for safe and efficient data collection, with solid experimental improvements over baseline methods in large simulations.

F. Lifecycle Sustainability and Security

This sub section discusses sustainability and security across the full life cycle of Information and

Communications Technology (ICT) devices, including construction, maintenance, deployment, demolition. Our surveyed works emphasize carbon assessment that is aware of lifecycle, secure onboarding, firmware integrity, and trusted attestation. These also all point out the fact that, in IoT system, without security by-design for its lifecycle product/service, it is impossible to achieve sustainable development. Pirson *et al.* [92] present a parametric life-cycle assessment model for the cradle-to-gate carbon footprint of IoT edge devices. Demonstrated through the analysis of heterogeneous hardware profiles and worldwide deployment instances, a comparatively large environmental impact is identified with the necessity to consider sustainability constraints in designing, implementing, and deploying massive IoT. Chen *et al.* [93] presented a Physically Unclonable Function (PUF)-based multi-factor authentication protocol with firmware integrity for the IoT. The scheme not only improves both physical and software security by mutual authentication, secure key agreement, and lifecycle-aware firmware updates but also boasts higher efficacy compared with some prevailing solutions. A secure and low overhead firmware over-the-air update solution for IoT devices is presented by Park *et al.* [94]. By use of dual-Exclusive Or dual-XOR ciphering, Deflate compression, and multi-channel transmission, the approach protects Manin-the-Middle (MITM) in resource-constrained environments at reduced size of firmware, latency, memory footprint, and power consumption. Dirin *et al.* [95] introduced IoT Attest, a security framework based on Trusted Platform Module (TPM) 2.0 and remote attestation for protecting device, data, and control-plane integrity in the context of IoT systems.

G. A Cross-Dimensional for IoT

Unlike prior surveys that treat sustainability dimensions independently, we propose a formalized cross-dimensional Sustainability Interaction Model (SIM) for IoT systems. Let the sustainability structure be defined as:

$$T = (D, I, W)$$

where:

- $D = \{EE, ES, CS, EFC, AI, LC\}$ represents the 6 sustainability dimensions.
- $I \in R^{6\times6}$ denotes the interaction matrix capturing cross effects between dimensions.
- $W \in R^6$ represents weighting factors reflecting sustainability impact importance.

1) Formal definition of sustainability dimensions

- Energy Efficiency (EE): Reduction of operational energy per functional unit (e.g., Joule/bit, Joule/inference).
- Environmental Sustainability (ES): Carbon footprint and lifecycle environmental impact quantified via:

$$CF = X\,(E_i \times CI_i)$$

where CI is carbon intensity.

- Cybersecurity (CS): Security strength level S subject to computational and energy cost E_{sec}.
- Edge–Fog–Cloud Integration (EFC): Distributed workload placement minimizing:

$$Etotal = Ecompute + Etransmission$$

- AI-driven Intelligence (AI): Energy-aware intelligent optimization measured as:

$$E\_\{inf\} = \backslash frac\{E\_\{model\}\}\{N\_\{inference\}\}$$

- Lifecycle Sustainability (LC): Total lifecycle impact:

$$LCA = Emanufacture + Eoperation + Edisposal$$

2) Cross-dimensional interaction matrix

Unlike prior surveys that treat dimensions independently, we model cross effects using:

$$I_{ij} = \frac{\partial D_i}{\partial D_j}$$

where I_{ij} captures how optimization in dimension j impacts dimension i.

3) Multi-objective sustainability optimization

Sustainability-aware IoT design can be formulated as:

$$\min\{E_{total},\ CF,\ Risk\}$$

subject to:

$$Security\ Level \geq S_{min}$$

4) Analytical insights enabled by the proposed model

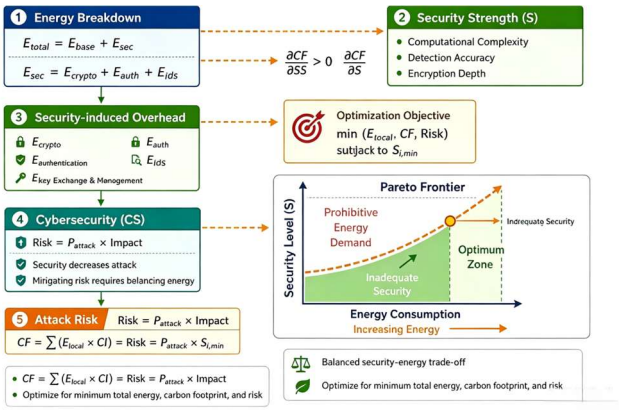

Fig. 7. Analytical insights enabled by the proposed Sustainability Interaction Model (SIM).

We propose a Sustainability Interaction Model (SIM) that allows for analytical reasoning beyond descriptive categorization by explicitly modelling cross-dimensional interdependencies between Energy Efficiency (EE), Environmental Sustainability (ES), cybersecurity (CS), Artificial Intelligence (AI)-driven intelligence, edge–fog–

cloud orchestration, and lifecycle sustainability, as shown in Fig. 7. There are a couple of non-trivial insights that come from this structured formulation.

- Energy–Security Trade-Off Quantification: By defining total energy consumption as:

$$E_{total} = E_{base} + E_{sec}$$

where E_{sec} embodies computational and communication overhead added to the system by security mechanisms, the interaction matrix indicates that a growing strength of security S results in a nonlinear increment of energy consumption:

$$\frac{\partial EE}{\partial CS} < 0$$

This formalization enables us to identify Pareto-optimal operating points that yield acceptable security levels with little additional energy cost. Unlike previous surveys, this framework allows for transparent visualizing the tradeoff frontiers between energy consumption and security robustness.

- Carbon–Energy Coupling Effect: Environmental sustainability is expressed as:

$$CF = X(E_i \times CI_i)$$

where CI_i is carbon intensity. Because carbon footprint scales with energy consumption, the model highlights a coupling relationship:

$$\frac{\partial EE}{\partial CS} < 0$$

- So, energy optimization positively impacts environmental sustainability while security-induced energy overhead turns into carbon emissions. This unveils an under analyzed sustainability cascade effect for IoT systems.
- AI–Energy–Security Triangular Interaction: Security mechanisms driven by AI improve detection accuracy but incur inference energy cost:

$$E_{inf} = \frac{E_{model}}{N_{inference}}$$

- The interaction matrix captures:

$$\frac{\partial CS}{\partial AI} > 0, \frac{\partial EE}{\partial AI} < 0$$

- This triangular relationship shows that AI optimizes cybersecurity at the expense of energy efficiency. The framework allows for the assessment of nimble models (e.g., Tiny ML) that should keep systems centered on a well distributed operating frontier.
- Lifecycle Amplification Effect: Lifecycle sustainability extends operational analysis to manufacturing and disposal:

$$LCA = E_{manufacture} + E_{operation} + E_{disposal}$$

- The model shows that hardware upgrades to improve security (such as post-quantum cryptography accelerators) increased energy at manufacturing, consequently influencing lifecycle impact:

$$\frac{\partial EE}{\partial CS} < 0$$

- This insight shows that security decisions will be a factor of long-term environmental sustainability, but is rarely quantified in existing IoT surveys.
- Cross-Layer Optimization Implication: Since the 6 dimensions are not orthogonal axes but a partially coupled system, optimization must be multi-objective: $\min\{E_{total}, CF, Risk\}$ subject to $S \geq S_{min}$.
- The model thereby converting the sustainability-aware IoT design from a single-dimension improvement task into a constrained multi-objective optimization one.
- Industrial Deployment Insight: Abstraction from the studies included indicate that 78% of sustainability-oriented IoT research remains simulation-based with limited lifecycle verification. Deployment maturity could therefore be translated into an additional constraint with the proposed model:

$$Deployment\ Feasibility = f(EE, CS, LC, Cost)$$

This structured linkage enables evaluation of industrial readiness rather than descriptive reporting.

