*future internet*

MDPI

*Review*

# AIoT-Based Security Systems for Smart Homes and Smart Buildings: A Tertiary Study

**Francesco Pilotti [1,*], Aurora Pavone [2], Lia Di Sabatino Farinelli [1], Simone Tinelli [2] and Gaetanino Paolone [2]**

[1] Gruppo SI S.c.a.r.l., 64100 Teramo, Italy; l.disabatino@softwareindustriale.it
[2] B2B S.r.l., 64100 Teramo, Italy; a.pavone@b2binformatica.it (A.P.); s.tinelli@b2binformatica.it (S.T.); g.paolone@b2binformatica.it (G.P.)
* Correspondence: f.pilotti@softwareindustriale.it

**Abstract**

The rapid evolution of Smart Homes and Smart Buildings is driven by the transition from the Internet of Things (IoT) to the Artificial Intelligence of Things (AIoT). Within this scenario, Security Systems are particularly critical and data-intensive systems. Despite extensive research, a high-level synthesis focusing exclusively on the synergy between AIoT and Security Systems in Smart Home and Smart Building application domains is still lacking. To bridge this gap, this paper presents a systematic Tertiary Study (TS) following a well-known research protocol. 13 Secondary Studies (SSs) were synthesized and discussed from an initial pool of 139 publications (years 2024–2025). Findings reveal that monitoring is the most addressed system, followed by security and alarm, while surveillance and access control remain comparatively underexplored. Moreover, results highlight a definitive shift toward Edge and Fog computing to meet latency and privacy requirements, whereas Deep Learning and Ensemble Learning techniques predominate for anomaly detection and predictive maintenance. This study identifies open challenges and future research directions, providing a foundational roadmap for resilient, cognitive-driven security infrastructures in smart environments.

**Keywords:** internet of things; artificial intelligence; artificial internet of things; security systems; smart home; smart building; edge computing; machine learning

## 1. Introduction

In recent years, the evolution of urban and domestic environments toward Smart Building and Smart Home paradigms has triggered a deep structural redefinition, driven by the convergence of pervasive connectivity and advanced cognitive computational models. The transition from the IoT toward the AIoT is transforming homes and buildings from static infrastructures into active, intelligent nodes. Within this ecosystem, Security Systems are particularly critical and data-intensive. From a macroeconomic perspective, the integration of AIoT constitutes a decisive technological acceleration: in a global market projected to reach a value of USD 369.18 billion by 2032 (source: https://www.snsinsider.com/reports/artificial-intelligence-of-things-market-3793 (accessed on 9 March 2026)), and driven by the estimated proliferation of over 32 billion connected devices by the end of the decade, the implementation of Artificial Intelligence (AI) is no longer merely optional. Conversely, the adoption of distributed computing paradigms (such as Edge Computing) has become a strategic necessity to manage massive information flows in real-time, mitigate



Academic Editors: Qiang Duan and Ernesto Iadanza

Received: 16 April 2026
Revised: 27 May 2026
Accepted: 2 June 2026
Published: 5 June 2026

latency, and ensure the stringent privacy standards required by modern physical and logical Security Systems.

Despite an increasing number of primary studies and literature reviews (SSs), a comprehensive, high-level synthesis exclusively dedicated to AIoT-based Security Systems within Smart Building and Smart Home application domains is currently lacking. To bridge this gap, the present TS consolidates the existing secondary literature into a structured mapping of the field, providing an accessible baseline and an orientation framework for the scientific community to navigate technological drivers, architectural trade-offs, and unresolved research challenges. Accordingly, the study offers the following primary contributions:

- a structured state-of-the-art overview of AIoT-based Security Systems in Smart Home/Building application domains, mapping existing studies and identifying core research topics, technological solutions, and recurring themes;
- a critical assessment of predominant technologies, specifically highlighting the adoption degree of Cloud, Edge, and Fog Computing paradigms combined with Machine/Deep Learning to address bottlenecks related to latency, bandwidth, and data security;
- identification of emerging trends and current research gaps, providing strategic and operational guidelines for the scientific community and industrial stakeholders, thereby facilitating technology transfer for the development of next-generation Security Systems.

The TS was conducted by strictly adhering to the guidelines for SSs and TSs proposed by [1], in order to ensure a systematic, transparent, and reproducible process for data extraction, synthesis, and quality assessment.

The remainder of this paper is organized as follows. Section 2 establishes the theoretical background, introducing the Smart Home/Smart Building application domains and elucidating key concepts related to AIoT, computational paradigms (Cloud, Fog, Edge Computing), and their deployment in Security Systems. Section 3 details the research methodology, specifying the Research Questions (RQs), search strings, inclusion/exclusion criteria, and Quality Assessment metrics. Section 4 presents the extracted findings, systematically addressing each formulated RQ. Based on these results, Section 5 discusses open challenges and existing research limitations, while outlining potential future directions. Section 6 analyzes threats to the validity of the study. Finally, Section 7 concludes the paper and suggests directions for future research activities.

The TS provides a rigorous and accessible reference framework, offering a consolidated perspective of the existing secondary literature and supporting the scientific and industrial community as an orientation tool for navigating the complexity of the AIoT landscape.

The remaining Sections of the Paper are shown in Figure 1.

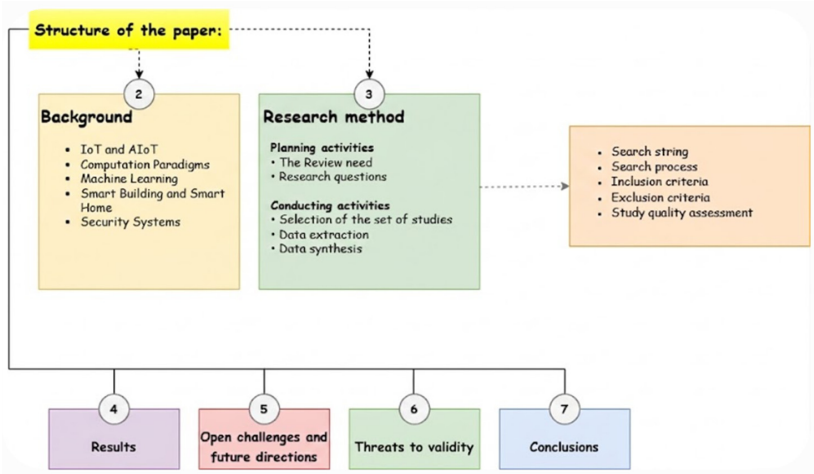


**Figure 1.** Organization of this TS. The numbers refer to the sections.

## 2. Background

### 2.1. IoT and AIoT

IoT refers to an ecosystem of physical objects connected to the Internet and other devices [2]. This ecosystem encompasses sensors, actuators, microcontrollers, communication modules, and Cloud infrastructure. IoT environments generate substantial volumes of heterogeneous data, frequently acquired and transmitted in real time. To extract actionable insights and operational value from such data, intelligent processing workflows enabled by AI are essential. This synergy between IoT and AI is formally defined as AIoT [3]. AIoT imbues interconnected objects with "smart" capabilities—specifically, the computational capacity to comprehend, learn, and act upon data instantaneously [4], typically within the devices themselves or in their immediate proximity (edge computing [5]). This approach reduces the data burden on the cloud, yielding significant advantages in terms of latency, memory optimization, and energy efficiency [5,6].

Consequently, AIoT enables the realization of smart, adaptive, and autonomous ecosystems capable of supporting critical employment in application domains such as Smart Buildings and Smart Homes.

### 2.2. Computation Paradigms

The current IoT landscape is experiencing a computational paradigm shift driven by the proliferation of intelligent devices and the exponential growth of AI-driven services, which have catalyzed the advent of AIoT [7,8]. In this context, although Cloud Computing has traditionally served as the backbone for data processing and storage, its centralized architecture exhibits clear limitations when confronting the massive generation of heterogeneous data at the network edge. Specifically, transmission latency, bandwidth constraints, and privacy concerns are the primary bottlenecks driving the decentralization of computational resources [9].

#### 2.2.1. Cloud Computing

In the AIoT domain, Cloud Computing represents the top tier of the infrastructure, offering centralized computational and storage resources accessible on demand via IP-based connectivity. The Cloud serves as a critical enabler for Big Data management, providing scalability through standardized service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [10]. While it remains unparalleled for long-term storage capacity and the training of complex Machine Learning (ML) models, the cloud-centric model exhibits significant weaknesses in time-sensitive applications. Dependence on Wide Area Networks (WANs) introduces unpredictable latencies and bandwidth bottlenecks, frequently rendering it inadequate for real-time process control [11].

#### 2.2.2. Edge Computing

In response to Cloud limitations, Edge Computing shifts application execution, data processing, and services directly to the logical network periphery, in close proximity to the data source [12]. This paradigm is essential for enabling AIoT, allowing for local processing (e.g., AI model inference) that ensures ultra-low latency responses and substantially reduces the volume of raw data transmitted across the network. Beyond performance benefits, Edge Computing offers advantages in terms of privacy, as sensitive data can be processed locally without leaving the physical perimeter of the device or the local network [9]. However, Edge nodes exhibit significantly more stringent power and computational constraints compared to the virtually unlimited resources of the Cloud [12].

#### 2.2.3. Fog Computing

Fog Computing serves as an intermediate layer between the Edge and the Cloud, extending the latter's functionalities toward the network periphery while maintaining a more distributed structure than centralized data centers. Unlike the Edge, which is often confined to individual devices or local gateways, Fog Computing encompasses a geographically distributed infrastructure of nodes—such as routers, switches, and local servers—that facilitate connectivity, processing, and storage across a broader area [13]. This architecture acts as a bridge, enabling data filtering, aggregation, and analysis before transmission to the Cloud, thereby optimizing network efficiency and supporting scenarios that require mobility and location awareness [14].

### *2.3. Machine Learning*

ML paradigms constitute the frameworks through which data streams are converted into actionable decision assets, enabling the extraction of high-value insights from complex and voluminous datasets [15]. In contemporary software engineering, a structural transition is occurring from rigid deterministic models—often based on static rules—toward systems capable of generalizing behavior from complex, unstructured inputs [15]. This evolution represents the cornerstone of AIoT: massive data collection via the Edge or Cloud remains ineffective without inference engines designed to extract latent patterns and optimize real-time control loops, especially in latency-critical contexts [16]. However, the selection of the optimal paradigm is not arbitrary; it is dictated by a multi-objective optimization involving labeled data availability, the computational resources of the target hardware—where Tree-Based models often outperform Deep Learning (DL) in terms of efficiency—and output reliability requirements [16,17].

#### 2.3.1. Supervised Learnings

Supervised Learning constitutes the predominant approach in current industrial applications, relying on model training using datasets where each input is associated with a known target output (label). This paradigm excels in classification and regression tasks—such as predictive maintenance or optical recognition—where the relationship between variables is inherently complex [18,19]. Despite its high achievable accuracy, Supervised Learning presents a significant operational constraint: its critical dependence on large volumes of high-quality annotated data. The creation of such datasets often requires costly and specialized human intervention, making this approach challenging in environments where underlying phenomena shift rapidly and historical labeled data are scarce [20].

#### 2.3.2. Unsupervised Learning

In contrast to the supervised approaches, Unsupervised Learning operates on unlabeled datasets with the objective of inferring the intrinsic structure or distribution of the data. This paradigm is fundamental in AIoT scenarios where the volume of raw data generated by sensors (at the Fog/Edge layers) is too vast for manual annotation [21]. Clustering and dimensionality reduction techniques enable the identification of anomalies, user segmentation, and data compression while preserving salient features [22]. Although it eliminates the labeling bottleneck, Unsupervised Learning relies on less direct evaluation metrics, and its results are often more challenging to interpret, requiring subsequent expert analysis to transform detected patterns into actionable insights [23].

#### 2.3.3. Deep Learning

DL is defined not merely by network depth but by its underlying architecture, currently dominated by Convolutional Neural Networks (CNNs) and Transformers. Its superiority lies in the ability to learn hierarchical representations directly from raw data, bypassing the rigid manual feature engineering typical of traditional ML [24]. This capability has established it as the de facto standard for processing complex unstructured data, ensuring superior performance in computer vision tasks and long-term time-series forecasting [25]. However, this approach is characterized by high computational intensity: the requirement to train and deploy millions of parameters necessitates dedicated accelerators (GPUs/NPUs), frequently shifting inference toward the Cloud or high-end Edge devices, thus imposing inevitable trade-offs among accuracy, power consumption, and latency [26].

#### 2.3.4. Ensemble Learning

Ensemble Learning is based on the premise that combining multiple weak or diverse models can produce a predictor that is more robust and accurate than any single constituent model. Techniques such as bagging, boosting, and stacking aim to reduce variance (mitigating overfitting) and bias (enhancing learning capacity), respectively, within the overall system [27]. In critical contexts, where decision reliability takes precedence over raw inference speed, Ensemble Learning offers superior stability and enhanced resilience against adversarial attacks and traffic anomalies—common occurrences in distributed environments [28].

#### 2.3.5. Reinforcement Learning

Reinforcement Learning (RL) diverges significantly from other paradigms by focusing on learning an optimal decision policy through direct interaction with a dynamic environment: an agent learns via trial and error, maximizing a cumulative reward function over time. This approach is the cornerstone of autonomous systems and robotics, where the objective extends beyond data classification to active intervention and control [29]. Although powerful, RL is computationally intensive and inherently unstable during the training phase. Furthermore, convergence toward an optimal solution is not guaranteed, requiring high-fidelity simulation environments (e.g., digital twins) prior to real-world deployment to prevent catastrophic physical consequences [30].

### *2.4. Smart Building and Smart Home*

Both scientific literature and the industrial sector exhibit a pronounced semantic ambiguity regarding the nomenclature of "Intelligent Building" and "Smart Building". This conceptual overlap has been deeply rooted in research for more than a decade [31–33] and remains unresolved. In this regard, a recent study by [34] provides a recent confirmation of this semantic instability; their analysis highlights how technological evolution, rather than facilitating terminological convergence, is precipitating a continuous proliferation of new paradigms and nomenclatures that overlap with existing categories. This phenomenon fundamentally obstructs the establishment of a standardized and universally accepted taxonomy.

To delineate these conceptual boundaries and support the selection of the included reviews, we adopt an operational distinction in this paper: an Intelligent Building is conceptualized as a facility equipped with a centralized Building Management System (BMS) that aggregates environmental data to facilitate centrally configured responses and controls, such as Heating, Ventilation, and Air Conditioning (HVAC), lighting, and security (for a comprehensive review of data-driven BMS, see [35]).

Conversely, Smart Buildings leverage adaptive and predictive capabilities: networked devices and algorithms learn from data to anticipate operational states and proactively optimize performance. While [31] initially defined "smartness" through dynamic environmental adaptation, contemporary research significantly expands upon this perspective. According to [36], the focus has shifted toward proactive prediction: buildings now transcend reactive triggers to anticipate occupant needs and operational loads via data-driven models. This trajectory culminates in the autonomous ecosystem described by [37], where AIoT integration redefines the building as an autonomous agent learning from patterns to optimize costs and comfort.

This distinction underscores the transition from reactive direct control toward adaptivity, encompassing both learning and predictive automation.

The evolution toward "smart" environments is enabled by the large-scale integration of IoT and AI. IoT provides continuous telemetry—the automated process of measuring and transmitting data (e.g., temperature, humidity, energy consumption, and device status) from remote sources (such as distributed sensors and actuators) to central, Edge, or Cloud collection systems for monitoring and analysis—alongside the interconnection of sensors and actuators. Complementarily, AI facilitates predictive analytics, automated diagnostics, and autonomous decision-making (see [38] for an in-depth analysis of telemetry and sensor-based data collection in Smart Building monitoring systems).

The Smart Home constitutes the residential application of these principles: an interconnected domestic ecosystem where sensors, actuators, and digital platforms cooperate to optimize comfort, security, and energy efficiency according to user preferences and behavior [39].

In both Smart Building and Smart Home contexts, Security Systems—encompassing alarm, surveillance, monitoring, and access control systems—are transitioning from reactive functions toward intelligent networked components. These entities facilitate anomaly detection, critical scenario prediction, and automated response triggering.

This TS focuses on the deployment of these systems, integrating distributed telemetry and AIoT-based automated decision-making within the Smart Building and Smart Home application domains.

### *2.5. Security Systems: Overview of Relevant Systems in the Domains of Smart Building and Smart Home*

Integrated, cross-disciplinary Security Systems manage physical facilities and occupant safety by aggregating data from networked sources—such as monitoring, surveillance, alarm, and access control systems. These frameworks process telemetry to detect, prevent, and mitigate risk events through coordinated hardware-software synergy.

Within Smart Building and Smart Home domains, these systems function as integrated Cyber-Physical Systems (CPS), where this physical-digital integration ensures built environment safety, resilience, and adaptability. Pivotal to this framework, AIoT integration optimizes critical event responses and aligns system behavior with user requirements.

In this paradigm, security inherently converges with safety and operational resilience: protection objectives cannot be decoupled from the physical integrity and functional continuity of the environment, as traditional security mechanisms become ineffective in the presence of structural failure or power disruption.

This paper adopts the umbrella term "Security Systems" to categorize these frameworks as a cohesive ensemble of devices, algorithms, and protocols dedicated to the active and passive protection of physical facilities and occupants. This nomenclature underscores the inherent interoperability and interconnection among the constituent systems and devices.

The following subsections outline these systems and their deployment within Smart Building and Smart Home application domains.

#### 2.5.1. Security Systems

A security system is an architecture integrating technologies, procedures, and devices to safeguard individuals, assets, and information from physical, logical, or environmental threats [40]. Within Smart Homes, these systems significantly transcend traditional perimeter-focused solutions—formerly restricted to unauthorized access prevention—by offering an expanded range of services [41]. Common functionalities encompass automated gas leak detection coupled with ventilation activation; early-stage fire detection triggering containment and suppression protocols; and occupancy monitoring with real-time mobile alerting [40]. As highlighted by [42], AIoT advancements enable autonomous differentiation between human and non-human activity, augmenting traditional motion detection capabilities.