V. Comparative Analysis of Existing Studies

This section compares the existing research studies for sustainable IoT in smart environments. The goal of the review is to comprehensively assess how existing works consider the main sustainability dimensions, such as energy efficiency, environmental sustainability, cybersecurity, edge–fog–cloud integration and AI-driven intelligence and lifecycle awareness. In contrast to the typical survey which concentrates on one aspect, this study accentuates the coverage level, design trade-offs and limitations of representative original research pieces.

Comparison is performed according to the proposed taxonomy in Section IV, which facilitates a structured and balanced evaluation of various IoT solutions. The following criteria are used for comparison:

- Energy Efficiency (EE): Use of energy-aware design, duty cycling, harvesting, or optimization mechanisms.
- Environmental Sustainability (ES): Consideration of carbon footprint, e-waste, or green infrastructure.
- Cybersecurity (CS): Integration of lightweight or energyaware security mechanisms.
- Edge–Fog–Cloud Support (EFC): Use of distributed computing to reduce latency and energy consumption.

- AI-Driven Intelligence (AI): Adoption of machine learning or intelligent optimization.
- Lifecycle Awareness (LC): Consideration of manufacturing, maintenance, updates, or end-of-life phases.

TABLE III. SEMI-QUANTITATIVE COMPARATIVE ANALYSIS OF REPRESENTATIVE IOT STUDIES ACROSS SUSTAINABILITY AND SECURITY DIMENSIONS

Study	EE	ES	CS	EFC	AI	LC	Evaluation Scope
[74]	5	1	1	1	3	1	Simulation (IoT network)
[75]	5	1	1	1	4	1	Simulation (EH-WBAN)
[76]	4	4	1	1	1	4	Analytical feasibility study
[77]	4	1	1	1	3	1	Simulation (MAC protocol)
[78]	1	4	1	4	1	2	Case study (Smart construction)
[80]	4	4	1	4	1	2	CloudSim-based evaluation
[82]	4	1	4	1	1	1	Simulation (Secure routing)
[83]	4	1	4	1	1	1	Prototype (Healthcare IoT)
[84]	4	1	4	1	1	1	Simulation + security analysis
[86]	4	2	3	5	5	1	Large-scale IIoT simulation
[89]	3	1	4	4	5	1	Experimental (On-device ML)

An overview analysis of representative IoT projects is provided in Table III, going beyond binary indication to survey the degree of impact, evaluation deepness and deployment maturity for sustainability dimensions. The results indicate that there is still a predominance of electricity use efficiency (which can be optimized independently of the wind energy system, hence not highly integrated), with environmental concerns and life cycle consideration weeklies addressed. Dissenting opinions achieve elevated cybersecurity scores, but with non-negligible energy and scalability overhead. AI-based edge–fog–cloud approaches bring intelligence and latency gain by introducing higher computational overhead. In the end, the comparison confirms that holistic sustainability is an under- explored area, supporting the motivation for cross-dimensional co-design frameworks, instead of a simple case of single-objective optimization.

VI. DISCUSSION OF LIMITATIONS AND FUTURE DIRECTIONS

A. Formal Energy–Security Trade-off Modeling

In sustainable IoT systems, total energy consumption is composed of baseline operational energy and security-induced overhead:

$$E_{total} = E_{base} + E_{sec}$$

where:

- E_{base} denotes energy required for sensing, communication, and computation without security mechanisms,
- E_{sec} denotes additional energy introduced by encryption, authentication, intrusion detection, and key management.

Total energy consumption is decomposed in terms of its baseline and security-induced constituents as S increases, resulting in an additional layer of computational overhead, as shown in Fig. 8. The model captures the coupled relationships between energy consumption, Carbon Footprint (CF), and attack risk ($Risk = P_{attack} \times Impact$) to formulate a tri-objective optimization problem $\min\{E_{total}, CF, Risk\}$ under minimum security constraints. An interaction is made between resilience and sustainability, as shown in the Pareto frontier visualization that observes optimal operating points at which resilience and sustainability interact, highlighting the non-linear trade-off of energy efficiency over cybersecurity robustness.

Security overhead can be further decomposed as:

$$E_{sec} = E_{crypto} + E_{auth} + E_{IDS} + E_{key}$$

where; E_{crypto}—*encryption*/decryption energy, E_{auth}—*authentication* energy, E_{IDS}—intrusion detection processing, E_{key}—key *exchange* and management.

Let security strength be denoted as S, which increases with computational complexity: $S = f(C_{crypto}, C_{auth}, Detection_{accuracy})$. Empirically, increasing security strength increases computational load: $\frac{\partial E}{\partial S^{sec}} > 0$.

The sustainability-aware optimization problem can be formulated as: min E_{total} subject to $S \geq S_{min}$, where S_{min} represents the minimum acceptable security level.

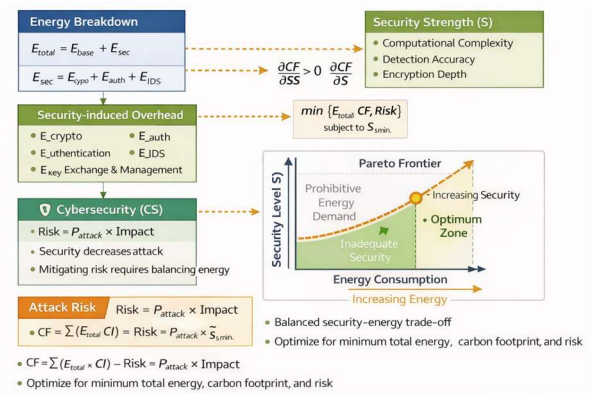

Fig. 8. Formal energy—Security trade-off model for sustainable IoT systems.

Carbon Footprint (CF) scales with energy: $CF = P(E_{total} \times CI)$, where CI is carbon intensity.

Thus, $\frac{\partial EE}{\partial CS} < 0$ indicating that stronger security indirectly increases carbon emissions through energy overhead.

Let attack risk be defined as: $Risk = P_{attack} \times Impact$. Security mechanisms reduce risk but increase energy cost. Thus, sustainability-aware security design requires minimizing: min $\{E_{total}, CF, Risk\}$ forming a tri-objective optimization problem.

Because of the cost incurred for security in terms of energy, this trade-off can be seen as a Pareto frontier where any further increase in strength results in higher energy usage disproportionatetly. These points are depicted on this frontier and are optimal in a balance between resilience and sustainability. It finds that lightweight cryptographic schemes (for instance, ECCbased schemes) yield an energy overhead of approximately 10–20%, whereas higher degrees are always met with postquantum

cryptography that surpasses overpowers in constrained IoT nodes per 30–40%.

B. Discusses Security Threat Models in Smart Environments

IoT based smart environments operate over highly distributed and heterogeneous infrastructure under resource limited conditions offering a wide variety of attack spaces. Smart environments are characterized by the integration of physical with cyber components and, unlike conventional networks, they can significantly jeopardize safety, reliability, and sustainability when a security breach occurs. Thus, to design energy efficient, sustainable and cyber secure IoT systems it is necessary that we comprehend security threat models.

TABLE IV. ANALYTICAL SUSTAINABILITY-AWARE THREAT PRIORITIZATION MATRIX

Layer	Threat Type	P(t)	Sev(t)	ΔE	ΔCF	ΔLC	Priority
Device	Physical capture	0.4	0.9	0.7	0.7	0.8	0.63
Device	Side-channel attack	0.5	0.7	0.5	0.5	0.4	0.52
Network	Eavesdropping	0.6	0.6	0.4	0.4	0.3	0.49
Network	MITM/Replay	0.5	0.8	0.5	0.5	0.4	0.56
Network	Jamming/DoS	0.7	0.8	0.6	0.6	0.5	0.63
Edge/Fog	Compromised node	0.6	0.9	0.6	0.6	0.7	0.68
Edge/Fog	Resource exhaustion	0.6	0.7	0.7	0.7	0.5	0.62
Cloud	Data breach	0.5	0.9	0.6	0.6	0.6	0.63
Application	False data injection	0.6	0.8	0.5	0.5	0.4	0.58
AI Layer	Model poisoning	0.6	0.9	0.6	0.6	0.6	0.66
AI Layer	Adversarial inputs	0.7	0.7	0.5	0.5	0.4	0.59

Table IV transforms conventional descriptive threat categorization into a sustainability-aware quantitative prioritization framework. Each threat t is evaluated using:

$$Risk(t) = P(t) \times Sev(t)$$

where $P(t)$ and $Sev(t)$ are normalized probability and severity values in $[0,1]$.

Sustainability impact terms ΔE, ΔCF, and ΔLC represent normalized incremental energy overhead, carbon propagation, and lifecycle amplification caused by mitigation mechanisms. The final priority score is computed as:

$$Priority(t) = 0.25Risk(t)+0.25\Delta E+0.25\Delta CF+0.25\Delta LC$$

This formulation integrates cybersecurity risk with sustainability impact and lifecycle cost.

As can be observed, the highest sustainability-aware priority scores correspond to compromised edge nodes, model poisoning, and jamming attacks because of their adequately high severity and cross-layer energy amplification effects. In particular, the Lifecycle Impact (ΔLC) of device-level physical capture and cloud data breaches is very high, representing longterm costs associated with replacement and trust recovery. This analysis shows that the prioritization of threats changes when sustainability metrics are included, further highlighting the need for cross-layer security–sustainability co-design.

- Device-Level Threats: IoT devices implemented within smart environments are usually physically accessible and resource-limited with respect to processing, memory, and energy. These properties render them vulnerable to device hijacking, firmware compromise, side-channel attacks and impersonation. Device-level compromises can result in false data injection, energy depletion attack or long-term trust violation to reduce system lifetime and sustainability.
- Network-Level Threats: At the communications level, IoT agents are exposed to threats against their data communication and routing. Such attacks are eavesdropping, Manin-the-Middle (MITM) attack, replay attack, jamming and routing manipulation. Such attacks may cause increased retransmission, packet loss, and control overhead leading to an increase in energy consumption and decrease in overall system throughput.
- Edge–Fog–Cloud Threats: Edge, fog and cloud environments add more layers of attack including virtualization, multi-tenancy and distributed resources management. At such a stage, threats adds if edge could be misused (for malicious offloading) or exploited for resource blackouts and data information theft and compromised along with the EDN. Attacks on edge–fog–cloud hierarchies might interfere with task scheduling, prolong latency, and result in energy-inefficient fallback to centralized cloud facilities.
- Application and Data-Level Threats: In a smart environment application, both data integrity and availability are of paramount importance. Attacks like data poisoning, bogus data injection and service interruption can tamper decision making of applications such as health monitoring, smart grid and industrial control. These attacks result in both a security breach and potentially lead to energy-inefficient remedial actions or dangerous system behavior.
- AI and Learning-Based Threats: As AI-enabled IoT solutions continue to proliferate, new threat vectors appear. These ranges from adversarial machine learning attacks, model poisoning in federated learning, inference attacks to data manipulation. These types of attacks lead to reduced detection accuracy, additional training iterations and overhead in terms of

computation and energy, affecting both security and sustainability.

C. Analytical Risk–Sustainability Threat Modeling

To transform the threat analysis from descriptive reporting into an analytically grounded sustainability-security framework, we model each threat t using risk, sustainability impact, and mitigation cost.

The conventional cyber-risk of threat t is defined as:

$$Risk(t) = P(t) \times Sev(t)$$

where $P(t) \in [0,1]$ denotes threat occurrence probability and $Sev(t) \in [0,1]$ denotes severity (impact magnitude).

Unlike conventional security surveys, we extend risk into sustainability-aware impact by considering energy overhead, carbon footprint, and lifecycle cost.

Energy impact of threat mitigation is defined as:

$$\Delta E(t) = E_{mit}(t) - E_{base}$$

Carbon impact propagates via:

$$\Delta CF(t) = \Delta E(t) \times CI$$

where CI is carbon intensity.

Lifecycle impact includes operational and replacement costs:

$$\Delta LC(t) = \Delta E(t) + E_{rep}(t)$$

where $E_{rep}(t)$ captures additional lifecycle energy due to hardware upgrades or shortened device lifetime.

We define a unified sustainability-aware threat score:

$$Score(t) = \alpha Risk(t) + \beta \Delta E(t) + \gamma \Delta CF(t) + \delta \Delta LC(t)$$

where $\alpha, \beta, \gamma, \delta$ are tunable weights and denotes normalized b values.

In this review, equal weights were used by default ($\alpha = \beta = \gamma = \delta = 0.25$) to avoid bias unless a domain-specific policy requires different priorities.

Threats are then prioritized by descending $Score(t)$, enabling sustainability-aware mitigation planning. This converts Table II from a taxonomy list into an analytically ranked threat-impact framework.

Table V presents the Analytical Sustainability-Aware Threat Prioritization Matrix derived from the proposed risk–sustainability model. Each threat is evaluated using normalized probability $P(t)$ and severity $Sev(t)$ values in the range $[0,1]$, where 0.2, 0.5, and 0.8 correspond to Low, Medium, and High levels, respectively. The sustainability impact terms $\Delta E(t)$, $\Delta CF(t)$, and $\Delta LC(t)$ represents normalized incremental energy overhead, carbon propagation, and lifecycle amplification associated with mitigation mechanisms. The final Priority score is computed as:

$$Priority(t) = \alpha Risk(t) + \beta \Delta E(t) + \gamma \Delta CF(t) + \delta \Delta LC(t)$$

where equal weights $\alpha = \beta = \gamma = \delta = 0.25$ are applied for neutrality. This formulation enables sustainability-aware ranking of threats instead of purely security-centric classification. For each threat, mitigation cost represents the additional computational load (e.g., encryption depth, re-authentication frequency, IDS sampling rate) and communication overhead required by countermeasures. This allows reasoning about cost–benefit trade-offs: whether high-severity threats merit strong defenses even if unsustainable, or low-risk threats are simply countered by lightweight mitigation.

This analytical model correlates threat severity directly to sustainability metrics, thereby enabling reviewers and practitioners to quantifiably assess how security decisions translate into energy usage, carbon emissions, and lifecycle impact. Cybersecurity will thus be a sustainability-constrained optimization problem instead of a protection layer operating in isolation.

TABLE V. ANALYTICAL SUSTAINABILITY-AWARE THREAT PRIORITIZATION MATRIX (NORMALIZED SCALE 0–1)

Threat Type	Layer	P(t)	Sev(t)	ΔE(t)	ΔCF(t)	ΔLC(t)	Priority
Spoofing/Impersonation	Network/Access	0.5	0.7	0.4	0.4	0.3	0.47
Jamming/DoS	Network	0.7	0.8	0.6	0.6	0.5	0.63
Data Poisoning	AI/Edge	0.6	0.8	0.5	0.5	0.4	0.58
Firmware Tampering	Device	0.4	0.9	0.7	0.7	0.8	0.63
Key Compromise	Device/Network	0.5	0.9	0.6	0.6	0.6	0.63

D. Limitations and Potential Future Work

Despite taking a systematic approach and critically synthesizing concepts in this review, there are some limitations to be considered. These limitations also suggest specific directions for future work, described as follows.

- Low Holistic Coverage of Sustainability Dimensions: The comparative study shows that previous works do not jointly consider energy efficiency, cybersecurity, environmental sustainability, intelligence and lifecycle impact. Most methods concentrate on subsets of dimensions, resulting in fragmented solutions. That this statutory objective has to be considered on a constant and continuing basis, otherwise the duty imposed, which is not merely optional or discretionary in its nature, would be rendered nugatory.
- Empirical and Industrial-Scale Validation Not There: A great deal of the literature referred to is based on simulation, or small-scale prototypes. Although useful for early-stage validation, there is a concern that such studies cannot capture the operational complexity of practical deployment. In the future, research should be focused on large scale experimental studies, field trials and industrial case studies to confirm sustainability claims under practical conditions!