#### 2.5.2. Alarm Systems

An alarm system is a networked platform that leverages a distributed array of sensors and intelligent devices for real-time security and operational monitoring. Its applications span diverse infrastructures, including industrial complexes [43], vehicles [44], and, with increasing prominence, Smart Building and Smart Home domains [45]. These systems utilize IoT infrastructures comprising Passive InfraRed (PIR) sensors [46], environmental sensors (temperature, humidity, $CO_2$), energy meters, and control devices (HVAC, lighting, automated windows) [45] to provide continuous telemetry on building parameters. Analysis of these data enables anomaly detection relative to predefined thresholds or policies, triggering alarms at critical levels. Such events activate automated notification and response modules for orchestrated local or centralized management.

#### 2.5.3. Surveillance Systems

A surveillance system is an interconnected IoT infrastructure that facilitates continuous monitoring, recording, and analysis to safeguard people, assets, and spaces. These frameworks integrate real-time heterogeneous data streams from visual sensors (IP, thermal, multispectral), acoustic arrays, and environmental transducers (temperature, humidity, gas), supported by mobile remote-management interfaces. This architecture ensures adaptive, scalable, and customizable surveillance [47,48] Surveillance systems in Smart Building and Smart Home are transitioning from passive recording solutions into intelligent platforms featuring distributed analytics and automated event recognition through AIoT and computer vision integration [48–50].

Edge-cloud architectures and cloud services optimize data processing between local devices and remote infrastructures, enhancing responsiveness while minimizing energy consumption and latency [48]. These frameworks facilitate the prompt detection of intrusions, fires, or hazardous conditions through native integration with alarm and access control modules.

BMS interoperability and contextual data management convert surveillance into an adaptive, predictive, and modular component of the connected building ecosystem. Beyond security, these systems bolster environmental management and comfort by integrating with smart infrastructure for intelligent lighting, HVAC, and access control [51]. Furthermore, behavior-based predictive functionalities enhance personalization and operational sustainability [50].

#### 2.5.4. Monitoring Systems

A monitoring system is an integrated framework enabling continuous or periodic data collection, transmission, and analysis to assess stability and detect variations across objects, facilities, processes, or environments. These architectures provide the foundational infrastructure for diverse intelligent and adaptive monitoring contexts. As highlighted by [52], monitoring systems span diverse domains—from industrial predictive maintenance to healthcare, agriculture, and environmental protection. Within Smart Buildings, monitoring parameters such as temperature, humidity, radiation, $CO_2$, and particulate matter enhances comfort, energy efficiency, and occupant health.

In modern monitoring systems, IoT plays a pivotal role, bolstered by Wireless Sensor Networks (WSN) and AI integration [53]. Collectively, these technologies enable real-time monitoring across distributed physical environments. These frameworks comprise three core components: (i) a synergistic array of sensors, actuators, and controllers for the acquisition and management of environmental or process variables [38]; (ii) IoT networks and devices ensuring real-time connectivity and data transmission to facilitate continuous monitoring [38]; and (iii) processing, analysis, and visualization platforms that convert raw telemetry into actionable insights for control and decision support. Collectively, these systems hybridize physical assets (e.g., sensors, HVAC systems, power grids) with digital infrastructures (e.g., BMS, data platforms, algorithms), making buildings more responsive, efficient, and sustainable.

#### 2.5.5. Access Control Systems

Access control systems function as distributed platforms for regulating and monitoring physical and logical access across confined spaces, critical resources, and services [54–56]. These systems facilitate access policy enforcement by verifying identity (who), temporal constraints (when), and specific environmental or operational conditions (contextual parameters) governing resource utilization. Within Smart Building and Smart Home contexts, access control systems orchestrate the interaction among human users, IoT devices (sensors and actuators), and the physical environment (e.g., doors, gates, and rooms). This interplay is facilitated by a middleware communication layer—comprising gateways, controllers, and smart locks—that ensures interoperability and semantic translation across heterogeneous devices and protocols. Simultaneously, this layer addresses the inherent energy, memory, and connectivity constraints of Edge devices [56,57].

## 3. Research Method

In the initial phase of our research, several searches were conducted in Scopus using various query strings, which yielded many outputs.

This iterative process ultimately led to the formulation of the final search string, combining the five systems under consideration—surveillance, security, monitoring, alarm, and access control—with AIoT technologies.

A preliminary analysis of the results obtained from the final search string, conducted on 20 July 2025, revealed a substantial number of retrieved works and showed that the majority were classified as Review articles, indicating a significant presence of SSs. Consequently, the output was refined by applying additional filters related to language and document type, resulting in a consolidated set of 173 records, published between 2017 and 2025.

A further step involved verifying the presence of TSs within the domain of interest. As the search yielded no results, it was determined that, to date, no TSs have been published linking the Security Systems under examination with AIoT technologies. This finding

motivated the decision to undertake this study, drawing on the retrieved SSs, in order to provide a comprehensive overview of the research area in question.

The search was subsequently repeated on 17 January 2026 using the same query string in order to verify whether new publications had emerged. This updated search retrieved 234 documents published between 2017 and 2026, representing an increase of 61 additional papers compared with the search conducted on 20 July 2025. These results therefore indicate a substantial growth in the literature over the considered period and once again confirmed the absence of TSs.

The process of identifying and selecting the studies is outlined in Section 3.2. The analysis is based on the last search, which subsumes the first and defines the initial pool of studies from which the subsequent filtering and selection criteria were applied.

A clearer explanation of the search steps with the associated number of papers retrieved and the filtering process applied is provided in Table 1 below.

**Table 1.** Preliminary overview of search steps and filtering process.

| Step | Description | Publication Years | No. of Documents |
|---|---|---|---|
| first raw results | 20 July 2025 preliminary Scopus search | 2017–2025 | 173 |
| second raw results | 17 January 2026 final Scopus search (includes the papers of the previous steps) | 2017–2026 | 234 |
| temporal refinement | temporal restriction of the 234 papers to the 2024–2025 timeframe | 2024–2025 | 139 |

As recommended by [1], this study is structured in accordance with the protocol and methodology of a Systematic Literature Review (SLR) and is therefore organized into three main phases, as detailed in the following sections:

- review planning: includes the identification of the review need, the definition of the research questions, and the elaboration of the review protocol;
- review conduction: includes the selection of SSs, the quality assessment, the data extraction and data synthesis;
- review reporting: includes the specification of the dissemination mechanisms, the formatting and the evaluation of the report.

### *3.1. Planning Activities*

#### 3.1.1. The Review Need

The present research is grounded in the need expressed by B2B S.r.l.—an Italian company operating in the Information and Communication Technology (ICT) sector—to conduct a structured survey on the Security Systems domain. This initiative was undertaken within the framework of a research and development project focused on IoT and AI—particularly ML—and their integration (AIoT).

In this context, the project initially concentrated on the analysis and critical investigation of selected use cases—such as automatic doors, elevators and lifting systems, among other comparable automated building subsystems—and subsequently expanded toward additional application areas considered of strategic interest, given that the integration of IoT and AI constitutes a significant driver of enhancement and innovation.

Security Systems—encompassing alarm, surveillance, monitoring, and access control systems—can substantially benefit from AIoT-based solutions across multiple dimensions, especially in the Smart Home and Smart Building application domains. These benefits include, for instance, the enhancement of safety and advanced control capabilities, the optimization of energy efficiency, the implementation of predictive maintenance strategies

for building installations and infrastructures, and the improvement of user experience, as well as other performance and service-oriented advancements.

#### 3.1.2. Research Questions

The objective of the present SLR is to address the overarching research need outlined in the previous section. This general objective is further articulated through the following RQs:

(RQ1) What is the map of published SSs concerning AIoT-based Security Systems within the Smart Home and Smart Building application domains?
(RQ2) What are the main topics addressed regarding AIoT-based Security Systems within the Smart Home and Smart Building application domains?
(RQ3) What are the key ML algorithms, methods, and techniques predominantly employed in the implementation of AIoT-based Security Systems within the Smart Home and Smart Building application domains, and what are the reasons for their adoption?
(RQ4) Which computing paradigms, among Edge, Fog and Cloud, are currently the most widely employed solutions for data processing in AIoT-based Security Systems within the Smart Home and Smart Building application domains, and what are the reasons for their adoption?

The RQs are designed to follow a structured progression that moves from landscape mapping to technical interpretation. RQ1 establishes the empirical perimeter of the review, defining the volume, distribution, and typology of SSs in the domain. RQ2 deepens this mapping by extracting and systematizing the core thematic directions that characterize AIoT-based Security Systems within Smart Home and Smart Building contexts.

On this basis, RQ3 and RQ4 introduce an analytical shift from what is studied to how it is technically realized. By examining the predominant ML approaches and the computing paradigms underpinning data processing architectures, these questions provide insight into the technological foundations and design rationales shaping current solutions.

This progression strengthens the analytical depth of the review by enabling a transition from a descriptive cartography of the literature to a more technical understanding of the field's developmental trajectory.

The examination of these specific aspects constitutes the ultimate objective of the present TS. All of the RQs listed above reflect specific research needs identified during the review's planning phase. The final formulation of these questions was established through a collaborative, consensus-driven process among the participating researchers.

### *3.2. Conducting Activities*

The review protocol adopted in this TS was based on a structured search conducted within the Scopus database. Figure 2 summarizes the study selection process, organized into five successive phases. Initially, the Scopus database was queried using the search string described in Section Search String, yielding a total of 234 documents. Considering these findings, and the broad heterogeneity of the identified contributions, it was deemed appropriate to restrict the subsequent steps to the 2024–2025 timeframe, adopting an iterative and incremental approach. The analysis began with the most recent studies (published in 2025, totaling 102 works) and then proceeded to the 2024 contributions (37 studies), resulting in a subset of 139 papers taken into consideration. This approach ensured systematic coverage of the selected time interval, aligning with the objective of focusing on the most relevant and up-to-date developments in the state of the art. The distribution of the retrieved papers is detailed in Section Search Process.

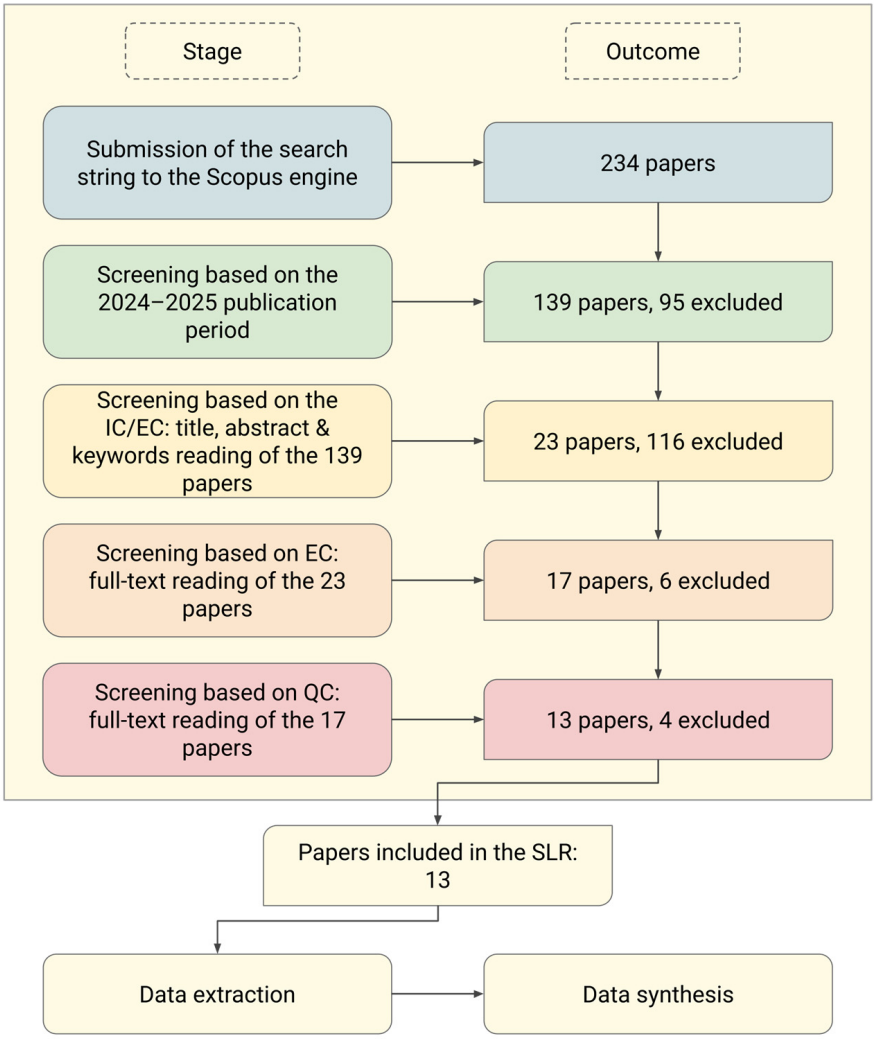


**Figure 2.** The implemented protocol. The study selection process spans from initial Scopus retrieval through successive screening steps and protocol-defined criteria, leading to a progressive reduction of the study pool. Data extraction and synthesis phases support the structured consolidation and mapping of the selected literature.

Subsequently, the retrieved documents were screened by applying the established inclusion and exclusion criteria (Sections Inclusion Criteria (IC) and Exclusion Criteria (EC)) through a review of their title, abstract and keywords, leading to an initial subset of 23 studies. These were then subjected to a full-text assessment, resulting in 17 potentially eligible studies. The final quality assessment phase (Section Study Quality Assessment) enabled the selection of 13 studies to be included in the present TS.

The dynamic that led to the final selection of these 13 studies is grounded in three core methodological decisions. First, while the initial retrieval was intentionally broad to prevent the loss of relevant cross-disciplinary contributions, it was a precise intention to restrict the analytical scope strictly to the intersection of Security Systems, AIoT, and Smart Buildings. Second, the temporal restriction to the 2024–2025 timeframe was inherently imposed by the rapid technological evolution of AIoT; this choice allowed the study to focus exclusively on the immediate state-of-the-art and emerging commercial solutions, deliberately bypassing earlier, less mature stages of research. Finally, the punctual and rigorous implementation of this selection protocol structurally ensures the validity and reliability of the evidence extracted for the targeted domain. The activities carried out during the review conduction phase are detailed below.

3.2.1. Selection of the Set of Studies (Querying Scopus DB)

Search String

The core search string used to identify relevant studies before the application of database-specific filters, was defined as follows:

("surveillance system*" OR "security system*" OR "monitoring system*" OR "alarm system*" OR "Access Control System*") AND
(IoT OR "Internet of things") AND
(AI OR "Artificial Intelligence" OR ML OR "Machine Learning" OR Learning)

In defining the search string, the keywords "smart home" and "smart building" were deliberately excluded from the search string to avoid an excessively restrictive filtering effect. Although these terms are frequently used within the IoT and AI/ML contexts, their inclusion could have inadvertently omitted relevant contributions that do not explicitly adopt such terminology.

The focus of this study is to analyze the current state of the art and applications of AIoT within the domain of the five systems of interest. The inclusion of overly specific terms might have led to the exclusion of relevant contributions—such as studies on structural security or advanced building monitoring—which fully fall within the scope of these five systems, despite not being explicitly categorized under the Smart Home or Smart Building application domains.

Search Process

The research was conducted as a manual search of Scopus articles that mention the keywords from the search string in the title, abstract, or author keywords. The initial search formutation was then refined by applying a language filter ("English") and additional filters to restrict the retrieval to the following document types: articles and reviews. The complete syntax of the Scopus search string is reported below:

TITLE-ABS-KEY (("surveillance system*" OR "security system*" OR "monitoring system*" OR "alarm system*" OR "Access Control System*") AND
(IoT OR "Internet of things") AND
(AI OR "Artificial Intelligence" OR ML OR "Machine Learning" OR learning) AND
(review OR "Mapping study")) AND
(LIMIT-TO (LANGUAGE, "English")) AND
(LIMIT-TO (DOCTYPE, "re") OR
LIMIT-TO (DOCTYPE, "ar"))

The search was conducted on 17 January 2026 and yielded 139 records after applying the publication time-frame filter.

Table 2 shows the temporal distribution of the retrieved articles, while Table 3 reports the number of publications aggregated by document type. For each retrieved study, Scopus was queried to provide the following metadata: author names, title, abstract, author keywords, publication venue, DOI, and number of citations.

**Table 2.** Distribution of papers over the years.

| Year | Documents |
|---|---|
| 2025 | 102 |
| 2024 | 37 |

**Table 3.** Aggregation of papers by types.

| Document Type | Documents |
|---|---|
| Article | 47 (33.8%) |
| Review | 92 (66.2%) |

Inclusion Criteria (IC)

The selection of the initial set of studies was guided by the following inclusion criteria:

- all documents contain one or more keywords from the search string in the title and/or abstract and/or among the author-provided keywords;
- all documents were exclusively retrieved from the Scopus database, limiting the search to SSs (in English) classified as "Review" or "Article" and containing the terms "review" or "Mapping study". This approach ensures the inclusion of publications from peer-reviewed scientific journals, thereby maintaining the methodological rigor and scholarly reliability of the selected works;
- all documents are unique, as Scopus guarantees that no work is represented more than once in the search results.

Exclusion Criteria (EC)

Articles retrieved from Scopus, restricted to the defined time interval, were further refined by excluding any document classified under one of the five categories listed in Table 4.