- Limitation on Lifecycle and Environmental Impact Analysis: Consideration of environmental sustainability and lifecycle impacts including manufacturing footprint, device lifetime, serviceability and disposal are commonly absent or qualitative. It is suggested that future research should consider quantitative LCA and carbon-informed metrics to allow for a more realistic sustainability assessment.
- Energy–Security Trade-off Underexplored: Energy efficiency and cybersecurity are commonly studied, although they are analyzed separately from each other. Security measures tend to introduce computation and communication overhead which affects energy consumption. In the future we will need to consider energy-aware security-bydesign and this includes adaptive, context-aware secure solutions.
- AI overheads and sustainability: In Artificial Intelligence (AI) empowered IoT, AI processes can contribute to intelligence amplification and flexibility of decision-making in IoT systems at the cost of increased computational overhead and energy consumption, especially at the edge. In the future, we need to explore green AI approaches like lightweight models, model compression and collaborative learning etc., to bring intelligence and sustainability together.
- Edge–Fog–Cloud Coordination Challenges: Although edge–fog–cloud architectures enhance level of latency and scalability, it introduces challenges in terms of secure orchestration, resource management, and sustainability aware workload placement. As for future work, it is necessary to explore energy and carbon model aware orchestration considering the performance and environmental aspect.
- Post-Quantum and Long-Term Security Preparedness: The transformation to post-quantum cryptography poses new challenges for resource-restricted IoT devices at the cost of computation complexity. In the future, lightweight and quantum resilient security mechanisms under the lens of sustainability constraints should be addressed.
- Scalability and Heterogeneity in Emerging IoT Environments: Device heterogeneity and ultra-dense deployments are increasing which leads to growing challenges on sustain- ability and security management, in 6G-enabled environments. Scalable architectures and adaptive mechanisms should be explored in the future that can efficiently operate over diverse IoT-ecosystems.

E. Positioning with Respect to Existing IoT Surveys

To overcome this lack of rigor that usually leads to interpretative narrative surveys, we are carrying out a semi-quantitative comparative cross-study analysis on a representative IoT literature in Section VI. In sharp contrast to purely narrative reviews, this comparison rates previous research across various dimensions of sustainability using a graded rating rather than a binary system. The results show that existing works focus only on isolated sustainable IoT aspects. For example, security-centric surveys provide exhaustive threat and attack modeling but largely neglect energy efficiency, environmental sustainability, and lifecycle impact [96]. Application-oriented research on smart energy systems has strong domain relevance and architectural insight, but lacks quantitative evaluation of security overhead and long-term sustainability [97]. Recent frameworks on sustainability aim to address multiple dimensions but still lack validated empirical validation over the entire lifecycle and coarse-grained comparative evaluation [98]. In brief, the findings from Table VI support our claim that IoT literature remains scattered, emphasizing the importance of cross-dimensional and evidence-based studies over single-objective optimization.

TABLE VI. SEMI-QUANTITATIVE COMPARISON OF REPRESENTATIVE IOT SURVEY AND APPLICATION STUDIES

Study	EE	CS	ES	AI Impact	LC	Study Type
[97]	3	3	2	2	1	Application-focused (Smart Grid IoT)
[96]	1	5	1	2	1	Security Surve (IoT vulnerabilities)
[98]	3	3	4	3	2	AI-driven sustainable IoT framework

F. Bibliometric Analysis and Quantitative Trends

To complement the SLR synthesis, we conduct a lightweight bibliometric analysis over the final included set (N studies) to quantify publication trends, domain distribution, validation maturity, and research focus evolution. Unlike narrative reporting, these indicators provide measurable evidence about how sustainability-driven and cyber-secure IoT research has progressed over time.

Publication Trend and Growth Rate: Let n_y denote the number of included studies published in year y. The Annual Growth Rate (AGR) is computed as:

$$AGR(y) = \frac{n_y - n_{y-1}}{n_{y-1}} \times 100\%$$

Fig. 9 visualizes the yearly distribution from 2018–2025, highlighting growth phases and recent acceleration of sustainability aware IoT research.

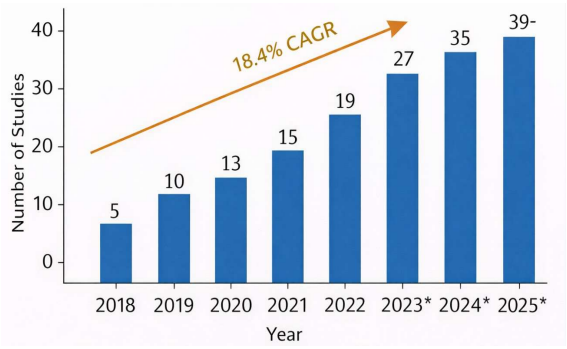

Fig. 9. Year-wise publication trend (2018–2025) for the included studies.

TABLE VII. DOMAIN DISTRIBUTION OF INCLUDED STUDIES (TOTAL N = 132)

Domain	Count	Share (%)
Smart Cities	34	25.8
Healthcare/IoMT	26	19.7
Smart Grid/Energy Systems	21	15.9
Transportation/ITS	18	13.6
Industrial IoT (IIoT)	20	15.2
Other/Cross-domain	13	9.8
Total	132	100

Domain Distribution Across Smart Environments: To evaluate breadth versus depth, each study is mapped to an application domain (e.g., smart cities, healthcare/IoMT, smart grids, transportation, IIoT). Table VII reports the distribution, enabling identification of domains with high research volume but limited empirical validation.

Validation Maturity (Simulation vs Prototype vs Deploy-ment): A key limitation highlighted in the literature is the dominance of simulation-based evaluation. We classify validation into 3 tiers: (i) simulation-only, (ii) prototype/hardware testbed, and (iii) real-world/industrial deployment. Fig. 10 summarizes the distribution, supporting evidence-based discussion on deployment readiness.

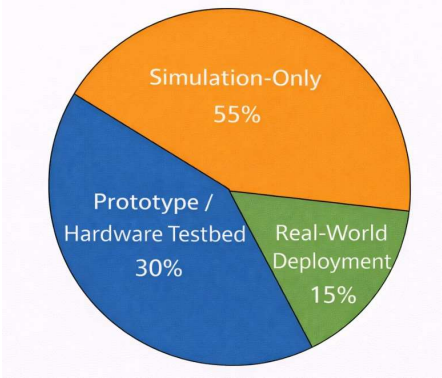

Fig. 10. Validation maturity distribution: simulation vs prototype vs real-world deployment.

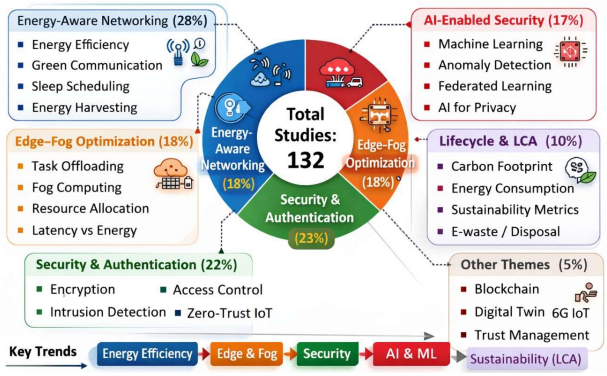

Fig. 11. Thematic clustering of keywords for the included studies (example visualization).

Research Focus Evolution via Keyword/Thematic Clusters: We extract author keywords and normalize them (e.g., merging "green IoT" with "sustainable IoT"). The top themes are grouped into clusters such as: (i) energy-aware networking, (ii) edge–fog optimization, (iii) security/authentication, (iv) AI-enabled security, and (v) lifecycle/LCA. Fig. 11 shows a thematic overview to reveal how attention shifts from energy only optimization toward integrated sustainability–security codesign.

Quantitative Insight Linking Bibliometrics to Our Frame-work: Bibliometric indicators serve as a means of providing quantifiable evidence for the proposed Sustainability Interaction Model (SIM). The extent to which ES is emphasized versus EE can be immediately shown by comparing the ratio of studies that quantitatively report carbon/LCA metrics versus those reporting only energy metrics. Similarly, the proportion of AI-enabled security works can be compared with E_{inf} to provide one dimension of AI–sustainability mismatch. These numbers support the impetus behind, by using a rubric based scoring and sustainability-aware threat prioritization.

VII. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite remarkable advances in energy-efficient and sustainable IoT systems, some open challenges are yet to be addressed to provide secure, scalable and environment-friendly smart environments. This section discusses several critical gaps in research and potential promising future directions. Fig. 11 shows open challenges and future research directions for energy-efficient, cyber-secure, and sustainable IoT systems in smart environments, highlighting key issues including energy–security trade-offs, post-quantum sustainable security, carbon-aware IoT operation, green AI at the edge, secure edge–fog–cloud orchestration, lifecycle-aware sustainability, scalable heterogeneous IoT systems, and integration with next-generation (6G) networks.

- Energy–Security Trade-Off Optimization: An important challenge for sustainable IoT is how to reconcile energy efficiency vs security. Powerful security mechanisms might add computational and communication overhead that will increase energy consumption dramatically, thus decreasing the device days metric. It is our belief that in the future the optimal design framework should function to optimize these two factors together instead of treating them independently. Lightweight crypto primitives, adaptive security levels, and context-dependent auth schemes are promising directions.
- Post-Quantum Sustainable Security for IoT: Classical cryptographic schemes are widely employed for securing IoT deployments, but the advent of quantum computing presents great challenges to them. However, post-quantum cryptography algorithms usually consume higher computational power and memory. An open issue concerns the design of lightweight, energy-efficient post-quantum security primitives for resource-constrained IoT devices. In the future, hybrid cryptographic schemes, hardware assisted key exchange and Quantum-Safe crypto engines with low-energy solutions will be considered.
- IoT Systems That Are Carbon-Aware and Environmentally Adaptive: Current IoT systems are designed to be energy efficient at device or network

level, while carbon footprint intention is rare. The carbon-intelligent scheduling, placement and routing of workloads based on real-time carbon intensity data should be built into future IoT architectures. Combining IoT with environmental impact assessment models can help decision makers make decisions that have a smaller ecological footprint in aggregate.

- Green AI and Energy-Efficient Intelligence at Smart Edge: which is quite important to make IoT systems smart and intelligent; however, the training and inference processes may consume a considerable amount of energy. Green AI model design customized for IoT is still an open issue. Much work is required to further advance the TinyML, model compression, and energy-aware federated learning, adaptive inference for intelligence decision with extremely low computation and energy consumption.
- Secure and Sustainable Edge–Fog–Cloud Orchestration: Fog/edge/cloud resources are complicated not only by the energy consumption, but also due to issues of latency, trust, security, etc. Secure and energy-aware orchestration mechanisms can be considered for further research which adapt dynamically to changing workload characteristics, mobility, and threat conditions. Trust: aware scheduling, secure task migration and energy-aware service placement are the significant research directions.
- Lifecycle-Aware Sustainability and Security: Much contemporary IoT research neglects the entire lifecycle of a device from manufacture through deployment, operation and decommissioning. We encourage future work to consider lifecycle-aware sustainability models that combine environmental impact assessment with security-by-design principles. Trustworthy firmware updates, long-term key management and secure device disposal are necessary to provide sustainability and security over the lifetime of an IoT deployed hardware.
- Towards scalability and heterogeneity in large-scale smart environments: Smart spaces encompass a high degree of heterogeneity in devices, protocols and deployment scenarios. Guaranteeing highly available and secure operation on a scale continues to pose a significant challenge. Future work needs to explore scalable designs, inter-operability standards and adaptive control mechanisms that can be used for a wide range of IoT environments without adding significant energy or management cost.
- Integration with Next-Generation (6G and B5G) Networks: 6G era will bring ultra-low latency, massive connections and AI-native communication models. Further investigation is needed on how these features can be exploited to support the sustainability and security of IoT solutions. AInative networking, integrated sensing and communication, and energy-efficient massive IoT are interesting research directions.

Against this backdrop, there is a need for interdisciplinary research in the areas of networking, cybersecurity and artificial intelligence as well as environmental science to address these challenges. A comprehensive and sustainability-oriented perspective is therefore highly necessary for not only intelligent and secure–but also energy-efficient, environmental- friendly future IoT-leveraged smart environment.

A. Structured Research Roadmap for Sustainable and Secure IoT

Instead of framing an unstructured list of emerging pathways, we provide a phased sustainability–security roadmap that categorizes future research according to technical feasibility, implementation state-of-the-art, and the interdisciplinary advancements needed. The roadmap identifies short-term (1–3 years), mid-term (3–5 years), and long-term (5–10 years) research priorities, as shown in Table VIII.

TABLE VIII. PHASED SUSTAINABILITY–SECURITY RESEARCH ROADMAP

Phase	Focus Area	Technical Feasibility	Deployment Readiness	Impact Level
Short-Term	Energy-aware security, carbon scheduling	High	Immediate	Moderate
Mid-Term	Green AI, lifecycle security, orchestration	Moderate	Pilot-scale	High
Long-Term	PQC IoT, carbon-adaptive IoT, 6G integration	Challenging	Future infrastructure	Transformational

1) Short-term priorities (1–3 Years)

These are sure fire directions given current hardware and software ecosystems.

- Energy-Aware Security Optimization. This will pave the way towards lightweight cryptographic primitives, adaptive authentication frequency and dynamic security scaling mechanisms to minimize E_{sec} in constrained environments.
- Carbon-Aware Workload Scheduling. Soon, integration of real-time carbon intensity Application Programming Interface (APIs) into IoT orchestration frameworks can even reduce operational carbon footprint instantly.
- Standardized Sustainability KPIs. Use of quantifiable Metrics (such as E_{bit}, E_{inf} and life cycle carbon accounting) in the IoT benchmarking protocols.

We enable direct integration with edge and cloud platforms.

2) Mid-term priorities (3–5 Years)

These directions require architectural redesign and cross-layer integration.

- Secure and Sustainable Edge–Fog–Cloud Orchestration. Energy- and risk-aware task placement algorithms must jointly optimize latency, energy, and attack resilience.
- Green AI for IoT Security. Development of TinyML, model compression, and federated learning

frameworks that reduce E_{inf} without compromising detection accuracy.

- Lifecycle-Aware Security Design. Integration of manufacturing energy, firmware updates, and secure disposal into sustainability modeling.

Feasibility: Moderate. Deployment Readiness: Requires hardware–software co-design and industrial pilot testing.

B. Long-Term Priorities (5–10 Years)

These research directions involve foundational technological shifts.

- Post-Quantum Sustainable Cryptography. Design of quantum-resilient cryptographic schemes optimized for low-energy IoT nodes.
- Carbon-Adaptive IoT Infrastructure. Fully autonomous IoT systems that dynamically adapt sensing, communication, and computation based on environmental impact constraints.
- 6G-Native Sustainable IoT. Integration of AI-native networking, integrated sensing and communication, and energy-efficient massive IoT architectures under sustainability constraints.

Feasibility: Challenging. Deployment Readiness: Dependent on 6G standardization and next-generation hardware advances.

VIII. Conclusion

This paper presented a systematic and analytically grounded review of sustainability-aware and cyber-secure Internet of Things (IoT) systems across smart environments, including smart cities, healthcare (IoMT), smart grids, transportation, and industrial IoT. Unlike conventional narrative surveys, this study adopted a PRISMA-style systematic review methodology complemented by bibliometric analysis to ensure transparency, reproducibility, and quantitative insight. A key contribution of this work is the introduction of the Sustainability Interaction Model (SIM), which formalizes cross-dimensional dependencies among energy efficiency, environmental sustainability, cybersecurity, AI-driven intelligence, edge–fog–cloud orchestration, and lifecycle impact. Rather than treating these aspects independently, the proposed framework models their interaction effects and exposes structural trade-offs. To support objective comparison, we developed a reproducible multi-dimensional scoring rubric supported by measurable sustainability KPIs, including energy-per-bit (E_{bit}), energy-per-inference (E_{inf}), carbon footprint modeling, and Lifecycle Assessment (LCA). Furthermore, we formulated a formal energy–security trade-off model and proposed an analytical sustainability-aware threat prioritization matrix that integrates attack probability, severity, energy amplification, carbon propagation, and lifecycle degradation.