**Table 4.** Reasons for exclusion of a study retrieved by the Scopus engine.

| Exclusion Criterion | Reason for Exclusion |
|---|---|
| EC1. In the retrieved paper, the sub-strings "Artificial Intelligence" (or "AI") and/or "Machine Learning" (or "ML") and/or "Internet of Things" (or "IoT") are mentioned in the title, author's keywords, or abstract, but the manuscript does not describe the AI/ML/IoT themes theoretically, nor does it elaborate on the integration of AI/ML/IoT in relation to the systems under investigation. | False positive |
| EC2. In the analyzed contribution, the themes of AI and/or ML and IoT are presented in theoretical or introductory terms, with a descriptive and general treatment, or are mentioned exclusively as potential future developments or research recommendations; however, the study does not operationally delve into or deepen the concrete integration of these technologies into the types of systems under investigation. | Not Relevant |
| EC3. The analyzed study addresses the themes of AI and/or ML and IoT in relation to the types of systems under investigation, but not in reference to the specific domain of interest of this review. | Out of scope |
| EC4. The identified contribution is classified as a primary study, as it presents original data or unpublished contributions. This review, being a tertiary literature review, focuses exclusively on SSs and secondary-level reviews that synthesize existing scientific literature. Therefore, the paper is excluded as it does not fall within the methodological and analytical scope defined for this study. | Out of scope |
| EC5 The analyzed contribution explores the application of AI for the types of systems under investigation, but it does not contemplate ML methodologies, limiting itself to alternative or generic approaches. | Out of scope |

Study selection for the present review was carried out through an iterative process in accordance with established guidelines for systematic literature reviews, ensuring both rigor and reliability.

Initially, titles, abstracts and keywords of the 139 retrieved papers were independently evaluated by five reviewers against the above exclusion criteria. Involving multiple reviewers is a recommended practice to minimize bias in activities requiring subjective judgment [58].

At the end of this stage, 116 articles were excluded. A total of 23 publications subsequently proceeded to the full-text screening phase (Figure 2). The list of the 116 articles excluded after title, abstract and keywords review, along with the primary reason for their exclusion, is provided in Table 5.

**Table 5.** Excluded papers after reading title, abstract and keywords.

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [59] | Worker behavior tracking and human resource management and financial services. | EC3 |
| [60] | IoT-enabled biosensors for real-time monitoring and early detection of chronic diseases. | EC3 |
| [61] | Structural health monitoring of bridges (specifically, timber bridges). | EC3 |
| [62] | Bibliometric analysis of Machine Learning and IoT adoption for innovation management in healthcare institutions. | EC3 |
| [63] | Analysis of Industry 4.0 technologies (IoT, AI, computer vision) for automation and monitoring of industrial fish-cutting processes. | EC3 |
| [64] | Monitoring and optimization of power generation (solar, wind, hydroelectric). | EC3 |
| [65] | Analysis of real-time tool condition monitoring systems for computer numerical control machines through IIoT and Machine Learning integration. | EC3 |
| [66] | Analysis of Generative AI and Internet of Robotic Things (IoRT) in developing the industrial metaverse and digital twins for smart logistics and production. | EC2 |
| [67] | Bibliometric and scientometric analysis of global research trends in crack monitoring for concrete structures. | EC2 |
| [68] | State-of-the-art review of IoT and AI systems for soil hydrological monitoring and slope movement detection (landslides) using on-site sensors and remote sensing techniques. | EC3 |
| [69] | Literature review on integrating AI, Computer Vision, and IoT for predictive maintenance and fault detection in conveyor belt systems. | EC3 |
| [70] | Analysis of analytical methods for nanowaste detection in the food industry and evaluation of technologies (IoT, blockchain, ML) for their tracking. | EC3 |
| [71] | Development of a multi-scale IoT occupancy sensing system for occupancy state classification. | EC4 |
| [72] | Scoping review and case studies on the adoption of ICT tools (EHR, telemedicine, remote monitoring) for nursing management and patient healthcare. | EC3 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [73] | Systematic survey of AI/ML/DL/RL-enabled solutions for authentication, data privacy, and layered threat mitigation (TCP/IP stack) in UAV-assisted IoT ecosystems. | EC3 |
| [74] | Review of IoT security threats (malware, MITM) and proposal of countermeasures based on artificial immune systems, differential privacy, and federated learning for the Energy and Medical IoT sectors. | EC3 |
| [75] | Analysis of smart contract vulnerabilities and proposal of a few-shot learning-based detection method for unknown threats. | EC3 |
| [76] | Analysis of reconfigurable intelligent surfaces for physical layer security in 6G-IoT networks, focusing on beamforming and mitigation of eavesdropping and jamming attacks. | EC3 |
| [77] | Development of IoT/Edge system for leaf disease instance segmentation in precision agriculture. | EC4 |
| [78] | Systematic analysis of technological gaps in risk management for earthmoving equipment based on Rasmussen's framework. | EC3 |
| [79] | Review of diabetes monitoring architectures: biofluidic sensors, BLE/NB-IoT standards, and Cloud/Edge AI integration. | EC3 |
| [80] | Overview of the state-of-the-art in wearable devices and their clinical/sports applications. | EC3 |
| [81] | Literature review on merging Federated Learning and Explainable AI for security and transparency in Internet of Medical Things and data security | EC3 |
| [82] | Framework for predictive chronic disease monitoring using DL and Ambient Assisted Living. | EC4 |
| [83] | Proposal of a theoretical framework for Federated Learning based on bibliometric analysis and systems theory. | EC3 |
| [84] | Systematic review of adversarial attacks and defense mechanisms for IoT security systems. | EC3 |
| [85] | Review on IoT, AI, and ML applications for monitoring and automating wastewater treatment and hydroponics. | EC3 |
| [86] | Analysis of ML algorithms for security and energy efficiency in WSN. | EC3 |
| [87] | Review on multifault diagnosis and monitoring systems for rotating bearings using IoT, Cloud, and AI. | EC3 |
| [88] | Analysis of Distributed Denial of Service (DDoS) threats in IoT and evaluation of DL and Explainable AI for defense. | EC3 |
| [89] | Review on postharvest cold storage technologies: focus on energy efficiency, IoT, and digital twins for sustainability. | EC3 |
| [90] | Review of commercial tool condition monitoring systems. | EC3 |
| [91] | Systematic analysis of DL applications in animal farming to identify advancements, gaps, and solutions. | EC3 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [92] | Examination of air monitoring systems integration with hybrid vehicles for emission control. | EC3 |
| [93] | Examination of organic fertilizer production from domestic food waste. | EC1 |
| [94] | Analysis of Industry 4.0 technologies for food quality and safety. | EC3 |
| [95] | Proposal of a multi-layered security architecture for Internet of Everything integrating Blockchain, Edge Computing, and post-quantum cryptography. | EC3 |
| [96] | Exploration of computer vision and IoT integration for automated agricultural pest management systems | EC3 |
| [97] | Review of advanced fire sensors. | EC2 |
| [98] | Analysis of the development, efficiency, and environmental impact of ULT freezers, focusing on refrigerants, biomedical and food applications. | EC3 |
| [99] | Examining advanced monitoring technologies for photobioreactors, including multi-sensor systems and AI integration, to optimize microalgae cultivation and the synthesis of biofuels and high-value bioproducts | EC3 |
| [100] | Systematic review on DL defenses for Denial of Service (DoS) attacks in IoT/WoT. | EC3 |
| [101] | Analysis of the effectiveness of DL and Big Data Analytics approaches in IoT threat detection and identification of application limitations. | EC3 |
| [102] | Implementation of advanced air quality monitoring systems in metropolitan cities in Indonesia. | EC3 |
| [103] | Classification of electronic devices with AI on edge devices. | EC4 |
| [104] | Analysis and comparison of traditional and emerging methods for slope stability monitoring in open-pit mines. | EC3 |
| [105] | Optimization of piezoelectric nanogenerators (PENG) using artificial intelligence for energy harvesting. | EC3 |
| [106] | Scientific mapping of smart technologies for sustainable organic waste management. | EC1 |
| [107] | Evaluation of natural water quality monitoring systems for achieving Sustainable Development Goals (SDGs). | EC3 |
| [108] | Mapping research trends and promoting advanced technologies for steel corrosion detection. | EC2 |
| [109] | Improvement of research methodologies on the impacts of land use on water quality. | EC3 |
| [110] | Analysis of the transformative impact of emerging technologies (AI, IoT, Virtual Reality (VR)/Augmented Reality (AR)) in multidisciplinary sectors. | EC3 |
| [111] | Development of advanced and interdisciplinary diagnostic technologies for early plant virus detection. | EC3 |
| [112] | Analysis and optimization of monitoring systems for electric vehicle batteries through advanced modeling and integrated technologies. | EC3 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [113] | Design of a multi-level blockchain framework for transparency and automation of land management. | EC3 |
| [114] | Development of integrated monitoring and early warning systems for hydrogeological risk reduction. | EC3 |
| [115] | Innovation in food freshness assessment systems through imaging techniques and DL. | EC3 |
| [116] | Development of intelligent environmental monitoring systems through synergistic integration of artificial intelligence and IoT. | EC3 |
| [117] | Implementation of a Generative Artificial Intelligence-based assistance service for simplified configuration of IoT platforms. | EC4 |
| [118] | Systematic analysis of ML methodologies for estimating the state of health of lithium batteries in sustainable reuse. | EC3 |
| [119] | Evaluation of the effectiveness of wearable devices for continuous postoperative monitoring in surgical wards. | EC3 |
| [120] | Implementation of integrated IoT and artificial intelligence systems for personalized chronic disease management. | EC3 |
| [121] | Review of predictive systems for peatland fires through integration of IoT and weather indices. | EC3 |
| [122] | Implementation of intelligent integrated monitoring systems for road safety in the Internet of Vehicles. | EC3 |
| [123] | Integration of IoT and artificial intelligence for smart weather monitoring. | EC3 |
| [124] | Systematic analysis of physical security in wireless networks through reconfigurable intelligent surfaces (RIS) for radio frequency and optical communications. | EC3 |
| [125] | Systematic evaluation and qualitative framework for pedestrian monitoring in complex urban environments. | EC3 |
| [126] | Review of blockchain and artificial intelligence integration for sustainable water resource management. | EC3 |
| [127] | Systematic analysis of IoT architectures and intelligent algorithms for livestock health monitoring. | EC3 |
| [128] | Review of the integration of advanced technologies (AI, big data, IoT, Geographic Information System (GIS)) for enhancing epidemic intelligence systems. | EC3 |
| [129] | Development of remote patient monitoring frameworks using Internet of Medical Things (IoMT) for neurodegenerative disease care | EC3 |
| [130] | Systematic analysis of IoT technologies for waste management optimization in smart cities. | EC3 |
| [131] | Propose a diet and nutrition monitoring system combining DL and IoT for food portion estimation. | EC4 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [132] | Systematic review of vibration sensors and their application in industrial equipment-monitoring systems. | EC3 |
| [133] | Thematic review of Federated Learning challenges and approaches for data privacy in smart city environments | EC3 |
| [134] | Potential of 5G and IoT for sustainable urban resource management and security. | EC3 |
| [135] | Sensor technologies for ammonia monitoring in industrial and environmental contexts. | EC3 |
| [136] | Security and privacy frameworks for ubiquitous computing services in smart educational settings. | EC3 |
| [137] | Multimodal AI systems for poultry welfare assessment and livestock productivity optimization. | EC3 |
| [138] | Multimedia data transmission strategies and challenges over low-power LoRa networks. | EC3 |
| [139] | Intelligent and distributed security frameworks for the evolution of the healthcare sector. | EC3 |
| [140] | Non-invasive sensor techniques for food quality monitoring in the edible oil industry. | EC3 |
| [141] | AI-powered non-invasive testing methods for improving food quality and safety control | EC3 |
| [142] | Emerging technologies for detecting and controlling chemical and biological food contaminants | EC3 |
| [143] | Systematic review of AI, IoT, and Digital Twins integration for human–robot collaboration in smart construction sites. | EC3 |
| [144] | Proposed an IoT-based authorization and monitoring solution for wood transport and forest resource protection. | EC4 |
| [145] | Review of AI trends and challenges in the assessment and prediction of bathing water quality. | EC3 |
| [146] | Digital twin and IoT potential for human movement monitoring in healthcare prehabilitation | EC3 |
| [147] | AI and IoT integration for cholesterol monitoring and coronary artery disease management | EC3 |
| [148] | Review and evaluation of existing approaches for detecting and mitigating reactive jamming attacks in IoT networks. | EC3 |
| [149] | Advances in AI application for improving efficiency, sustainability, and resource optimization across modern agricultural systems. | EC3 |
| [150] | Overview of electrochemical and optical nanosensor technologies for heavy metal detection in agricultural soils. | EC3 |
| [151] | A review of advanced sensing, AI, and edge computing technologies for early detection and prediction of crop diseases in precision agriculture. | EC3 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [152] | A systematic review of IoT security architectures, threats, and defense mechanisms across application domains. | EC3 |
| [153] | A comprehensive analysis of Cyber Threat Intelligence and ML approaches for detecting and mitigating security threats in IoT environments. | EC3 |
| [154] | Review of artificial intelligence applications in cardiopulmonary resuscitation to improve prediction, intervention, and post-arrest outcomes. | EC3 |
| [155] | Overview of traditional and advanced methods for water quality monitoring and assessment. | EC2 |
| [156] | Overview of unmanned and intelligent technologies for monitoring and managing deep-sea aquaculture within IoT-based precision aquaculture systems. | EC3 |
| [157] | AIoT technologies and edge-based systems for comprehensive crop health monitoring and smart farming applications. | EC3 |
| [158] | A review of shrimp aquaculture insurance models, risk management strategies, and digital technologies for sustainable and resilient farming. | EC3 |
| [159] | Analysis of material-based advances in wearable, non-invasive respiratory monitoring sensors and their physiological relevance. | EC3 |
| [160] | Evaluation of IoT-enabled healthcare monitoring systems, focusing on architectures, technologies, applications, and challenges for real-time, intelligent patient management. | EC3 |
| [161] | Synthesis of mechanisms, risk factors, and multidisciplinary prevention strategies for orotracheal intubation–related oral mucosal pressure injuries in ICU patients. | EC3 |
| [162] | Systematic assessment of non-invasive sensing technologies, computational methods, and applications for intelligent crop disease monitoring, prediction, and early warning in agriculture. | EC3 |
| [163] | Systematic analysis of digital interventions for enhancing diagnostic accuracy and patient adherence in clinical psoriasis care. | EC3 |
| [164] | Assessment of acoustic sensor architectures for non-invasive health monitoring. | EC3 |
| [165] | Overview of free space optics implementation utilizing diffractive optical elements and AI-based optimization for beam steering, adaptive optics, and predictive maintenance in wireless communication. | EC3 |
| [166] | Evaluation of IoT-enabled healthcare monitoring systems, focusing on architectures, ML/DL methods, and challenges regarding data security, scalability, and interoperability for remote patient management. | EC3 |
| [167] | Comprehensive review of Intelligent transportation systems leveraging ML, IoT, and edge computing for demand prediction, real-time vehicle monitoring, and route optimization in public transit planning. | EC3 |

**Table 5.** *Cont.*

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [168] | Overview of implementation and advancements in wireless data transmission utilizing diffractive optics and AI for adaptive beam steering and fault detection. | EC3 |
| [169] | SLR of IoT, blockchain, and ML integration for enhanced product traceability and patient safety, addressing challenges in data standardization, compliance, and real-time alert systems. | EC3 |
| [170] | Methodological review of continuous monitoring for anaerobic digestion, with focus on the integration of soft sensors and computer vision for enhanced process control and predictive maintenance. | EC3 |
| [171] | Analysis of AI-driven strategies and smart sensor networks for automated pest identification, real-time crop health monitoring, and precision resource management in sustainable agriculture. | EC3 |
| [172] | Systematic survey of Deep Learning-based Autonomous Anomaly Detection for SDN-IoT networks, with focus on CNN/Recurrent Neural Network (RNN)/Long Short-Term Memory (LSTM) architectures for the mitigation of DDoS attacks and real-time traffic breaches. | EC3 |
| [173] | Analysis of proactive defense strategies in IIoT through a 3-D methodological framework based on game theory models for the mitigation of APT and DDoS threats. | EC3 |
| [174] | Development and validation of a Digital Twin-based Site Resource Monitoring system through the integration of 4D BIM, IoT networks, and ML algorithms for real-time productivity prediction and inventory tracking. | EC4 |

It should be emphasized that the screening outcomes presented in Tables 5 and 6 do not constitute a critique of the scientific merit or inherent quality of the excluded papers; rather, they signify a strict lack of adherence to the narrow methodological scope and specific eligibility criteria defined for this tertiary study.

**Table 6.** Excluded papers after full-text reading.

| References | Aim | Motivation for Exclusion |
| --- | --- | --- |
| [175] | Review of recent advances in fingerprint liveness detection for strengthening biometric security systems. | EC3 |
| [176] | Assessment of adversarial machine learning vulnerabilities in IoT-based security systems. | EC3 |
| [177] | Review of AI-driven monitoring, control, and predictive maintenance approaches for hydrogen fuel cell systems. | EC3 |
| [178] | Review of blockchain applications for construction safety. | EC2 |
| [179] | Mapping the development of Ambient Intelligence. | EC3 |
| [180] | Evaluation of renewable microgrid controls. | EC2 |

The full texts of the 23 selected contributions underwent independent evaluation by five reviewers. Decisions regarding study inclusion and exclusion were made in accordance with predefined criteria; individual assessments were discussed collectively and resolved by majority consensus.

Following this comprehensive assessment phase, 6 papers were excluded. Consequently, the set of studies advancing to the next evaluation stage comprised 17 publications (Figure 2). The references for the 6 papers excluded after full-text assessment, along with the corresponding reasons for their exclusion, are provided in Table 6.

### Study Quality Assessment

To ensure the highest standard of evidence synthesis, a set of quality criteria (QCs) was applied to verify the alignment of the selected papers with the methodological requirements of this review. In strict accordance with the formal established by Kitchenham and Charters [1], this assessment was conducted to enhance the robustness of the synthesized findings and ensure the overall reliability of the final conclusions.

In this study, quality assessment was conducted on the selected SSs based on the QCs listed below:

QC1. Are the RQs explicit?
QC2. Is the review protocol well-defined?
QC3. Is the search string reported?
QC4. Are the inclusion criteria described and related to the study goals?
QC5. Are the exclusion criteria described and related to the study goals?
QC6. Are the years covered in the review declared?
QC7. Do the queried scientific databases ensure that the result of the search can cover all the significant published studies?
QC8. Is the quality of the included studies assessed?
QC9. Is the data-extraction activity adequate to the purpose of the study?
QC10. Is the data-synthesis method described?
QC11. Are the selected studies adequately illustrated?
QC12. Does the study adequately answer the RQs?
QC13. Are the open issues adequately discussed?
QC14. Is there an analysis of the threats to validity?
QC15. Is the publication venue a journal, a conference, or a book chapter?

The QC score of each study was calculated using the following schema: N(o) = 0, Y(es) = 1, P(artial) = 0.5. In detail, the QCs were scored as follows:

QC1. The RQs are implicit: N; the RQs are explicit: Y; the RQs can be inferred: P.
QC2. The review protocol is missing: N; the review protocol is well-defined: Y; the review protocol is not fully defined: P.
QC3. The search string is not reported: N; the search string is reported: Y; the search string can be inferred: P.
QC4. The inclusion criteria are not mentioned: N; the inclusion criteria are described and they relate to the study goals: Y; the inclusion criteria are not explicitly described: P.
QC5. The exclusion criteria are not mentioned: N; the exclusion criteria are described and they relate to the study goals: Y; the exclusion criteria are not explicitly described: P.
QC6. The years covered in the review are not declared: N; the years covered in the review are declared: Y; the years covered in the review can be inferred: P.
QC7. The searched databases are not mentioned: N; the searched databases are scientifically relevant and ensure a wide coverage of published articles: Y; the authors have searched only a small set of scientific sources (either journals or proceedings). So, not all the relevant published articles are investigated: P.

QC8. The quality-assessment stage of the selected studies is omitted: N; quality criteria are defined and applied to each primary study: Y; the quality-assessment strategy can be inferred: P.
QC9. The data-extraction activity is not described: N; the data-extraction activity is adequate to the purpose of the study: Y; the data-extraction activity does not provide sufficient details on all the aspects that are part of such a stage (e.g., the output of the exclusion criteria, the procedure to remove duplicate publications, the type of paper (e.g., article, book chapter, or conference paper), etc.): P.
QC10. The data-synthesis method is not described: N; it is described: Y; it could be derived: P.
QC11. The findings of each study are not specified: N; the information is carefully summarized for each study: Y; only a recapped description is given for each individual paper: P.
QC12. The study does not answer the RQs: N; the study adequately answers the RQs: Y; the answer to the RQs is not fully satisfactory: P.
QC13. Open issues are not discussed: N; open issues are listed and adequately discussed in the study: Y; open issues are listed, but emerging lines of research potentially suitable for solving them are just touched: P.
QC14. Threats to validity analysis are omitted: N; there is an analysis of the threats to validity and countermeasures are taken to limit potential threats: Y; the analysis of the threats to validity is superficial: P.
QC15. The publication venue is either a conference or a book chapter: N; the publication venue is a top-class journal (i.e., an ACM, IEEE, Elsevier, Springer, Wiley publication): Y; the publication venue is not a top-class journal; however, it is indexed by Scopus: P.

To minimize potential errors, the scores assigned to each QC were finalized through collective verification and discussion following independent assessments by each author. The evaluation scores for the 17 analyzed papers are reported in Table 7. 4 articles were excluded due to low scores; these studies are listed in Table 8.

**Table 7.** Quality-assessment results for 17 studies.

| References | QC1 | QC2 | QC3 | QC4 | QC5 | QC6 | QC7 | QC8 | QC9 | QC10 | QC11 | QC12 | QC13 | QC14 | QC15 | Score |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [181] | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 1 | 1 | 0 | 1 | 12.5 |
| [182] | 1 | 1 | 0.5 | 1 | 1 | 1 | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 1 | 1 | 0.5 | 1 | 12 |
| [183] | 0.5 | 1 | 0.5 | 1 | 1 | 1 | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 1 | 1 | 0 | 1 | 11 |
| [184] | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 1 | 0 | 0 | 0.5 | 11 |
| [185] | 1 | 1 | 0.5 | 0.5 | 0.5 | 1 | 1 | 0 | 0.5 | 0.5 | 1 | 1 | 1 | 0 | 1 | 10.5 |
| [186] | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0.5 | 0.5 | 0.5 | 0.5 | 1 | 0 | 0.5 | 10 |
| [187] | 1 | 1 | 0.5 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0.5 | 1 | 0.5 | 0 | 0.5 | 9 |
| [188] | 0.5 | 1 | 0.5 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0.5 | 0.5 | 1 | 0 | 0.5 | 8.5 |
| [189] | 0 | 1 | 1 | 0.5 | 1 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0 | 1 | 0 | 1 | 8.5 |
| [190] | 0.5 | 1 | 0.5 | 1 | 0 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0.5 | 1 | 0 | 1 | 8.5 |
| [191] | 0.5 | 0.5 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0.5 | 0 | 0.5 | 1 | 0 | 0.5 | 6.5 |
| [192] | 0.5 | 0 | 0 | 0.5 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 6 |
| [193] | 0.5 | 0 | 0 | 0 | 0 | 0.5 | 0 | 0 | 0 | 0.5 | 1 | 1 | 1 | 0 | 1 | 5.5 |
| [194] | 0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.5 | 1 | 1 | 0 | 1 | 4 |
| [195] | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.5 | 1 | 0 | 1 | 3.5 |
| [196] | 0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.5 | 1 | 0 | 1 | 0 | 0.5 | 3.5 |
| [38] | 0 | 0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 2.5 |

#### 3.2.2. Data Extraction

Aligned with methodological guidance proposed by [1], the data extraction phase was conducted through a systematic and protocol-based approach.

The metadata defining the information to be extracted from the selected studies, as reported in Table 9, were established prior to the analysis to mitigate subjective bias and ensure consistency across all included studies. The table specifies the set of metadata to be collected—such as research questions, methodological approaches, ML techniques, and

types of contribution—and establishes a clear correspondence between each metadata item and the related research question addressed in this tertiary review.

**Table 8.** Reference to the four studies excluded at the quality-assessment stage.

| References |
|---|
| [194] |
| [195] |
| [196] |
| [38] |

**Table 9.** Data items to be extracted from the selected studies.

| Metadata | Explanation | RQs |
|---|---|---|
| Source | Article, conference paper, review, book chapter | RQ1 |
| Year | Year of publication | RQ1 |
| Length | Number of pages of the paper | RQ1 |
| Scientific DB(s) | Scientific databases queried by authors | RQ1 |
| Time interval | The range of years covered by the study | RQ1 |
| References | Number of references listed in the study | RQ1 |
| Citations | Number of citations got by the study | RQ1 |
| Number of RQs | Number of RQs investigated | RQ2 |
| Surveyed papers topic | Number of papers investigated in deep | RQ1 |
| Topic | Topic addressed by the study | RQ2 |
| Paper's key words | List of key words proposed by authors of the study | RQ2 |
| The RQs | The research questions addressed in the study | RQ2 |
| ML method(s) | ML Method(s) mentioned/cited | RQ3 |
| Application area | The application area of the paper | RQ2 |
| Computing paradigm | The computing paradigm mentioned/Cited | RQ4 |
| Employed IoT devices | Employed IoT devices in Smart Home/Smart Building's implementation | RQ4 |
| Classification Scheme | The logical structure or classification framework used by the review to organize and analyze the studies | RQ2, RQ3 |
| Contribution | Contribution of the study | RQ2, RQ3 |

The outcome of this process was documented in dedicated individual data extraction tables, each comprising a column for every metadata category. These tables were progressively populated with the relevant information retrieved from the papers during the synthesis phase. The adoption of a predefined and systematic extraction structure ensured traceability, reproducibility, and methodological transparency.

#### 3.2.3. Data Synthesis

The data synthesis phase aimed to systematically integrate and interpret the information extracted from the selected studies to provide robust, evidence-based answers to the research questions defined in the review protocol. Each included article corresponds to a row within the extraction matrix, and the synthesis process consisted of comparatively aggregating these rows into a coherent and structured analytical framework.

The analysis of each study was independently conducted by all authors, with any discrepancies resolved through discussion and consensus to ensure the reliability of the process.

Tables 10–16 present the data synthesis of the 13 selected studies.

**Table 10.** Data synthesis from studies (1).

| Refs. | Source | Year | Length | Scientific DB(s) |
|---|---|---|---|---|
| [181] | Journal | 2024 | 46 | Not declared |
| [182] | Journal | 2025 | 67 | Scopus<br>Google Scholar |
| [183] | Journal | 2025 | 34 | Scopus<br>Google Scholar |
| [184] | Journal | 2025 | 17 | Web of Science<br>Science Direct<br>Scopus<br>IEEE Xplore<br>EBSCOhost<br>ProQuest |
| [185] | Journal | 2025 | 33 | IEEE Xplore<br>Springer<br>ScienceDirect<br>Google Scholar<br>ResearchGate |
| [186] | Journal | 2025 | 15 | Scopus |
| [187] | Conference | 2025 | 7 | Scopus<br>IEEE Xplore<br>ScienceDirect<br>Google Scholar |
| [188] | Journal | 2025 | 57 | Google Scholar |
| [189] | Journal | 2025 | 26 | Scopus<br>IEEE Xplore<br>Google Scholar<br>EUPVSEC |
| [190] | Journal | 2025 | 37 | Scopus<br>Web of Science<br>Google Scholar |
| [191] | Journal | 2024 | 19 | Web of Science Core Collection |
| [192] | Journal | 2024 | 42 | Not declared |
| [193] | Journal | 2025 | 35 | Not declared |

**Table 11.** Data synthesis from studies (2).

| Refs. | Time Interval | References | Citations | Number of RQs | Surveyed Papers |
|---|---|---|---|---|---|
| [181] | 2015–2021 | 91 | 5 | 5 | 51 |
| [182] | January 2016–December 2024 | 147 | 0 | 5 | 147 |
| [183] | 2013–2023 | 98 | 4 | 0 | 82 |
| [184] | 2021–2025 | 62 | 1 | 5 | 42 |
| [185] | 2019–2014 | 160 | 4 | 6 | 98 |
| [186] | 2019–2025 | 62 | 0 | 0 | 60 |
| [187] | 2015–2024 | 15 | 0 | 3 | 13 |
| [188] | 2015–2025 | 199 | 1 | 0 | 199 |

**Table 11.** *Cont.*

| Refs. | Time Interval | References | Citations | Number of RQs | Surveyed Papers |
|---|---|---|---|---|---|
| [189] | 2010–2025 | 154 | 0 | 0 | 154 |
| [190] | January 2004–March 2024 | 218 | 0 | 0 | 130 |
| [191] | 1991–2023 | 172 | 107 | 0 | 115 |
| [192] | 2016–2021 | 136 | 7 | 0 | 124 |
| [193] | 2020–2024 (mainly) | 20 | 0 | 0 | 17 |

**Table 12.** Data synthesis from studies (3).

| Refs. | Topic | Paper's Keywords |
|---|---|---|
| [181] | Data transmission reduction techniques and physical security. | Wireless Multimedia Sensor Networks (WMSN), Data transmission reduction, IoT, Energy saving, SLR, Compressive sensing, Machine and deep learning |
| [182] | A review on AIoT techniques for air quality monitoring systems, and environmental management. | Air quality monitoring, AI, DL, IoT, ML, predictive modeling, sensor calibration |
| [183] | A review of ultrasonic testing and evaluation methods in civil NDT/E for infrastructure Integrity. | Structural Health Monitoring (SHM), Non-Destructive Testing (NDT), Ultrasonic Testing (UT), Synthetic Aperture focusing Technique (SAFT), Total Focusing Method (TFM), Computed Tomography (CT), ML, sensor technologies, data analysis, civil infrastructure |
| [184] | A review of AI in video surveillance systems for physical security, such as suspicious activity detection and incident response. | AI, video vigilance, DL, security, SDG 16 |
| [185] | A review of ML and DL approaches for physical and software security, such as IDS in IoT environments and data management and transmission optimization. | Dataset balancing, feature selection, intrusion detection systems (IDS), IoT security, ML, DL |
| [186] | A systematic review of Digital twin applications for structural health monitoring, predictive maintenance, and smart city frameworks in the management of civil infrastructure integrity. | Digital twins, civil infrastructure, structural health monitoring, AI-driven predictive model, cybersecurity |
| [187] | SLR on the integration of Artificial Intelligence and IoT technologies for physical security, such as real-time threat detection and automated surveillance in smart home security systems. | Artificial intelligence, home security systems, AI-based surveillance, IoT in security, smart home technology, machine learning, computer vision |
| [188] | On the adoption of AIoT for solar energy efficiency, monitoring and control. | AI, IoT, AIoT, photovoltaic, fault detection and diagnosis, predictive maintenance, energy forecasting, solar energy monitoring, solar tracking, automated cleaning systems |
| [189] | A review of smart maintenance approaches using AIoT for PV systems, for energy efficiency. | AI, performance, photovoltaic, predictive maintenance, reliability |
| [190] | A review of piezo impedance-based SHM for reinforcement-concrete bond deterioration, for infrastructure integrity. | AI, bond strength, corrosion, EMI techniques, PZT sensor, reinforced concrete, structural health monitoring (SHM) |
| [191] | Review of recent advancements in the use of AI, sensors, and IoT for environmental management: detection and monitoring of hazardous substances and environmental pollution. | Environmental pollution, monitoring, safety, advance technologies, machine learning, IoT |

**Table 12.** *Cont.*

| Refs. | Topic | Paper's Keywords |
| --- | --- | --- |
| [192] | Systematic review of physical and software security challenges and solutions (traditional and intelligent) for HetIoT (Heterogeneous Internet of Things) networks in the era towards 6G. | Heterogeneous IoT, Lightweight cryptography, Intelligent security, Deep learning, Deep reinforcement learning, Lightweight access control |
| [193] | A review and comparison of image-based (ML/DL) and IoT-based sensing methods for the autonomous detection and monitoring of integrity and cracks in civil infrastructure and cultural heritage. | not declared |

**Table 13.** Data synthesis from studies (4).

| Refs. | The RQs |
| --- | --- |
| [181] | RQ1. What is the publication distribution and quantity between 2015 and 2021?<br>RQ2. What processes, methods, and techniques are employed for data reduction in WMSN?<br>RQ3. What are the benefits of data reduction in the context of WMSN?<br>RQ4. Did the studies under review utilize real experiments or simulation environments?<br>RQ5. What data sets are used in the analyzed research? |
| [182] | RQ1. What architectures have been used to build IoT-based air quality monitoring stations and what key features have been considered in their design?<br>RQ2. What data-related problems have been identified in IoT-based air quality monitoring?<br>RQ3. How have these data-related problems been addressed using AI techniques, such as ML and DL?<br>RQ4. What specific ML and DL models have been used to address data related problems in IoT-based air quality monitoring?<br>RQ5. What challenges remain in the implementation and scalability of AI-driven IoT-based air quality monitoring systems? |
| [183] | They are not explicit |
| [184] | RQ1. Which are the countries with the most research implemented and under development in the use of AI technologies applied to video surveillance systems?<br>RQ2. What are the main technologies that can be combined with AI to improve the efficiency and accuracy of video surveillance systems?<br>RQ3. What approaches to integrating AI with incident management systems improve critical event response in video surveillance environments?<br>RQ4. What are the recent trends in the development of architectures for real-time detection of suspicious activity in surveillance video?<br>RQ5. How have detection techniques in video surveillance systems influenced the identification of suspicious activity and incident response? |
| [185] | RQ1. What are the prevalent types of cyberattacks targeting IoT devices, and what makes securing IoT ecosystems inherently challenging?<br>RQ2. What countermeasures are currently employed to safeguard IoT networks?<br>RQ3. Which ML and DL methodologies are currently applied in IDS, especially for IoT networks, and what are their associated challenges?<br>RQ4. What datasets are predominantly utilized for evaluating ML or DL- based IDS, and how are issues of data imbalance addressed within these datasets?<br>RQ5. What feature selection strategies are employed in preparing datasets for IDS, and how do they contribute to developing lightweight IDS solutions?<br>RQ6. What are the emerging trends and future research directions for AI- powered lightweight IDS solutions in the IoT domain? |
| [186] | They are not explicit |
| [187] | RQ1. How Does AI Integration Enhance the Automation and Effciency of Home Security Systems?<br>RQ2. What Types of AI Technologies Are Commonly Used in Modern Home Security Systems?<br>RQ3. Why Is AI Considered a Transformative Technology for Improving Home Safety and Monitoring? |
| [188] | They are not explicit |
| [189] | They are not explicit |

**Table 13.** *Cont.*

| Refs. | The RQs |
|---|---|
| [190] | They are not explicit |
| [191] | They are not explicit |
| [192] | They are not explicit |
| [193] | They are not explicit |