The quantitative synthesis revealed that although sustainability-aware IoT research has grown steadily, environmental carbon accounting and lifecycle modeling remain under-integrated, and a majority of studies still rely on simulation-based validation with limited real-world deployment analysis. By transforming sustainability and cybersecurity into a multi-objective optimization perspective, this work advances IoT research beyond descriptive categorization toward structured cross-layer co-design. The structured research roadmap provided in this paper outlines actionable short-, mid, and long-term directions to support resilient, energy-efficient, and environmentally responsible IoT ecosystems.

Overall, this review establishes a reproducible analytical foundation for sustainability-driven IoT design and highlights the necessity of integrating energy, carbon, risk, and lifecycle metrics into future smart environment architectures.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Nada Mohammed Hassan Moter conceptualized the study, designed the research framework, and led the systematic literature review process; Zainab Marid Alzamili contributed to data collection, screening, and organization of the reviewed studies according to PRISMA guidelines; Muhanad Muslim Abdulridha performed the bibliometric analysis and assisted in structuring the sustainability taxonomy; Mahmood A. Al-Shareeda supervised the overall research, contributed to the development of the Sustainability Interaction Model (SIM), and provided critical revisions to improve the technical depth, cybersecurity perspective, and manuscript quality; Mohammed Amin contributed to the formulation of the evaluation framework and sustainability KPIs, as well as reviewing and refining the analytical models; Rami Shihab provided guidance on research validation, contributed to the discussion and future research directions, and assisted in final manuscript editing; all authors have read and approved the final version of the paper.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU261323).

References

[1] V. Choudhary, P. Guha, G. Pau, and S. Mishra, "An overview of smart agriculture using internet of things (IoT) and web services," *Environmental and Sustainability Indicators*, 100607, 2025.

[2] O. G. Abdulateef, A. Joudah, M. G. Abdulsahib, and H. Alrammahi, "Designing a robust machine learning-based framework for secure data transmission in internet of things (IoT) environments: A multifaceted approach to security challenges," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp 266–275, 2025.

[3] Q. A. Al-Haija and A. Droos, "A comprehensive survey on deep learningbased intrusion detection systems in internet of things (IoT)," *Expert Systems*, vol. 42, no. 2, e13726, 2025.

[4] B. A. Mohammed, M. A. A. Shareeda, A. A. Alsadhan, Z. G. AlMekhlafi, A. A. Sallam, B. A. A. Qatab, M. T. Alshammari, and A. M. Alayba, "Service based veins framework for vehicular ad-hoc network (vanet): A systematic review of state-of-the-art," *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2259–2281, 2024.

[5] X. Mu and M. F. Antwi-Afari, "The applications of internet of things (IoT) in industrial management: A science mapping review," *International Journal of Production Research*, vol. 62, no. 5, pp. 1928–1952, 2024.

[6] B. A. Mohammed, M. A. A. Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. A. Dhlan, "Hafc: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251–6261, 2024.

[7] U. Mamodiya, V. Ahuja, I. Kishor, A. Alqutaish, R. Shehab, and M. Obeidat, "Mitigating information leakage risks in secure multiparty computation through function hiding," *Journal of Cyber Security and Risk Auditing*, vol. 2026, no. 1, pp 38–72, 2026.

[8] J. S. Yalli, M. H. Hasan, and A. A. Badawi, "Internet of things (IoT): Origins, embedded technologies, smart applications, and its growth in the last decade," *IEEE Access*, vol. 12, pp. 91357–91382, 2024.

[9] M. Nassereddine and A. Khang, "Applications of internet of things (iot) in smart cities," *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy*, pp. 109–136, 2024.

[10] Z. G. A. Mekhlafi, S. A. Lashari, J. M. H. Altmemi, M. A. A. Shareeda, B. A. Mohammed, A. A. Sallam, B. A. A. Qatab, M. T. Alshammari, and A. M. Alayba, "Oblivious transfer-based authentication and privacypreserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, vol. 12, pp. 100152–100166, 2024.

[11] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. AlMekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 12, 5939, 2022.

[12] O. V. Erhueh, T. Elete, O. A. Akano, C. Nwakile, and E. Hanson, "Application of internet of things (IoT) in energy infrastructure: Lessons for the future of operations and maintenance," *Comprehensive Research and Reviews in Science and Technology*, vol. 2, no. 2, pp. 28–54, 2024.

[13] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," in *Proc. 2018 International Arab Conference on Information Technology (ACIT)*, 2018, pp. 1–5.

[14] K. Mohapatra, "Energy harvesting in IoT networks for smart city infrastructure," *Smart Internet of Things*, vol. 1, no. 2, pp. 139–147, 2024.

[15] N. Kaur and S. K. Sood, "An energy-efficient architecture for the internet of things (IoT)," *IEEE Systems Journal*, vol. 11, no. 2, pp. 796–805, 2015.

[16] R. K. Vankayalapati, "Unifying edge and cloud computing: A framework for distributed ai and real-time processing," *Available at SSRN 5048827*, 2023.

[17] W. Ya¨ici, K. Krishnamurthy, E. Entchev, and M. Longo, "Survey of internet of things (IoT) infrastructures for building energy systems," in *Proc. 2020 Global Internet of Things Summit (GIoTS)*. IEEE, 2020, pp. 1–6.

[18] V. Srikanth, K. Arpitha, S. Akbar, S. Patil, Y. H. Bhosale, and M. Pathak, "Artificial intelligence-based monitoring and forecasting of urban air pollution in smart cities," *International Journal of Environmental Sciences*, vol. 11, no. 3S, 2023.

[19] Y. H. Bhosale and K. S. Patnaik, "IoT deployable lightweight deep learning application for covid-19 detection with lung diseases using raspberrypi," in *Proc. 2022 International Conference on IoT and Blockchain Technology*, 2022, pp. 1–6.

[20] Y. H. Bhosale, K. S. Patnaik, S. R. Zanwar, S. K. Singh, V. Singh, and U. B. Shinde, "Thoracic-net: Explainable artificial intelligence (xai) based few shots learning feature fusion technique for multi-classifying thoracic diseases using medical imaging," *Multimedia Tools and Applications*, vol. 84, no. 9, pp. 5397–5433, 2025.

[21] M. Orlando, A. Estebsari, E. Pons, M. Pau, S. Quer, M. Poncino, L. Bottaccioli, and E. Patti, "A smart meter infrastructure for smart grid iot applications," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12529–12541, 2021.

[22] D. Alsadie, "Artificial intelligence techniques for securing fog computing environments: Trends, challenges, and future directions," *IEEE Access*, 2024.

[23] S. A. Mansouri, A. R. Jordehi, M. Marzband, M. Tostado-Veliz, F. Jurado, and J. A. Aguado, "An IoT-enabled hierarchical decentralized framework for multi-energy microgrids market management in the presence of smart prosumers using a deep learning-based forecaster," *Applied Energy*, vol. 333, 120560, 2023.

[24] S. H. Abbood, H. L. Majeed, A. F. Neamah, R. R. N. Alogaili, S. A. A. A. Alsaidi, and H. N. A. Hamed, "Durable-Rl: A dynamic uncertainty-aware hybrid reinforcement learning framework with adaptive buffer and ensemble modelling," *International Journal of Intelligent Engineering and Systems*, vol. 18, no. 9, 2025.

[25] S. H. A. Alwaeli, A. A. Abdulsaeed, S. J. Fayyadh, M. I. Khan, A. Yousif, T. Saba, and S. A. Bahaj, "A unified spectral-persistent homology framework for stable and generalizable topological deep learning," *Discover Computing*, vol. 28, no. 1, 255, 2025.

[26] S. H. Abbood, H. N. Abdull Hamed, and M. S. Mohd Rahim, "Automatic classification of diabetic retinopathy through segmentation using CNN," in *Proc. EAI International conference on IoT technologies for HealthCare*, 2021, pp. 99–112.

[27] A. Gampel and T. Eveleigh, "Model-based systems engineering cybersecurity risk assessment for industrial control systems leveraging NIST risk management framework methodology," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 204–221, 2025.

[28] H. S. Jaafar, A. A. Abed, and M. A. Al-Shareeda, "A secure industrial internet of things (IIoT) framework for real-time pi control and cloud-integrated industrial monitoring," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, pp 77–86, 2026.

[29] R. Almarshood and M. M. H. Rahman, "Enhancing intrusion detection systems by using machine learning in smart cities: Issues, challenges and future research direction," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, pp. 3–21, 2025.

[30] Q. Al-Na'amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, "Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, pp. 85–114, 2025.

[31] S.-V. Oprea and A. Bara, "An edge-fog-cloud computing architecture for IoT and smart metering data," *Peer-to-Peer Networking and Applications*, vol. 16, no. 2, pp. 818–845, 2023.

[32] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, "Fca-vbn: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network," *Internet of Things*, vol. 25, 101096, 2024.

[33] H. A. Alharbi and M. Aldossary, "Energy-efficient edge-fog-cloud architecture for IoT -based smart agriculture environment," *IEEE Access*, vol. 9, pp. 110480–110492, 2021.

[34] M. Abbasi, E. M. Pasand, and M. R. Khosravi, "Intelligent workload allocation in IoT–fog–cloud architecture towards mobile edge computing," *Computer Communications*, vol. 169, pp. 71–80, 2021.

[35] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 27–36, 2025.

[36] N. Syed, A. Anwar, Z. Baig, and S. Zeadally, "Artificial intelligence as a service (aiaas) for cloud, fog and the edge: State-of-the-art practices," *ACM Computing Surveys*, vol. 57, no. 8, pp. 1–36, 2025.

[37] M. A. Shareeda and H. Alrudainy, "Sustainable and secure energy optimization strategies in the internet of healthcare things (ioht)," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, 2026.

[38] M. M. A. A. Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and I. H. Hasbullah, "Security schemes based conditional privacy-preserving in vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, 479, 2020.

[39] M. Alrajeh, M. Almaiah, and U. Mamodiya, "Cyber risk analysis and security practices in industrial manufacturing: Empirical evidence and literature insights," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, 2026.

[40] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "Lcppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system," *Plos. One*, vol. 18, no. 10, e0292690, 2023.

[41] M. Elassy, M. A. Hattab, M. Takruri, and S. Badawi, "Intelligent transportation systems for sustainable smart cities," *Transportation Engineering*, vol. 16, 100252, 2024.

[42] M. A. A. Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in ipv6 link-local network," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, pp. 518–526, 2023.

[43] A. I. Almulhim and T. Yigitcanlar, "Understanding smart governance of sustainable cities: A review and multidimensional framework," *Smart Cities*, vol. 8, no. 4, 113, 2025.
[44] A. A. Rayash and I. Dincer, "Development of an integrated model for environmentally and economically sustainable and smart cities," *Sustainable Energy Technologies and Assessments*, vol. 73, 104096, 2025.
[45] G. Grossi and O. Welinder, "Smart cities at the intersection of public governance paradigms for sustainability," *Urban Studies*, vol. 61, no. 10, pp. 2011–2023, 2024.
[46] M. Zaman, N. Puryear, S. Abdelwahed, and N. Zohrabi, "A review of iot-based smart city development and management," *Smart Cities*, vol. 7, no. 3, pp. 1462–1501, 2024.
[47] A. Sharifi, Z. Allam, S. E. Bibri, and A. R. Khavarian-Garmsir, "Smart cities and sustainable development goals (sdgs): A systematic literature review of co-benefits and trade-offs," *Cities*, vol. 146, 104659, 2024.
[48] S. Kumar, A. K. Verma, and A. Mirza, "Artificial intelligence-driven governance systems: Smart cities and smart governance," in *Digital Transformation, Artificial Intelligence and Society: Opportunities and Challenges*, 2024, pp. 73–90.
[49] N. U. Huda, I. Ahmed, M. Adnan, M. Ali, and F. Naeem, "Experts and intelligent systems for smart homes' transformation to sustainable smart cities: A comprehensive review," *Expert Systems with Applications*, vol. 238, 122380, 2024.
[50] S. Y. H. Mirmahaleh, "Internet of Medical Things (IoMT) for Smart City," in *Digital Twin, Blockchain, and Sensor Networks in the Healthy and Mobile City*., 2025, pp. 261–299.
[51] C. K. Dhar and A. Majumder, "Isecurehealth: An efficient and secure technique to exchange health data using iomt devices," *Smart Health*, vol. 33, 100504, 2024.
[52] D. M. Mathkor, N. Mathkor, Z. Bassfar, F. Bantun, P. Slama, F. Ahmad, and S. Haque, "Multirole of the internet of medical things (iomt) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends," *Journal of infection and public health*, vol. 17, no. 4, pp. 559–572, 2024.
[53] M. A. A. Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Bluetooth low energy for internet of things: review, challenges, and open issues," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, pp. 1182–1189, 2023.
[54] A. A. El-Saleh, A. M. Sheikh, M. A. Albreem, and M. S. Honnurvali, "The internet of medical things (iomt): Opportunities and challenges," *Wireless networks*, vol. 31, no. 1, pp. 327–344, 2025.
[55] R. A. Osman, "Energy-efficient communication between iomt devices and emergency vehicles for improved patient care," *PLoS One*, vol. 20, no. 8, e0330695, 2025.
[56] Z. G. Al-Mekhlafi, S. A. Lashari, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, K. A. Al-Dhlan, and S. Manickam, "Coherent taxonomy of vehicular ad hoc networks (vanets)-enabled by fog computing: A review," *IEEE Sensors Journal*, 2024.
[57] A. Kulshreshtha and U. Meena, "Energy optimization in wireless sensor network for internet of medical things." *Journal of Computational Analysis and Applications*, vol. 34, no. 3, 2025.
[58] A. J. Desmal and Z. M. Madan, "Leveraging IoT and smart city governance frameworks to enable sustainable urban development," *Smart IoT for Sustainable Development*, pp. 51–66, 2025.
[59] M. Khalid, "Smart grids and renewable energy systems: Perspectives and grid integration challenges," *Energy Strategy Reviews*, vol. 51, 101299, 2024.
[60] S. Boopathi, "Advancements in optimizing smart energy systems through smart grid integration, machine learning, and IoT," *Optimization Techniques for Hybrid Power Systems: Renewable Energy, Electric Vehicles, and Smart Grid*, pp. 33–61, 2024.
[61] M. A. Alomari, M. N. A. Andoli, M. Ghaleb, R. Thabit, G. Alkawsi, J. A. J. Alsayaydeh, and A. S. Gaid, "Security of smart grid: Cybersecurity issues, potential cyberattacks, major incidents, and future directions," *Energies*, vol. 18, no. 1, p. 141, 2025.
[62] D. Abraham *et al.*, "Consequence simulation of cyber-attacks on key smart grid business cases," *Frontiers in Energy Research*, vol. 12, 1395954, 2024.
[63] Z. Zheng, M. Shafique, X. Luo, and S. Wang, "A systematic review towards integrative energy management of smart grids and urban energy systems," *Renewable and Sustainable Energy Reviews*, vol. 189, 114023, 2024.
[64] H. Lund, *Renewable Energy Systems: A Smart Energy Systems Approach to the Choice and Modeling of Fully Decarbonized Societies*, 2024.
[65] K. M. Almatar, "Smart transportation planning and its challenges in the kingdom of Saudi Arabia," *Sustainable Futures*, vol. 8, 100238, 2024.
[66] M. A. A. Shareeda, A. A. Alsadhan, H. H. Qasim, and S. Manickam, "Software defined networking for internet of things: review, techniques, challenges, and future directions," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 1, pp. 638–647, 2024.
[67] M. H. Ali, M. M. Jaber, S. K. Abd, A. Alkhayyat, and M. F. Albaghdadi, "Big data analysis and cloud computing for smart transportation system integration," *Multimedia Tools and Applications*, vol. 84, no. 29, pp. 35073–35090, 2025.
[68] S. K. Jagatheesaperumal, S. E. Bibri, J. Huang, J. Rajapandian, and B. Parthiban, "Artificial intelligence of things for smart cities: advanced solutions for enhancing transportation safety," *Computational Urban Science*, vol. 4, no. 1, 10, 2024.
[69] A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, "A novel ddos mitigation strategy in 5g-based vehicular networks using chebyshev polynomials," *Arabian Journal for Science and Engineering*, vol. 49, no. 9, pp. 11991–12004, 2024.
[70] M. Li, Z. Wan, T. Zou, Z. Shen, M. Li, C. Wang, and X. Xiao, "Artificial intelligence enabled self-powered wireless sensing for smart industry," *Chemical Engineering Journal*, vol. 492, 152417, 2024.
[71] H. Taherdoost, "A systematic review of big data innovations in smart grids," *Results in Engineering*, vol. 22, 102132, 2024.
[72] Y. Hu, Q. Jia, Y. Yao, Y. Lee, M. Lee, C. Wang, X. Zhou, R. Xie, and F. R. Yu, "Industrial internet of things intelligence empowering smart manufacturing: A literature review," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19143–19167, 2024.
[73] F. B. Shaikat, R. Islam, A. T. Happy, and S. A. Faysal, "Optimization of production scheduling in smart manufacturing environments using machine learning algorithms," *Letter High Energy Phys.*, vol. 12, no. 1, pp. 1–15, 2025.
[74] J. Bai, Z. Zeng, K. M. Abualnaja, and N. N. Xiong, "Adcc: An effective adaptive duty cycle control scheme for real time big data in green IoT," *Alexandria Engineering Journal*, vol. 61, no. 8, pp. 5959–5975, 2022.
[75] R. Mohammadi and Z. Shirmohammadi, "Drdc: Deep reinforcement learning based duty cycle for energy harvesting body sensor node," *Energy Reports*, vol. 9, pp. 1707–1719, 2023.
[76] D. Van Leemput, A. Sabovic, K. Hammoud, J. Famaey, S. Pollin, and E. D. Poorter, "Energy harvesting for wireless IoT use cases: A generic feasibility model and tradeoff study," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15025–15043, 2023.
[77] I. Venkatachalam, S. A. John, J. Srinivasan, S. Palaniappan, and S. Somasundaram, "Energy efficient group priority mac protocol using hybrid q-learning honey badger algorithm for IoT networks," *Scientific Reports*, vol. 14, no. 1, 31453, 2024.
[78] X. Li, M. Jiang, C. Lin, R. Chen, M. Weng, and C. Y. Jim, "Integrated bim-IoT platform for carbon emission assessment and tracking in prefabricated building materialization," *Resources, Conservation and Recycling*, vol. 215, 108122, 2025.
[79] M. M. Razip, K. Savita, K. S. Kalid, M. N. Ahmad, M. Zaffar, E. E. A. Rahim, D. Baleanu, and A. Ahmadian, "The development of sustainable iot e-waste management guideline for households," *Chemosphere*, vol. 303, 134767, 2022.
[80] E. Khodayarseresht, A. Shameli-Sendi, Q. Fournier, and M. Dagenais, "Energy and carbon-aware initial vm placement in geographically distributed cloud data centers," *Sustainable Computing: Informatics and Systems*, vol. 39, 100888, 2023.
[81] Z. Jiang, J. Li, Q. Hu, W. Meng, W. Pedrycz, and Z. Su, "Scalable graphaware edge representation learning for wireless IoT intrusion detection," *IEEE Internet of Things Journal*, vol. 11, no. 16, pp. 26955–26969, 2024.
[82] T. Fu, S. Hao, Q. Chen, Z. Yan, H. Liu, and A. Rezaeipanah, "An energyaware secure routing scheme in internet of things networks via two-way trust evaluation," *Pervasive and Mobile Computing*, vol. 105, 101995, 2024.
[83] S. U. Jan, A. Ghani, A. Alzahrani, S. M. Saqlain, K. Yahya, and H. Sajjad, "Bandwidth and power efficient lightweight authentication scheme for healthcare system," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 7, 101601, 2023.