**Table 14.** Data synthesis from studies (5).

| Refs. | Contribution |
|---|---|
| [181] | This SLR provides a foundation strategy and road map for reducing energy consumption in WMSNs, offering a detailed taxonomy of multimedia data reduction techniques (compression, compressive sensing, ML) for IoT-based smart surveillance system. |
| [182] | A classification framework for AI techniques in air quality monitoring, organized into five main application areas: data imputation, sensor calibration, anomaly detection, air quality index (AQI) estimation, and short-term forecasting. It highlights research gaps about data quality, system scalability and integration challenges in AI-driven IoT systems. |
| [183] | This article emphasizes methods for analyzing ultrasound signals and images used in the NDT of civil infrastructure. |
| [184] | The objective of this research is to analyze the role of artificial intelligence in video surveillance systems for suspicious activity detection and incident response in urban environments. |
| [185] | This article provides a comprehensive synthesis of the existing research on IoT security threats and various IDS solutions; it underscores the crucial role of dataset optimization, mainly through effective feature selection and data balancing, to enhance the performance of ML/DL algorithms in IDS. In addition, the paper thoroughly reviews various ML and DL techniques applicable to IDS and covers the available datasets most commonly used for training and testing IDS models. |
| [186] | This systematic review offers a comprehensive synthesis of digital twin applications in civil engineering, focusing on structural health monitoring, predictive maintenance, and smart city frameworks. |
| [187] | This SLR evaluates the evolution of AI-driven technologies—including ML, Computer Vision, and NLP—and their integration with IoT for modern home security systems. |
| [188] | This survey offers a structured framework and a detailed analysis of AIoT applications in solar energy. The authors classified AIoT implementations into key areas such as fault detection, predictive maintenance, energy forecasting, solar monitoring systems, and optimization techniques. |
| [189] | This article analyzes the synergy between AI and IoT for smart maintenance in PV systems, in particular the transformation from traditional maintenance to predictive maintenance. |
| [190] | The novelty of the study focuses on the detailed literature studies on performance evaluation of reinforcement-concrete bond deterioration using impedance-based techniques. |
| [191] | Review exploring recent advances in the integrated use of AI, sensors, and IoT technologies for environmental pollution monitoring, examining its specific application in soil, air, and water. |
| [192] | First review to combine HetIoT security analysis across three approaches (layered, traditional, and Intelligent—ML/DL/DRL), providing a comprehensive road map with the identification of challenges and solutions. |
| [193] | This study proposes an original taxonomy for crack analysis. It provides a comparative evaluation of image-based and IoT-based processing pipelines, offering a conceptual roadmap for a robust, integrated "Image-IoT" system designed to overcome current sensing limitations in civil infrastructure and cultural heritage monitoring. |

**Table 15.** Data synthesis from studies (6).

| Refs. | ML Methods | Computing Paradigm |
|---|---|---|
| [181] | DT, RF, SVM, Bayesian, K-NN, PCA, K-means, DL, RNN, CNN | Cloud, Edge, Fog |
| [182] | DT, RF, RFR, SVM, CNN, LSTM, KNN, DNN, DBSCAN, ELM, MLP, RNN, GRU, SOM | Cloud |
| [183] | DL, CNN, YOLO, RNN, ANN, CNN, DNN, TL, SVM | Cloud, Edge |
| [184] | DL, CNN, LSTM, RNN, AEs, YOLO, SSD | Edge |
| [185] | DT, SVM, K-NN, RF, NB, LR, CNN, LSTM, ANN, DNN, RNN, AEs, MLP, SOM | Cloud, Edge |
| [186] | ANN, RF, ERTR, XGBoost | Cloud, Edge |
| [187] | CNN | Fog |
| [188] | ANN, DNN, CNN, RNN, LSTM, ResNet, MLP, PNN, RBFNN, FFNN, FFBP, YOLO, KNN, RF, DT, SVM, GRNN | Edge-ML |
| [189] | DT, KNN, SVM, ELM, ANN, CNN, DCNN, MLP, DNN, LSTM | Cloud, Edge |
| [190] | DL, ANN, CNN, LSTM, AdminGAN | Not declared |
| [191] | ANN, ENN, MLANN, MLP, RBFNN, CNN, DL, ERF, BAGGED CART, DT, SVM, KNN, SVR | Cloud, Edge |
| [192] | SVM, KNN, LR, RF, XGBoost, MLP, ANN | Cloud, Edge, Fog |
| [193] | CNN, SVM, RFC, U-NET, Swin U-Net | Edge, Cloud |

**Table 16.** Data synthesis from studies (7).

| Refs. | Application Area | Classification Scheme |
|---|---|---|
| [181] | Video surveillance | The techniques are classified into four main categories: data redundancy reduction (using different image techniques); ML schemes; video compression schemes; compressive sensing. |
| [182] | Air quality monitoring | The review divides the research contributions according to the data management stages: missing value correction, sensor calibration, error detection, and forecasting techniques. |
| [183] | NDT | The research is divided into two areas: ultrasonic signal analysis; ultrasonic imaging techniques. |
| [184] | Video surveillance | The analysis follows an approach focusing on three elements: the geopolitical landscape; AI technological foundation; incident detection and response capabilities. |
| [185] | IoT intrusion detection | The research organizes the study of connected device protection into three fundamental pillars: IoT security threats and various IDS solutions, the application of ML and DL techniques, and the datasets used for training and testing IDS models. |
| [186] | Civil Infrastructure | The research categorizes the analyzed papers into five main thematic macro-areas: bridge monitoring and structural health monitoring; Building Information Modeling, Geographic Information Systems, and IoT Integration; risk assessment and asset management; smart cities and emergency response; methodological studies and reviews. |
| [187] | Home security systems | The work classifies scientific literature findings into eight critical aspects defining AI effectiveness in home security: real-time surveillance and monitoring, threat detection and response; 24/7 operational capability; integration with IoT and smart systems; customizable security protocols; cost efficiency over time; remote access and control; environmental adaptability. |
| [188] | Solar optimization | The focus is on the fault detection; predictive maintenance; energy forecasting; solar monitoring systems; optimization techniques. |
| [189] | PV Maintenance and Fault Diagnostics | This research investigates three different approaches: corrective maintenance; preventive maintenance; extraordinary maintenance. |
| [190] | Monitoring of cement-reinforcement bond | The analysis organizes construction monitoring into three main areas: concrete strength monitoring, EMI-based corrosion effects on bond strength, and the implementation of EMI techniques for bond strength monitoring. |

**Table 16.** *Cont.*

| Refs. | Application Area | Classification Scheme |
|---|---|---|
| [191] | Environmental monitoring | A dual and progressive classification is used to analyze the contributions, based on: 1. monitored environment: soil, air, water, 2. AI-Powered technology: spectroscopy (e.g., SERS, Vis-NIR), ground-based sensors (integrated with ML: KNN, SVM), aerial imaging/UAV (e.g., HSI), ground robotics, satellite remote sensing (MSS). |
| [192] | HetIoT infrastructure security | The classification used for HetIoT security analysis includes the following categories: layered approach (threats for the four layers); traditional approaches (lightweight cryptography, privacy/trust, access control); Intelligent Security (IS) (classification by AI/ML technique). |
| [193] | Civil Infrastructure and cultural heritage | The paper proposes a classification framework based on five orthogonal characteristics: functionality; categories; responsiveness; use case; testing methodology. |

## 4. Results

The research questions outlined in Section 3.1.2 are addressed in the following sections, drawing upon the evidence derived from the systematic analysis of the selected studies.

### *4.1. (RQ1) What Is the Map of Published SSs Concerning AIoT-Based Security Systems Within the Smart Home and Smart Building Application Domains?*

Tables 16 and 17 provide an overview of the chronological distribution and document types of the selected corpus. As shown in Table 17, scientific production is concentrated within the 2024–2025 time interval, with 77% of the contributions published in 2025. This finding highlights the emerging nature of AIoT integration within Security Systems and underscores the current relevance of the topic addressed.

**Table 17.** Temporal distribution of the studies.

| Year | Documents |
|---|---|
| 2025 | 10 |
| 2024 | 3 |

From a methodological perspective (Table 18), the selection comprises 13 journal publications (69% articles and 31% reviews), thereby ensuring the scientific robustness of the extracted findings.

**Table 18.** Classification of the studies by document type.

| Document Type | Documents |
|---|---|
| Article | 9 (69%) |
| Review | 4 (31%) |

The analysis of the distribution of papers across AIoT-based Security Systems detailed in Table 19 (and illustrated in Figure 3) reveals a marked predominance of monitoring systems, which are addressed in 12 out of 13 studies (92.3% of the sample). Security systems follow with a significant incidence, being examined in 6 out of 13 contributions (46.2% of the selected studies), while alarm systems are acknowledged in 4 out of 13 (accounting for 30.8% of the reviewed literature).

Surveillance and access control systems emerge as the least represented areas within the selected literature, each being identified in 3 out of 13 studies (23.1% of the analyzed corpus each).

Since individual studies may address multiple systems simultaneously, these percentages should be interpreted as indicators of system presence within the literature, rather than a mutually exclusive research focus.

**Table 19.** Classification of the studies across the identified AIoT-based Security Systems.

| Refs. | Security | Alarm | Surveillance | Monitoring | Access Control |
|---|---|---|---|---|---|
| [181] | ✔ | | ✔ | ✔ | |
| [182] | | | | ✔ | |
| [183] | | | | ✔ | |
| [184] | ✔ | | ✔ | ✔ | |
| [185] | ✔ | | | | ✔ |
| [186] | ✔ | | | ✔ | |
| [187] | ✔ | ✔ | ✔ | ✔ | ✔ |
| [188] | | | | ✔ | |
| [189] | | ✔ | | ✔ | |
| [190] | | | | ✔ | |
| [191] | | ✔ | | ✔ | |
| [192] | ✔ | ✔ | | ✔ | ✔ |
| [193] | | | | ✔ | |
| Tot. | 6/13 | 4/13 | 3/13 | 12/13 | 3/13 |

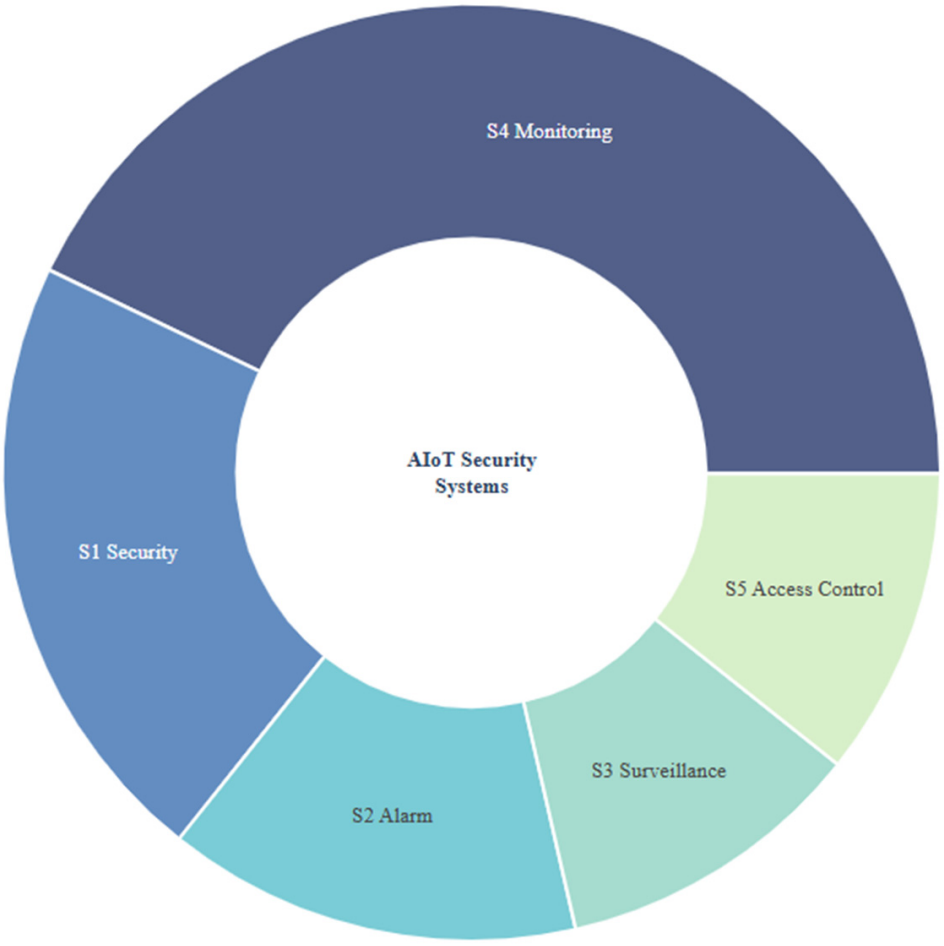


**Figure 3.** Distribution of Security Systems within the papers.

The clear predominance of monitoring systems (92.3%) is fundamentally driven by the operational imperatives of infrastructure safety and structural longevity. This strategic alignment reflects a transition from passive data collection toward proactive risk mitigation; as noted by Forlesi et al. [193], the priority lies in the early identification of structural anomalies to preclude catastrophic failures. Within this framework, the integration of Digital Twins [186] enables the seamless reconciliation of real-time monitoring and predictive simulations, reflecting the strategic convergence of these technologies in the AIoT landscape.

### *4.2. (RQ2) What Are the Main Topics Addressed Regarding AIoT-Based Security Systems Within the Smart Home and Smart Building Application Domains?*

To provide a comprehensive answer to RQ2, the thematic landscape of the selected studies has been synthesized through a multi-dimensional mapping.

Table 20 and Figure 4 offer a primary overview of the topics addressed within the analyzed corpus, highlighting the prevalence and frequency of each research theme. To further deepen this analysis, Figure 5 presents a heatmap that correlates the identified topics with the Security Systems. To ensure visual clarity and prevent graphical clutter within the matrix, alphanumeric indices are employed: topics are identified as T1–T6 (corresponding to the IDs established in Table 20), while Security Systems are represented by indices S1–S5 (specifically: S1—security, S2—alarm, S3—surveillance, S4—monitoring, and S5—access control). This dual representation enables an immediate visualization not only of the most debated subjects but also of the "hot spots" where research effort is most concentrated.

**Table 20.** Topic Coding.

| ID | Topic |
|---|---|
| T1 | Data Management and Transmission Optimization |
| T2 | Energy Efficiency |
| T3 | Environmental Management |
| T4 | Infrastructure Integrity |
| T5 | Logical Security |
| T6 | Physical Security |

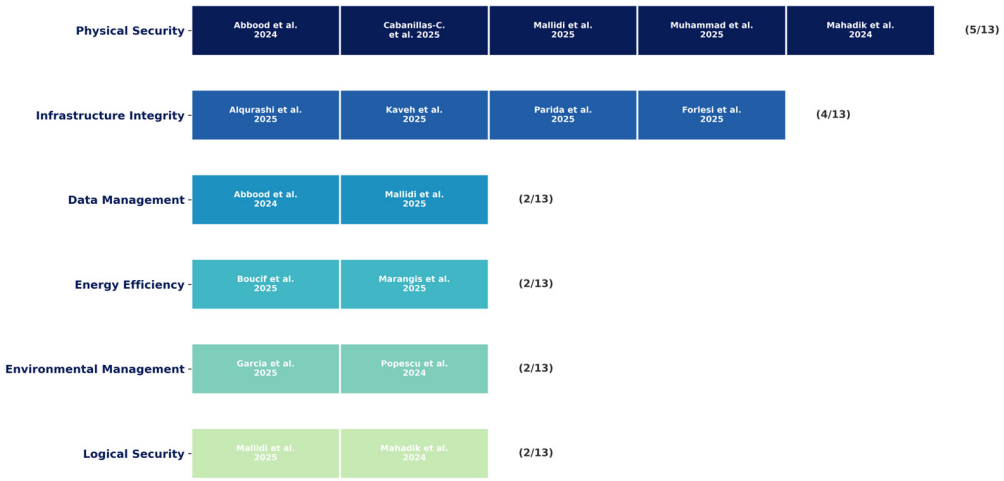


**Figure 4.** Thematic distribution and frequency of research topics in the selected literature [181–193].

The identification of these topics was made possible through a comparative analysis of the subjects explored in each examined work, resulting in the recognition of six distinct thematic areas. Table 21 relates each paper to the identified topics, presenting a matrix composed of the 13 selected studies, denoted by index <i>, and the six topics (T), denoted by index <j>. This representation facilitates a clear understanding of the covered topics and their relevance within the analyzed corpus.

The most frequently discussed topics in the examined SSs are listed below. For each topic, the number of papers addressing it is reported relative to the total. Given the interconnected nature of the themes and the analytical approach adopted—grounded in secondary contributions and oriented toward a holistic perspective—a single paper may be associated with multiple topics, reflecting the fact that many studies simultaneously address closely related content.


**Figure 5.** Heatmap mapping Security Systems against research topics.

**Table 21.** Cross link between the 6 topics in Table 20 (the columns <j>) and the SSs (the rows <i>).

| Refs. | T1 | T2 | T3 | T4 | T5 | T6 |
|---|---|---|---|---|---|---|
| [181] | ✔ | | | | | ✔ |
| [182] | | | ✔ | | | |
| [183] | | | | ✔ | | |
| [184] | | | | | | ✔ |
| [185] | ✔ | | | | ✔ | ✔ |
| [186] | | | | ✔ | | |
| [187] | | | | | | ✔ |
| [188] | | ✔ | | | | |
| [189] | | ✔ | | | | |
| [190] | | | | ✔ | | |
| [191] | | | ✔ | | | |
| [192] | | | | | ✔ | ✔ |
| [193] | | ✔ | | ✔ | | |

The ordering of the topics reflects the number of studies that engage with them, following a descending frequency based on their occurrences within the selected sample.

#### 4.2.1. Physical Security (5/13)

Physical security in Smart Homes and Smart Buildings focuses on the monitoring and protection of individuals and physical infrastructures through sensor-based systems and AI-driven analysis. The integration of AIoT-enabled smart ecosystems offers advanced operational intelligence and automation capabilities [185]. Key aspects related to this topic include the early identification of potential threats, enabled by the analysis of data collected from embedded sensors and video surveillance systems, which in turn allow for the detection of suspicious activity through AI-based techniques applied to video streams, such as pattern recognition and anomaly detection [184]. Compared to traditional standalone systems, these solutions support proactive threat prevention and automated responses, such as access restriction and alarm activation, significantly improving reaction time and protection effectiveness [181,187].

Another key feature is the access control mechanism, which regulates user and device permissions within smart environments, often relying on biometric authentication and multi-level authorization protocols. AI-based Security Systems also enable remote monitoring and control through digital interfaces, allowing users to manage security devices and respond to alerts in real time from any location [187,192]. Additional capabilities include continuous 24/7 operation, customizable security protocols, environmental adaptability, and long-term cost efficiency through automation and smart resource management [187].

#### 4.2.2. Infrastructure Integrity (4/13)

The main goal of infrastructure integrity is to evaluate and monitor the health condition of buildings and infrastructures through SHM, which integrates techniques such as NDT. The integration of AIoT technologies represents a natural evolution of SHM systems, enabling continuous monitoring and predictive analysis. Specifically, UT and piezoelectric-based EMI detect internal defects and early-stage damage in reinforced concrete [190]. In this context, ML has significantly improved automated defect detection, enabling real-time monitoring and classification of cracks by type, size, and progression over time [183,193].

Digital twins, often integrated with BIM and IoT platforms, extend SHM capabilities by supporting real-time structural assessment, risk management, and predictive maintenance, including seismic vulnerability analysis and early-warning applications for reinforced concrete buildings [186].

#### 4.2.3. Data Management and Transmission Optimization (2/13)

Data management and transmission optimization in IoT and WMSNs leverage AI-driven preprocessing, feature extraction, and data reduction to ensure that only the most relevant information is processed, thereby reducing computational overhead and enabling real-time analytics [181,185]. The integration of AIoT technologies supports continuous data collection and ML-based analysis, facilitating process optimization and improving overall system efficiency. In-network processing and Fog-node architectures minimize Cloud dependency, while transmission optimization lowers energy consumption by limiting multimedia data size, addressing the high-power demands of IoT data transfer [186].

#### 4.2.4. Energy Efficiency (2/13)

In modern power systems, energy efficiency is largely driven by the adoption of solar photovoltaic (PV) technologies. These solutions ensure optimal management of energy production and help meet rising electricity demands [188]. Solar PV systems are key enablers of a sustainable energy mix, reducing reliance on fossil fuels and supporting the transition toward greener power systems, while smart PV monitoring solutions enhance their grid integration through anomaly detection, failure prediction, and automated maintenance based on the system's operational status and health state [188,189]. The integration of AIoT technologies into photovoltaic systems enables a shift from reactive maintenance to intelligent and predictive approaches, thereby improving system reliability and performance [185].

#### 4.2.5. Environmental Management (2/13)

The use of AI- and IoT-based sensor systems in environmental monitoring and control enables the detection of pollution and general environmental parameters, including air pollutants, water contaminants, and soil toxins [191]. These technologies also support indoor air quality monitoring and urban pollution prediction, facilitating effective air quality management and impact mitigation, even in resource-constrained environments [182].

#### 4.2.6. Logical Security (2/13)

Logical security is the topic concerned with protecting digital systems, networks and data form cyber threats. In this context, Intelligent Security (IS) uses ML to monitor IoT devices and network activity in real time, learning from past behavior to predict and mitigate attacks, including zero-day vulnerabilities [192]. IDSs are operational tools within IS which identify anomalies and complex attack patterns by applying ML and DL techniques. These mechanisms address a wide range of threats across multiple system layers, including physical, network, and application-level attacks, supported by cryptographic, access control, and trust management approaches [185,192]. The integration of AIoT technologies represents a central component, playing a critical role within this security context.

The correspondence between the five systems and the six extracted topics is illustrated in Figure 5 using a heatmap that cross-tabulates each Security System (S) against the identified topics (T). This heatmap reports the number of papers associated with each system–topic intersection.

This visual representation enables an immediate assessment of the distribution and intensity of research efforts across different contexts, highlighting both the thematic coverage of each system and the relative concentration of studies within the analyzed sample.

To complement this, Table 22 offers a structured synthesis of the evidence presented in Figure 5, including individual paper references, thereby providing a traceable mapping of the observed distribution.

**Table 22.** Convergence matrix: correlation between Security Systems and topics.

| Topic | System | Refs. |
|---|---|---|
| T1 | S1, S3, S4, S5 | [181,185] |
| T2 | S2, S4 | [188,189,193] |
| T3 | S2, S4 | [182,191] |
| T4 | S1, S4 | [183,186,190,193] |
| T5 | S1, S2, S4, S5 | [185,192] |
| T6 | S1, S2, S3, S4, S5 | [181,184,185,187,192] |

### *4.3. (RQ3) What Are the Key ML Algorithms, Methods and Techniques Predominantly Employed in the Implementation of AIoT-Based Security Systems Within the Smart Home and Smart Building Application Domains, and What Are the Reasons for Their Adoption?*

The evidence concerning RQ3 is derived from the data extraction synthesized in Table 15 and the cross-analysis of studies previously mapped within the framework of RQ1 (Table 19). To ensure a cohesive and systematic analysis, data are categorized according to the five identified Security Systems: security, alarm, surveillance, monitoring, and access control.

To provide a quantitative visual representation of these distributions, Figure 6 illustrates the distribution of ML methods across these systems, highlighting the prevalence of specific methodologies within each Security System.

Consequently, Table 23 outlines this convergence by correlating prevalent ML methods and techniques with their respective motivations, thereby formalizing the alignment between specific system requirements and the adopted ML solutions.

#### 4.3.1. Security

The synthesized evidence from the selected literature [184,185,192] underscores a fundamental shift in the security architecture of AIoT-enabled environments. This evolution is driven by the imperative to safeguard not only digital assets but also the physical and structural integrity of the built environment.

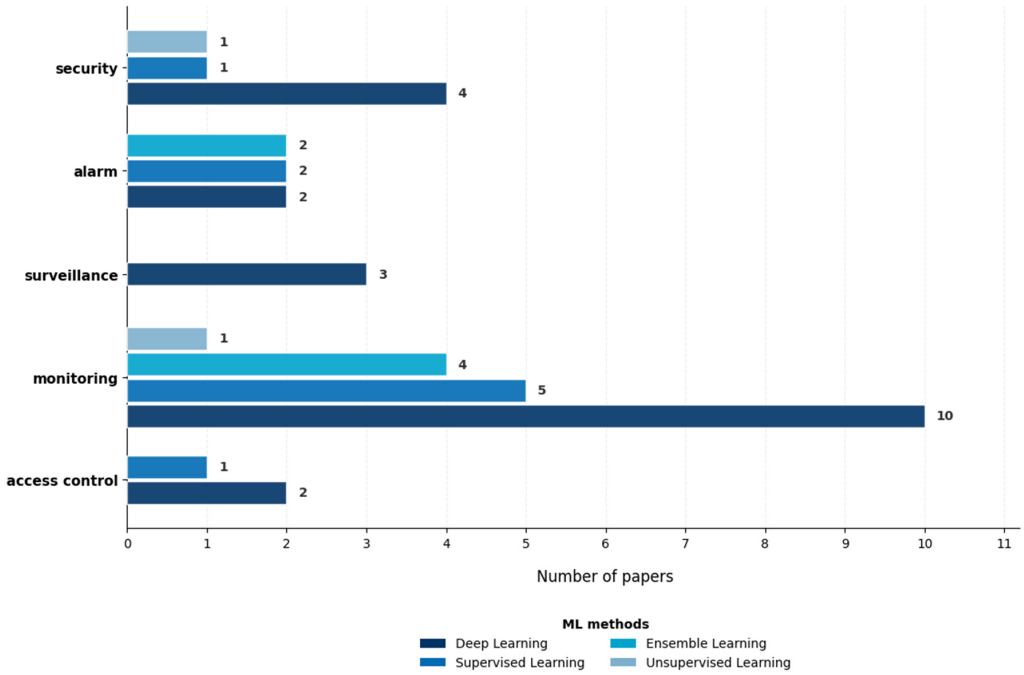


**Figure 6.** Distribution of ML methods across AIoT Security Systems.

**Table 23.** Mapping of Security Systems to ML methods and techniques.

| Systems | Refs. | ML Methods and Techniques | Motivation |
|---|---|---|---|
| S1 | [181,184–187,192] | Deep Learning (AEs, CNN, RNN, LSTM); Ensemble Learning (RF, XGBoost), Supervised Learning (DT, SVM, K-NN), Unsupervised Learning (K-Means) | (1) spatial-temporal complexities and semantic interpretation (DL); (2) Real-time detection and privacy-by-design (Ensemble/Supervised); and (3) identification of unlabeled anomalies or zero-day attacks (Unsupervised) |
| S2 | [187,189,191,192] | Ensemble Learning (RF, XGBoost); Deep Learning (AEs, CNN, YOLOv5, LSTM, SSD) Supervised Learning (DT, SVM, K-NN) | (1) zero-latency visual and sequential triggering for real-time incident identification (DL); (2) proactive early-warning capabilities through predictive anomaly detection (DL); (3) high-fidelity event validation to minimize false-positive (Ensemble/Supervised) |
| S3 | [181,184,187] | Deep Learning (CNN, YOLO) | (1) high-speed automated localization and identification of physical threats in complex visual environments (DL) |
| S4 | [181–184,186–193] | Ensemble Learning (Extreme RF), Deep Learning (AEs, CNN, LSTM) Supervised Learning (SVM, K-NN), Unsupervised Learning (DBSCAN) | (1) spatio-temporal modeling of environmental dynamics and structural degradation patterns (DL); (2) high-precision sensor calibration and predictive accuracy across heterogeneous, high-dimensional datasets (Ensemble Learning); and (3) efficient classification of structural health indicators and signal-based anomaly detection (Supervised Learning) |
| S5 | [185,187,192] | Deep Learning (CNN), Supervised Learning (SVM) | (1) high-precision biometric authentication for automated and secure entry management (DL); and (2) feature extraction for real-time identity verification and unauthorized access prevention in heterogeneous IoT security environments (DL). |

A dominant trend identified in response to RQ3 is the strategic adoption of hybrid architectures. While Ensemble Learning models—specifically RF and XGBoost—coupled with rigorous dataset balancing techniques remain the benchmark for IDSs in HetIoT

networks [192], a significant trajectory is observed toward the integration of DL and Computer Vision for physical protection [184].

#### 4.3.2. Alarm

The synthesis of the eight selected contributions [187,189,191,192] identifies Predictive Anomaly Detection as the technological cornerstone of contemporary AIoT-driven alarm systems. Within industrial and infrastructural frameworks [189], the integration of sophisticated ML and DL architectures facilitates a paradigm shift from reactive alerting to proactive diagnostics. Specifically, the deployment of the XGBoost algorithm, as demonstrated by Marangis et al. [189], yields a predictive accuracy of 98.62% in identifying maintenance requirements, thereby optimizing Operation & Maintenance (O&M) strategies.

#### 4.3.3. Surveillance

The selected contributions [181,184,187] delineate a transformative evolution in surveillance systems: monitoring is no longer characterized by passive observation process but has evolved into automated surveillance and real-time threat detection. DL emerges as the predominant technological driver, evidenced by the pervasive adoption of CNNs—spanning both 2D and 3D architectures—and state-of-the-art object detection frameworks such as YOLO [184]. According to the evidence gathered for RQ3, these methodologies are strategically prioritized to satisfy several critical technical imperatives.

Firstly, feature automation [184,187] represents a significant evolutionary step; CNNs eliminate the necessity for manual feature engineering by autonomously learning complex spatial hierarchies directly from raw video streams. Secondly, for sophisticated temporal analysis [184], 3D CNN and ConvLSTM architectures are deployed to interpret temporal sequences, thereby enabling the system to distinguish between normal activities and suspicious behavioral patterns with high granularity.

#### 4.3.4. Monitoring

The analysis carried out within this review suggests that monitoring constitutes the most mature system within the current AIoT landscape. The evidence gathered for RQ3 reveals a definitive shift in the state-of-the-art toward CPS. In this context, the contribution of Kaveh and Alhajj [186] is particularly relevant: the implementation of digital twins transcends mere observation, enabling the proactive simulation of infrastructural states fed by continuous, real-time IoT telemetry. This architectural framework redefines monitoring, transitioning it from a reactive diagnostic activity into a fundamental pillar of structural and operational resilience.

Furthermore, a significant convergence is observed regarding the deployment of AI for data calibration and accuracy enhancement across heterogeneous contexts. Within the domain of environmental monitoring, Garcia et al. [182] and Popescu et al. [191] demonstrate how advanced architectures—specifically Transformers (e.g., AirFormer) and Ensemble models (RF)—are indispensable for mitigating the intrinsic uncertainty of raw sensor telemetry and low-cost hardware. Similarly, the monitoring of civil infrastructures leverages highly specialized methodologies, such as PISHM [190] and ultrasonic signal analysis coupled with ML classifiers [183]. These findings confirm that the most effective technological response to RQ3 resides in the seamless integration of complex physical signals with high-fidelity digital predictive models, ensuring unprecedented precision in NDT and multi-modal sensing contexts.

#### 4.3.5. Access Control

Studies [187,192] outline an access control framework characterized by the convergence of physical and logical protection layers. In response to RQ3, two primary tech-

nological trajectories are identified: the implementation of DL architectures—specifically CNN—and Grassmann's algorithm [187] for advanced biometric authentication, complemented by lightweight cryptography protocols and trust-based management mechanisms [192].

Overall, the selection of ML approaches in AIoT-based security systems is primarily driven by data complexity, real-time constraints, and labeling availability: DL emerges as the predominant paradigm for perception-intensive and spatio-temporal tasks (e.g., surveillance, biometric access control), while Ensemble and Supervised Learning remain preferred for high-precision decision-making and false-positive reduction in IDS and monitoring systems; Unsupervised Learning is selectively adopted when labeled data are unavailable and zero-day or anomalous behaviors must be identified.

### *4.4. (RQ4) Which Computing Paradigms, Among Edge, Fog and Cloud, Are Currently the Most Widely Employed Solutions for Data Processing in AIoT-Based Security Systems Within the Smart Home and Smart Building Application Domains, and What Are the Reasons for Their Adoption?*

The systematic synthesis of the reviewed literature elucidates a profound paradigm shift in data management strategies: the conventional Cloud-centric architecture, traditionally prioritized for its near-infinite computational elasticity, is increasingly being superseded by a decentralized, distributed ecosystem. Within the surveyed papers, the determination of the optimal data-processing location is no longer dictated by simple cost-efficiency metrics; rather, it is driven by stringent, non-negotiable operational imperatives—such as ultra-low latency requirements, bandwidth preservation, and local autonomy—which necessitate a transition towards Edge and Fog computing layers.

This prioritization of specific computing tiers is governed by a multifaceted set of technical determinants. Primarily, the need for near-zero latency and real-time responsiveness facilitates localized processing at the data source; such immediate intervention is a critical requirement in mission-critical scenarios, including acute pollution surges [191], DDoS attacks on IoT networks [192], and the propagation of structural instabilities [193].

Secondly, data privacy and security frameworks benefit significantly from Edge/Fog paradigms. By confining sensitive data processing within the local perimeter, these architectures drastically reduce the attack surface and mitigate the risk of data exfiltration during transit to remote servers—a vital consideration for HetIoT ecosystems [192].

Additionally, the optimization of network bandwidth remains a decisive factor. Large-scale environmental or structural sensing grids generate vast volumes of bandwidth-intensive telemetry that preclude continuous transmission. Implementing data filtering and edge-based pre-processing not only alleviates network congestion but also extends the operational lifespan of energy-constrained devices [181,192].

Finally, despite the shift towards the periphery, hardware-induced computational constraints persist. Since edge nodes typically possess restricted processing power, the Cloud remains the exclusive environment for high-complexity DL model training, Big Data analytics, and long-term historical storage. Hence, this inherent limitation makes the adoption of hybrid and federated architectural approaches a technical necessity for modern AIoT-based Security Systems [191–193].

Consequently, Edge and Fog computing emerge as the primary architectural benchmarks for data ingestion and real-time inference-grade workloads. In this decentralized framework, the Cloud layer undergoes a functional repositioning, evolving into a high-level strategic orchestrator dedicated to large-scale historical telemetry analysis and the iterative refinement of complex ML models.

To provide a structured synthesis of these findings, the RQ4 Matrix (Table 24) and Figure 7 presented below delineate the distribution of these architectural paradigms and identify the specific motivations mapped across each Security System analyzed in this review.

**Table 24.** RQ4 Matrix.

| System | Computational Paradigm | Refs. | Motivation |
|---|---|---|---|
| S1 | Hybrid (Edge-Cloud) | [181,184–187,192] | (1) ensures offline operational autonomy and network fault resilience (2) optimizing multimedia bandwidth through localized data reduction, (3) employs distributed defense and monitoring to mitigate centralized architectural vulnerabilities |
| S2 | Edge/Fog | [187,189,191,192] | (1) guarantees near-zero latency for life-critical alerts (2) and proactive warnings (3) through network-independent processing to ensure continuous reliability |
| S3 | Edge | [181,184,187] | (1) optimizes uplink bandwidth through localized multimedia data reduction (2) and safeguards privacy by confining sensitive visual processing to the network edge |
| S4 | Hybrid (Edge-Cloud) | [181–184,186–193] | (1) filters high-frequency raw data at the edge (2) while leveraging cloud resources for long-term predictive analytics and digital twin modeling (3) to optimize transmission efficiency and insight depth |
| S5 | Edge/Fog | [185,187,192] | (1) enables real-time biometric authentication (2) and lightweight cryptographic validation to ensure secure access in resource-constrained environments |

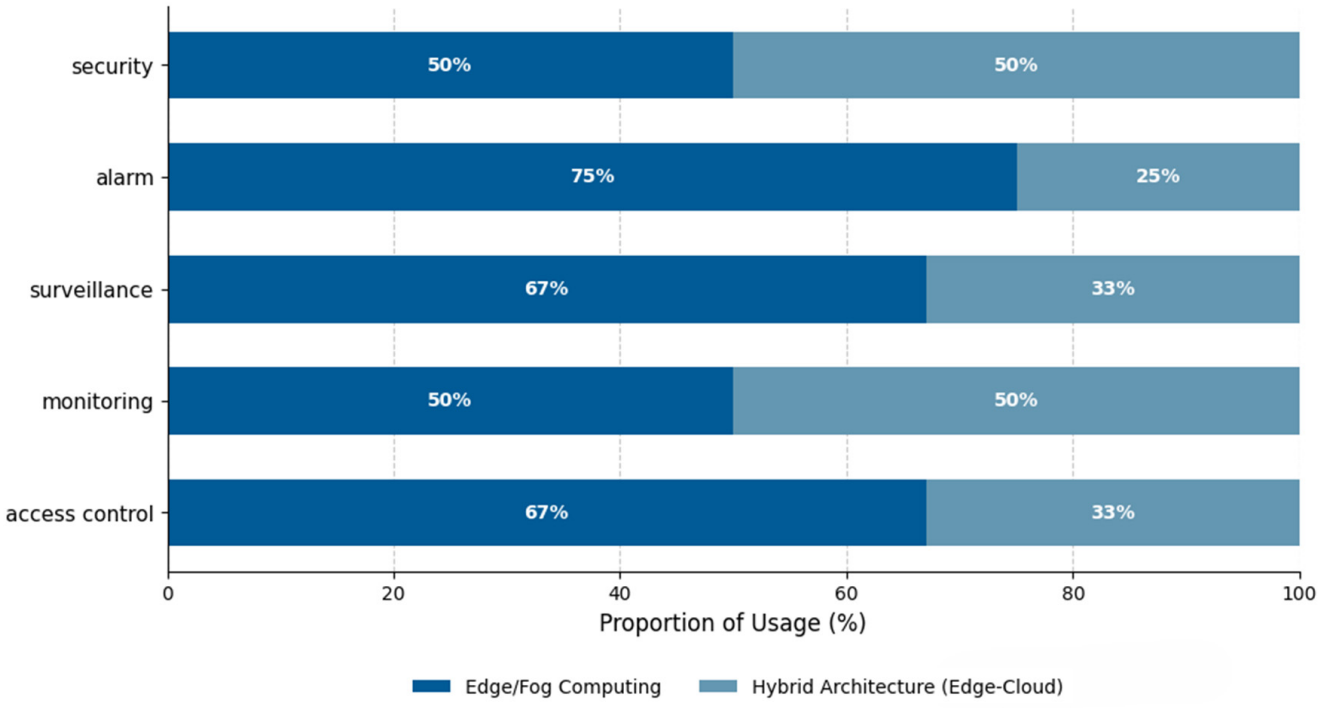


**Figure 7.** Percentage distribution of computing architectures.

Based on the examination of motivations behind their adoption, the five systems can be aggregated into two distinct macro-clusters that elucidate their respective architectural rationales.