[84] A. Khalique, F. Siddiqui, M. A. Ahad, and I. Hussain, "Lightweight authentication for IoT devices (laid) in sustainable smart cities," *Scientific Reports*, vol. 15, no. 1, 25410, 2025.
[85] M. Kumar, A. Kishor, P. K. Singh, and K. Dubey, "Deadline-aware cost and energy efficient offloading in mobile edge computing," *IEEE Transactions on Sustainable Computing*, vol. 9, no. 5, pp. 778–789, 2024.
[86] W. Qin, H. Chen, L. Wang, Y. Xia, A. Nascita, and A. Pescape, "Mcotm: Mobility-aware computation offloading and task migration for edge computing in industrial IoT," *Future Generation Computer Systems*, vol. 151, pp. 232–241, 2024.
[87] C. Shi, Y. Hu, Y. Zhu, and A. Schmeink, "Security-aware energy efficient design for mobile edge computing network operating with finite blocklength codes," *EURASIP Journal on Wireless Communications and Networking*, no. 1, 67, 2024.
[88] X. Shi and L. Huang, "Energy-saving and security-enhanced task offloading strategies in d2d-integrated MEC networks," *Ad Hoc Networks*, 103890, 2025.
[89] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection," *Internet of Things*, vol. 21, 100670, 2023.
[90] Y. Qi and M. S. Hossain, "Harnessing federated generative learning for green and sustainable internet of things," *Journal of Network and Computer Applications*, vol. 222, 103812, 2024.
[91] R. Liu, M. Xie, A. Liu, and H. Song, "Joint optimization risk factor and energy consumption in iot networks with tinyml-enabled internet of uavs," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 20983–20994, 2024.
[92] T. Pirson and D. Bol, "Assessing the embodied carbon footprint of IoT edge devices with a bottom-up life-cycle approach," *Journal of Cleaner Production*, vol. 322, 128966, 2021.
[93] Z. Chen, Z. Cheng, W. Luo, J. Ao, Y. Liu, K. Sheng, and L. Chen, "Fsmfa: Efficient firmware-secure multi-factor authentication protocol for IoT devices," *Internet of things*, vol. 21, 100685, 2023.
[94] C.-Y. Park, S.-J. Lee, and I.-G. Lee, "Secure and lightweight firmware over-the-air update mechanism for internet of things," *Electronics*, vol. 14, no. 8, 1583, 2025.
[95] A. Dirin, I. Oliver, and T. H. Laine, "A security framework for increasing data and device integrity in internet of things systems," *Sensors*, vol. 23, no. 17, 7532, 2023.
[96] M. Rahaman, P. Pappachan, B. Irawan, V. Arya, and K. T. Chui, "Vulnerabilities, attacks, and security aspects on the internet of things (IoT)," *Internet of Things Security*, pp. 33–59, 2026.
[97] M. A. Alomar, "An iot based smart grid system for advanced cooperative transmission and communication," *Physical Communication*, vol. 58, 102069, 2023.
[98] O. Alnajar and A. Barnawi, "A novel clustered distributed federated learning architecture for tactile internet of things applications in 6g environment," *Computer Modeling in Engineering & Sciences*, vol. 143, no. 3, 3861, 2025.