4.4.1. The "Action-Oriented" Cluster (Alarm, Surveillance, Access Control)

In this cluster, the operational utility of data is transient and strictly coupled with the immediacy of the required intervention. Consequently, the adoption of Edge Computing/Fog Computing for network reliability is an architectural imperative. Current literature establishes that delegating mission-critical triggers—such as fire alarms or smart-lock deactivation—to the Cloud introduces critical vulnerabilities related to centralized architecture and connectivity dependence. As underscored by Muhammad et al. [187],

in domains such as domestic security, processing must be executed on-device to ensure physical safety regardless of network status. Similarly, for surveillance, local pre-processing mitigates the bandwidth bottlenecks inherent in multimedia telemetry.

#### 4.4.2. The "Data-Oriented" Cluster (Monitoring, Security)

These systems exhibit an operational duality that mandates the adoption of a hybrid architecture. While localized Edge inference is required for prompt intervention—such as detecting a structural crack [193] or a DDoS attack burst [192]—the high-level security logic and long-term monitoring rely on the Cloud's analytical depth.

In the security and monitoring sub-sectors, the Cloud remains irreplaceable for hosting threat intelligence databases, complex anomaly detection algorithms, and digital twin simulations [186] that require spatial and temporal aggregation. In this configuration, the Edge acts as a first-line autonomous filter for data reduction [181], while the Cloud operates as the centralized computational engine for long-term data analytics focused on predictive maintenance [189] and for the coordinated management of security protocols at the network infrastructure level.

The synthesis of the reviewed literature highlights a decisive predominance of Edge/Fog Computing solutions (dark blue) in high-criticality operational clusters, specifically alarm (75%) and surveillance and access control (67% each), where sub-second latency is the primary functional requirement. In contrast, monitoring and security systems exhibit a balanced distribution (50%) with hybrid architectures, reflecting the structural necessity to integrate localized raw data processing with the historical and predictive analytics delegated to the Cloud. The complete absence of purely Cloud-centric solutions (0%) corroborates a definitive paradigm shift in computational offloading toward the network periphery.

Overall, the choice between edge/fog and hybrid architectures is primarily driven by the temporal criticality of data usage and the need for global analytical context: systems requiring immediate, safety-critical responses favor edge/fog solutions, while applications combining real-time detection with long-term analytics structurally require hybrid architectures.

## 5. Open Challenges and Future Directions

While the systematic evidence-based mapping provided in the preceding sections demonstrates a sophisticated synergy between AI and the IoT for securing smart infrastructures, the actual operationalization of these frameworks remains highly intricated. The transition from isolated experimental models to holistic, Edge-integrated implementations within Smart Home and Smart Building ecosystems is currently hampered by a set of pervasive technical and systemic impediments.

### *5.1. The Lab-to-Field Gap and Data Dependency Constraints*

A critical challenge concerns the pronounced dependency on annotated datasets, which fosters a profound "lab-to-field" gap between laboratory-validated performance and actual operational efficacy. In this regard, Ref. [193] observes that the scarcity of large-scale, pre-labeled datasets in dynamic domestic environments severely constrains the accuracy of monitoring and surveillance architectures. This deficiency is particularly detrimental for proactive predictive analysis which, as underscored by [189], remains significantly underutilized compared to traditional reactive models, thereby limiting the capacity for preemptive threat mitigation. To mitigate this reliance, future research directions suggest a paradigm shift toward unsupervised learning frameworks and the synergistic integration of digital twins. According to [186], these high-fidelity virtual replicas can serve as generative

engines for synthetic data, enabling the simulation of realistic structural anomalies and security breaches prior to physical deployment.

### 5.2. Computational Resource-Performance Trade-Offs in Edge Architectures

Alongside data management constraints, a significant challenge emerges regarding the trade-off between computational overhead and performance within Edge architectures. Although computational proximity ensures reduced latency and enhanced privacy preservation, the execution of resource-intensive DL models on IoT nodes—characterized by inherent memory and battery limitations—remains problematic. As [181,184] highlight, real-time processing of complex video streams often imposes a computational burden that is unsustainable for standard commercial hardware. Consequently, the research focus is shifting from maximizing absolute accuracy toward optimizing algorithmic efficiency. In this context, Ref. [185] identifies the standardization of feature selection techniques as a fundamental enabler for developing lightweight IDSs capable of sustained operation at the network periphery.

### 5.3. Systemic Fragmentation and Interoperability in HetIoT Ecosystems

Finally, the fragmentation of HetIoT ecosystems, particularly concerning inter-component communication, constitutes an additional barrier to the realization of uniform, global security policies. The coexistence of multi-vendor sensors and actuators, operating via non-interoperable protocols, inevitably expands the attack surface for both logical and physical threats. As emphasized in [192], the absence of a unified AIoT framework, as explicitly noted by Boucif et al. [188], perpetuates technological "silos" that complicate the implementation of standardized security protocols. Overcoming this fragmentation necessitates a concerted effort toward the development of hardware-agnostic middleware. From this perspective, the adoption of distributed architectures based on Federated Learning appears particularly promising: this paradigm enables the collaborative training of anomaly detection models across heterogeneous networks, preserving the confidentiality of sensitive raw data while simultaneously addressing the requirements of interoperability and privacy.

## 6. Threats to Validity

The rigorous adherence to the methodology ensures the reliability of the findings in this TS; nonetheless, certain threats to validity must be acknowledged and mitigated. To ensure the construct validity of the research, we optimized our search strategy by identifying key terms encompassing Security Systems within the AIoT domain, utilizing Scopus as the primary repository due to its comprehensive coverage of software engineering and IoT literature. Internal validity risks were neutralized through a multi-stage screening protocol. Involving multiple reviewers is a recommended practice to minimize bias in activities requiring subjective judgment [58]; accordingly, the selection process followed a sequential analysis of titles, abstracts, and full texts based on predefined inclusion and exclusion criteria (EC1–EC5). Furthermore, the quality of the included reviews was appraised using 15 specialized Quality Criteria (QC1–QC15), ensuring that the synthesis is predicated on high-standard academic evidence.

Regarding external validity, while the findings are intrinsically linked to the scope and quality of the underlying SSs, the inclusion of diverse topics—such as structural health monitoring and energy efficiency—along with a temporal focus on the 2024–2025 period, guarantees that the conclusions reflect the current state-of-the-art in a rapidly evolving technological landscape. Finally, conclusion validity was addressed by employing a systematic data extraction and synthesis framework aligned with established guidelines. The

implementation of detailed synthesis tables (e.g., Tables 10 and 11) provides a transparent audit trail, facilitating a verifiable mapping between the primary evidence and the thematic conclusions presented throughout the study.

## 7. Conclusions

The TS conducted on AIoT-based Security Systems within the Smart Home and Smart Building application domains provides a multifaceted understanding of the current research landscape. A set of 13 studies was selected for an in-depth analysis, highlighting a rapid growth in scientific production, with the majority of contributions emerging in 2025. Monitoring systems dominate the literature, followed by security and alarm architectures, whereas surveillance and access control remain comparatively underrepresented, indicating an uneven distribution of research attention.

From a meta-analytical perspective, the study integrates thematic trends, ML methodologies, and computing paradigms into a unified interpretative framework. This cross-layer synthesis offers a technically grounded overview of how research priorities translate into architectural and algorithmic choices, bridging descriptive mappings with the operational implications of AIoT integration.

Architecturally, Edge and Fog computing paradigms are increasingly adopted to meet latency, privacy, and bandwidth requirements, while Cloud resources remain essential for historical analytics and training of complex models. ML techniques, particularly hybrid ensembles, DL architectures, and computer vision models, are deployed in alignment with system requirements, highlighting the necessity of co-designing algorithms and infrastructural configurations.

Despite these advances, critical consolidation needs persist. Data scarcity and the reliance on annotated datasets hinder the transferability of laboratory-validated models to operational contexts. The computational demands of advanced ML/DL models challenge sustainable Edge deployment, and the lack of standardized AIoT frameworks and interoperable security policies amplifies fragmentation across heterogeneous ecosystems, increasing exposure to both logical and physical threats.

In addition, this review highlights an emerging research gap concerning the systematic inclusion of human behavior and activities of daily living monitoring within AIoT-based security systems, suggesting that future research should progressively shift from an infrastructure-centric perspective toward a more user-oriented approach, where behavioral analysis plays a central role in proactive risk detection, adaptive security policies, and personalized emergency response.

Overall, while AIoT-based Security Systems demonstrate growing sophistication, a coordinated focus on underrepresented systems and proactive technological strategies is required to ensure scalable and resilient integration within smart environments.

**Author Contributions:** Conceptualization, G.P. and F.P.; methodology, G.P.; validation, G.P., L.D.S.F. and A.P.; formal analysis, G.P. and F.P.; investigation, F.P., L.D.S.F. and A.P.; resources, G.P.; data curation, S.T., L.D.S.F. and A.P.; writing—original draft preparation, S.T., L.D.S.F. and A.P.; writing—review and editing, F.P., S.T., L.D.S.F. and A.P.; visualization, L.D.S.F. and S.T.; supervision, F.P.; funding acquisition, G.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

**Acknowledgments:** Authors thank Paolino Di Felice for his methodological support during the preparation of this paper. During the preparation of this manuscript, the authors used Google Colab (https://colab.research.google.com/, accessed on 4 June 2026) for the purposes of creating the figures.

**Conflicts of Interest:** Francesco Pilotti and Lia Di Sabatino Farinelli are employed by the company Gruppo S.I. S.c.a.r.l.; Aurora Pavone, Simone Tinelli and Gaetanino Paolone are employed by the company B2B S.r.l. The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| AEs | Autoenconders |
| AI | Artificial Intelligence |
| AIoT | Artificial Intelligence of Things |
| ANN | Artificial Neural Network |
| API | Application Programming Interface |
| AQI | Air Quality Index |
| AR | Augmented Reality |
| BDA | Big Data Analytics |
| BMS | Building Management Systems |
| CNN | Convolutional Neural Network |
| CPS | Cyber-Physical Systems |
| CT | Computed Tomography |
| DBSCAN | Density-Based Spatial Clustering of Applications with Noise |
| DCNN | Deep Convolutional Neural Network |
| DDoS | Distributed Denial of Service |
| DL | Deep Learning |
| DNN | Deep Neural Network |
| DoS | Denial of Service |
| DT | Decision Tree |
| ELM | Extreme Learning Machine |
| EMI | Electro-Mechanical Impedance |
| ERTR | Extreme Randomized Trees |
| FFBP | Feedforward Backpropagation Neural Networks |
| FFNN | Feedforward Neural Network |
| FWI | Fire Weather Index |
| GIS | Geographic Information System |
| GRNN | General Regression Neural Network |
| GRU | Gated Recurrent Unit |
| HVAC | Heating, Ventilation and Air Conditioning |
| IaaS | Infrastructure as a Service |
| ICT | Information and Communication Technology |
| IDS | Intrusion Detection System |
| IoE | Internet of Everything |
| IoET | Internet of Energy Things |
| IoMT | Internet of Medical Things |
| IoRT | Internet of Robotic Things |
| IoT | Internet of Things |
| IS | Intelligent Security |
| KNN/K-NN | K-Nearest Neighbors |
| LG/LR | Logistic Regression |
| LSTM | Long Short-Term Memory |
| ML | Machine Learning |
| MLP | Multilayer Perceptron |

| | |
|---|---|
| NB | Naive Bayes |
| NDT | Non-Destructive Testing |
| NDT/E | Non-Destructive Testing/Evaluation |
| O&M | Operation & Maintenance |
| PaaS | Platform as a Service |
| PIR | Passive InfraRed |
| PNN | Probabilistic Neural Network |
| PV | Photovoltaic |
| RBFNN | Radial Basis Function Neural Network |
| RF | Random Forest |
| RFC | Random Forest Classifier |
| RFR | Random Forest Regression |
| RL | Reinforcement Learning |
| RNN | Recurrent Neural Network |
| SaaS | Software as a Service |
| SAFT | Synthetic Aperture Focusing Technique |
| SDG | Sustainable Development Goal |
| SHM | Structural Health Monitoring |
| SoH | State of Health |
| SVM | Support Vector Machine |
| TFM | Total Focusing Method |
| TL | Transfer Learning |
| UAV | Unmanned Aerial Vehicle |
| UT | Ultrasonic Testing |
| VR | Virtual Reality |
| WANs | Wide Area Networks |
| WSN | Wireless Sensor Network |
| YOLO | You Only Look Once |

## References

1. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report EBSE-2007-01; EBSE: Delhi, India, 2007. Available online: https://www.researchgate.net/publication/302924724_Guidlines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering (accessed on 25 June 2025).
2. Paolone, G.; Iachetti, D.; Paesani, R.; Pilotti, F.; Marinelli, M.; Di Felice, P. A Holistic Overview of the Internet of Things Ecosystem. *IoT* **2022**, *3*, 398–434. [CrossRef]
3. Sung, T.W.; Tsai, P.W.; Gaber, T.; Lee, C.Y. Artificial intelligence of things (AIoT) technologies and applications. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9781271. [CrossRef]
4. Singh, R.; Gill, S.S. Edge AI: A survey. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 71–92. [CrossRef]
5. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An overview on edge computing research. *IEEE Access* **2020**, *8*, 85714–85728. [CrossRef]
6. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87. [CrossRef]
7. Luo, X.; Wang, A.; Zhang, X.; Huang, K.; Wang, S.; Chen, L.; Cui, Y. Toward intelligent AIoT: A comprehensive survey on digital twin and multimodal generative AI integration. *Mathematics* **2025**, *13*, 3382. [CrossRef]
8. Zhang, J.; Tao, D. Empowering things with intelligence: A survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet Things J.* **2020**, *8*, 7789–7817. [CrossRef]
9. Sheikh, A.M.; Islam, M.R.; Habaebi, M.H.; Zabidi, S.A.; Bin Najeeb, A.R.; Kabbani, A. A survey on edge computing (EC) security challenges: Classification, threats, and mitigation strategies. *Future Internet* **2025**, *17*, 175. [CrossRef]
10. Wang, X.; Wan, Z.; Hekmati, A.; Zong, M.; Alam, S.; Zhang, M.; Krishnamachari, B. The internet of things in the era of generative AI: Vision and challenges. *IEEE Internet Comput.* **2024**, *28*, 57–64. [CrossRef]
11. Jiang, W.; Zhang, Y.; Han, H.; Mu, J. Generative AI for consumer internet of things: Challenges and opportunities. *IEEE Consum. Electron. Mag.* **2025**, *14*, 40–50. [CrossRef]
12. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2462–2488. [CrossRef]

13. Agrawal, A.V.; Gowridurga, A.; Shaikh, A.A.; Kalaipriya, V. Fog Computing in IoT: Architecture and Applications. In Proceedings of the 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 4–5 April 2024; pp. 1–6. [CrossRef]
14. Chuan, W.C.; Laghari, S.U.A.; Manickam, S.; Ashraf, E.; Karuppayah, S. Challenges and opportunities in fog computing scheduling: A literature review. *IEEE Access* **2025**, *13*, 14702–14726. [CrossRef]
15. Dritsas, E.; Trigka, M. Exploring the Intersection of Machine Learning and Big Data: A Survey. *Mach. Learn. Knowl. Extr.* **2025**, *7*, 13. [CrossRef]
16. Trigka, M.; Dritsas, E. A Comprehensive Survey of Machine Learning Techniques and Models for Object Detection. *Sensors* **2025**, *25*, 214. [CrossRef]
17. Hall, T.; Rasheed, K. A Survey of Machine Learning Methods for Time Series Prediction. *Appl. Sci.* **2025**, *15*, 5957. [CrossRef]
18. Guidotti, D.; Pandolfo, L.; Pulina, L. A systematic literature review of supervised machine learning techniques for predictive maintenance in Industry 4.0. *IEEE Access* **2025**, *13*, 102479–102504. [CrossRef]
19. Wei, L.; Solihin, M.I.; Saruchi, S.A.; Astuti, W.; Hong, L.W.; Kit, A.C. Surface defects detection of cylindrical high-precision industrial parts based on deep learning algorithms: A review. *Oper. Res. Forum* **2024**, *5*, 58. [CrossRef]
20. Saleem, F.; Umar, M.; Kim, J.M. An Optimized Few-Shot Learning Framework for Fault Diagnosis in Milling Machines. *Machines* **2025**, *13*, 1010. [CrossRef]
21. Hoang, D.C.; Tan, P.X.; Nguyen, A.N.; Pham, M.K.; Duong, T.H.A.; Huynh, T.M.; Bui, S.A.; Nguyen, D.M.; Ha, Q.H.; Trinh, V.A.; et al. Unsupervised industrial anomaly detection using paired well-lit and low-light images. *J. Comput. Des. Eng.* **2025**, *12*, 41–61. [CrossRef]
22. Hoang, M.T.; Nguyen, N.V.; Pham, T.A.; Nguyen, T.T.; Dang, T.M.; Nguyen, H.N. Evaluating Dimensionality Reduction Methods for the Detection of Industrial IoT Attacks in Edge Computing. *Int. J. Comput. Commun. Control* **2024**, *19*, 6767. [CrossRef]
23. Gummadi, A.N.; Napier, J.C.; Abdallah, M. XAI-IoT: An explainable AI framework for enhancing anomaly detection in IoT systems. *IEEE Access* **2024**, *12*, 71024–71054. [CrossRef]
24. Han, K.; Wang, Y.; Chen, H.; Chen, X.; Guo, J.; Liu, Z.; Tang, Y.; Xiao, A.; Xu, C.; Xu, Z.; et al. A survey on vision transformer. *IEEE Trans. Pattern Anal. Mach. Intell.* **2023**, *45*, 87–110. [CrossRef]
25. Kong, X.; Chen, Z.; Liu, W.; Ning, K.; Zhang, L.; Muhammad Marier, S.; Liu, Y.; Chen, Y.; Xia, F. Deep learning for time series forecasting: A survey. *Int. J. Mach. Learn. Cybern.* **2025**, *16*, 5079–5112. [CrossRef]
26. Chen, J.; Ran, X. Deep learning with edge computing: A review. *Proc. IEEE* **2019**, *107*, 1655–1674. [CrossRef]
27. Mienye, I.D.; Sun, Y. A survey of ensemble learning: Concepts, algorithms, applications, and prospects. *IEEE Access* **2022**, *10*, 99129–99149. [CrossRef]
28. Alkadi, S.; Al-Ahmadi, S.; Ben Ismail, M.M. RobEns: Robust ensemble adversarial machine learning framework for securing IoT traffic. *Sensors* **2024**, *24*, 2626. [CrossRef]
29. Zhu, K.; Zhang, T. Deep reinforcement learning based mobile robot navigation: A review. *Tsinghua Sci. Technol.* **2021**, *26*, 674–691. [CrossRef]
30. Xia, K.; Sacco, C.; Kirkpatrick, M.; Saidy, C.; Nguyen, L.; Kircaliali, A.; Harik, R. A digital twin to train deep reinforcement learning agent for smart manufacturing plants: Environment, interfaces and intelligence. *J. Manuf. Syst.* **2021**, *58*, 210–230. [CrossRef]
31. Buckman, A.H.; Mayfield, M.; Beck, S.B. What is a smart building? Smart Sustain. *Built Environ.* **2014**, *3*, 92–109. [CrossRef]
32. Omar, O. Intelligent building, definitions, factors and evaluation criteria of selection. *Alex. Eng. J.* **2018**, *57*, 2903–2910. [CrossRef]
33. Froufe, M.M.; Chinelli, C.K.; Guedes, A.L.A.; Haddad, A.N.; Hammad, A.W.; Soares, C.A.P. Smart buildings: Systems and drivers. *Buildings* **2020**, *10*, 153. [CrossRef]
34. Bayasgalan, A.; Park, Y.S.; Koh, S.B.; Son, S.Y. Comprehensive review of building energy management models: Grid-interactive efficient building perspective. *Energies* **2024**, *17*, 4794. [CrossRef]
35. Taboada-Orozco, A.; Yetongnon, K.; Nicolle, C. Smart buildings: A comprehensive systematic literature review on data-driven building management systems. *Sensors* **2024**, *24*, 4405. [CrossRef] [PubMed]
36. Luan, B.; Feng, X. Artificial intelligence in Smart Buildings: A bibliometrics-based visualization analysis. *J. Asian Archit. Build. Eng.* **2025**, 1–25. [CrossRef]
37. Emedo, C.; Wada, O.Z.; David-Olawade, A.C.; Ling, J.; Esan, D.T.; Ijiwade, J.; Olawade, D.B. AI-driven transformations in smart buildings: A review of energy efficiency and sustainable operations. *Dig. Eng.* **2025**, *7*, 100068. [CrossRef]
38. Lavrinovica, I.; Judvaitis, J.; Laksis, D.; Skromule, M.; Ozols, K. A Comprehensive Review of Sensor-Based Smart Building Monitoring and Data Gathering Techniques. *Appl. Sci.* **2024**, *14*, 10057. [CrossRef]
39. Saad Al-Sumaiti, A.; Ahmed, M.H.; Salama, M.M. Smart home activities: A literature review. *Electr. Power Compon. Syst.* **2014**, *42*, 294–305. [CrossRef]
40. Sarhan, Q.I. Systematic survey on smart home safety and security systems using the Arduino platform. *IEEE Access* **2020**, *8*, 128362–128384. [CrossRef]

41. Robles, R.J.; Kim, T.H.; Cook, D.; Das, S. A review on security in smart home development. *Int. J. Adv. Sci. Technol.* **2010**, *15*, 7–22.
42. Surantha, N.; Wicaksono, W.R. Design of smart home security system using object recognition and PIR sensor. *Procedia Comput. Sci.* **2018**, *135*, 465–472. [CrossRef]
43. Wang, J.; Yang, F.; Chen, T.; Shah, S.L. An overview of industrial alarm systems: Main causes for alarm overloading, research status, and open problems. *IEEE Trans. Autom. Sci. Eng.* **2015**, *13*, 1045–1061. [CrossRef]
44. Desima, M.A.; Ramli, P.; Ramdani, D.F.; Rahman, S. Alarm system to detect the location of IOT-based public vehicle accidents. In Proceedings of the 2017 International Conference on Computing, Engineering, and Design (ICCED), Kuala Lumpur, Malaysia, 23–25 November 2017; pp. 1–5. [CrossRef]
45. Silva, F.; Santos, G.; Praça, I.; Vale, Z. A context-based building security alarm through power and sensors analysis. *Energy Inform.* **2018**, *1*, 41. [CrossRef]
46. Mohapatra, B.N.; Taware, S.S.; Parab, P.P. Smart Security Alarm System using PIR Sensor. *Perspect. Commun. Embed. Syst. Signal-Process.—PiCES* **2021**, *5*, 90–92. [CrossRef]
47. Jain, A.; Basantwani, S.; Kazi, O.; Bang, Y. Smart surveillance monitoring system. In Proceedings of the 2017 International Conference on Data Management, Analytics and Innovation (ICDMAI), Pune, India, 24–26 February 2017; pp. 269–273. [CrossRef]
48. Ullah, A.W.U.; Shah, J.A.; Kadir, K.; Wahid, A. Development of smart surveillance system using cloud for security application. In Proceedings of the 2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Glasgow, UK, 17–20 May 2021; pp. 1–6. [CrossRef]
49. Taiwo, O.; Ezugwu, A.E.; Oyelade, O.N.; Almutairi, M.S. Enhanced intelligent smart home control and security system based on deep learning model. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9307961. [CrossRef]
50. Gayathri, P.; Stalin, A.; Anand, S. Intelligent Smart Home Security System: A Deep Learning Approach. In Proceedings of the 2022 IEEE 10th Region 10 Humanitarian Technology Conference (R10-HTC), Hyderabad, India, 16–18 September 2022; pp. 438–444. [CrossRef]
51. Bouwmans, T.; Porikli, F.; Höferlin, B.; Vacavant, A. *Background Modeling and Foreground Detection for Video Surveillance*; Routledge: New York, NY, USA, 2014.
52. Ullo, S.L.; Sinha, G.R. Advances in smart environment monitoring systems using IoT and sensors. *Sensors* **2020**, *20*, 3113. [CrossRef] [PubMed]
53. Saini, J.; Dutta, M.; Marques, G. Indoor air quality monitoring systems based on internet of things: A systematic review. *Int. J. Environ. Res. Public Health* **2020**, *17*, 4942. [CrossRef]
54. Bindra, L.; Lin, C.; Stroulia, E.; Ardakanian, O. Decentralized access control for smart buildings using metadata and smart contracts. In Proceedings of the 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Montreal, QC, Canada, 28 May 2019; pp. 32–38. [CrossRef]
55. Pal, S.; Jadidi, Z. Protocol-based and hybrid access control for the IoT: Approaches and research opportunities. *Sensors* **2021**, *21*, 6832. [CrossRef]
56. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access control for IoT: A survey of existing research, dynamic policies and future directions. *Sensors* **2023**, *23*, 1805. [CrossRef]
57. Xue, N.; Liang, L.; Zhang, J.; Huang, X. An access control system for intelligent buildings. In Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications (MOBIMEDIA), Xi'an, China, 18–20 June 2016; pp. 11–17. [CrossRef]
58. Brignardello-Petersen, R.; Santesso, N.; Guyatt, G.H. Systematic reviews of the literature: An introduction to current methods. *Am. J. Epidemiol.* **2025**, *194*, 536–542. [CrossRef] [PubMed]
59. Kliestik, T.; Dragomir, R.; Băluță, A.V.; Grecu, I.; Durana, P.; Karabolevski, O.L.; Kral, P.; Balica, R.; Suler, P.; Bușu, O.V.; et al. Enterprise generative artificial intelligence technologies, Internet of Things and blockchain-based fintech management, and digital twin industrial metaverse in the cognitive algorithmic economy. *Oecon. Copernic.* **2024**, *15*, 1183–1221. [CrossRef]
60. Hosain, M.N.; Kwak, Y.S.; Lee, J.; Choi, H.; Park, J.; Kim, J. IoT-enabled biosensors for real-time monitoring and early detection of chronic diseases. *Phys. Act. Nutr.* **2024**, *28*, 60–68. [CrossRef]
61. Abdoli, F.; Rashidi, M.; Wang, J.; Siddique, R.; Nasir, V. Structural health monitoring of timber bridges—A review. *Results Eng.* **2024**, *24*, 103084. [CrossRef]
62. Salhout, S.M. Machine learning in healthcare strategic management: A systematic literature review. *Arab Gulf J. Sci. Res.* **2024**, *42*, 1530–1554. [CrossRef]
63. Li, Q.; Ma, H.; Min, W.; Wang, Y.; Zhao, R.; Zhou, Y.; Than, Y.; Luo, Y.; Hong, H. Recent advances in fish cutting: From cutting schemes to automatic technologies and internet of things innovations. *Compr. Rev. Food Sci. Food Saf.* **2024**, *23*, e70039. [CrossRef] [PubMed]
64. Verma, S.; Kameswari, Y.L.; Kumar, S. A review on environmental parameters monitoring systems for power generation estimation from renewable energy systems. *BioNanoScience* **2024**, *14*, 3864–3888. [CrossRef]

65. Kasiviswanathan, S.; Gnanasekaran, S.; Thangamuthu, M.; Rakkiyannan, J. Machine-learning-and internet-of-things-driven techniques for monitoring tool wear in machining process: A comprehensive review. *J. Sens. Actuator Netw.* **2024**, *13*, 53. [CrossRef]
66. Lăzăroiu, G.; Gedeon, T.; Valaskova, K.; Vrbka, J.; Šuleř, P.; Zvarikova, K.; Kramarova, K.; Rowland, Z.; Stehel, V.; Gajanova, L.; et al. Cognitive digital twin-based Internet of Robotic Things, multi-sensory extended reality and simulation modeling technologies, and generative artificial intelligence and cyber–physical manufacturing systems in the immersive industrial metaverse. *Equilib. Q. J. Econ. Econ. Policy* **2024**, *19*, 719–748. [CrossRef]
67. Nindhita, K.W.; Zaki, A.; Nugroho, G. Mapping Publications of Cracks Monitoring in Concrete Structures: Bibliometric and Scientometric Review in 2013–2023. *Ann. Chim. Sci. Mater.* **2024**, *48*, 467–479. [CrossRef]
68. Alam, M.J.B.; Manzano, L.S.; Debnath, R.; Ahmed, A.A. Monitoring slope movement and soil hydrologic behavior using IoT and AI technologies: A systematic review. *Hydrology* **2024**, *11*, 111. [CrossRef]
69. Mahmood, M.S.; Shareef, I.R. Applications of Artificial Intelligence for Smart Conveyor Belt Monitoring Systems: A Comprehensive Review. *J. Eur. Syst. Autom.* **2024**, *57*, 1195–1206. [CrossRef]
70. Çiçek, S.; Yilmaz, M.T.; Hadnađev, T.D.; Tadesse, E.E.; Kulawik, P.; Ozogul, F. Definition, detection, and tracking of nanowaste in foods: Challenges and perspectives. *Compr. Rev. Food Sci. Food Saf.* **2024**, *23*, e13393. [CrossRef] [PubMed]
71. Mane, P.K.; Rao, K.N. Novel Framework for Multi-Scale Occupancy Sensing for Distributed Monitoring in Internet-of-Things. *Wirel. Pers. Commun.* **2024**, *136*, 601–616. [CrossRef]
72. Jayousi, S.; Barchielli, C.; Alaimo, M.; Caputo, S.; Paffetti, M.; Zoppi, P.; Mucchi, L. ICT in nursing and patient healthcare management: Scoping review and case studies. *Sensors* **2024**, *24*, 3129. [CrossRef]
73. Adil, M.; Song, H.; Mastorakis, S.; Abulkasim, H.; Farouk, A.; Jin, Z. UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions. *IEEE Trans. Intell. Veh.* **2024**, *9*, 4583–4605. [CrossRef]
74. Alrubayyi, H.; Alshareef, M.S.; Nadeem, Z.; Abdelmoniem, A.M.; Jaber, M. Security threats and promising solutions arising from the intersection of AI and IoT: A study of IoMT and IoET applications. *Future Internet* **2024**, *16*, 85. [CrossRef]
75. He, D.; Ding, K.; Chan, S.; Guizani, M. Unknown threats detection methods of smart contracts. *IEEE Internet Things J.* **2024**, *11*, 4430–4441. [CrossRef]
76. Khalid, W.; Rehman, M.A.U.; Van Chien, T.; Kaleem, Z.; Lee, H.; Yu, H. Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances. *IEEE Internet Things J.* **2024**, *11*, 3599–3613. [CrossRef]
77. Yauri, R.; Castro, A.; Espino, R. Automatic Leaf Health Monitoring with an IoT Camera System based on Computer Vision and Segmentation for Disease Detection. *WSEAS Trans. Electron.* **2024**, *15*, 148–156. [CrossRef]
78. Soltanmohammadlou, N.; Hon, C.K.; Drogemuller, R.; Sheikhkhoshkar, M.; Rahimian, F. An advanced exploration of technological functionalities addressing risk factors in earthmoving equipment operation on construction sites: A systematic literature review. *Smart Sustain. Built Environ.* **2026**, *15*, 1846–1876. [CrossRef]
79. Zou, Y.; Chu, Z.; Yang, T.; Guo, J.; Li, D. Research progress and prospects of intelligent diabetes monitoring systems: A review. *IEEE Sens. J.* **2024**, *24*, 23401–23435. [CrossRef]
80. Çelik, Y.S.; İlçe, E.; Mesut, B.; Özsoy, Y. An overview of wearable medical device applications. *J. Res. Pharm.* **2024**, *28*, 722–732. [CrossRef]
81. Govardanan, C.S.; Murugan, R.; Yenduri, G.; Gurrammagari, D.R.; Bhulakshmi, D.; Kandati, D.R.; Supriya, Y.; Gadekallu, T.R.; Rathore, S.R.; Jhaveri, R.H. The amalgamation of federated learning and explainable artificial intelligence for the internet of medical things: A review. *Recent Adv. Comput. Sci. Commun.* **2024**, *17*, 1–19. [CrossRef]
82. Sundas, A.; Badotra, S.; Shahi, G.S.; Verma, A.; Bharany, S.; Ibrahim, A.O.; Abulfaraj, A.W.; Binzagr, F. Smart patient monitoring and recommendation (Sp. PMR) using cloud analytics and deep learning. *IEEE Access* **2024**, *12*, 54238–54255. [CrossRef]
83. Zongxiang, Z.; Daqing, Z.; Chenghong, Z.; Lihua, H.; Gang, C.; Weiru, H. Literature review on federated learning application: Based on "element-process" framework. *J. Ind. Eng. Eng. Manag.* **2024**, *38*, 14–30. [CrossRef]
84. Khazane, H.; Ridouani, M.; Salahdine, F.; Kaabouch, N. A holistic review of machine learning adversarial attacks in IoT networks. *Future Internet* **2024**, *16*, 32. [CrossRef]
85. Alprol, A.E.; Mansour, A.T.; Ibrahim, M.E.E.D.; Ashour, M. Artificial intelligence technologies revolutionizing wastewater treatment: Current trends and future prospective. *Water* **2024**, *16*, 314. [CrossRef]
86. Ghadi, Y.Y.; Mazhar, T.; Al Shloul, T.; Shahzad, T.; Salaria, U.A.; Ahmed, A.; Hamam, H. Machine learning solutions for the security of wireless sensor networks: A review. *IEEE Access* **2024**, *12*, 12699–12719. [CrossRef]
87. Maurya, M.; Panigrahi, I.; Dash, D.; Malla, C. Intelligent fault diagnostic system for rotating machinery based on IoT with cloud computing and artificial intelligence techniques: A review. *Soft Comput.* **2024**, *28*, 477–494. [CrossRef]
88. Afraji, D.M.A.A.; Lloret, J.; Peñalver, L. Deep learning-driven defense strategies for mitigating DDoS attacks in cloud computing environments. *Cyber Secur. Appl.* **2025**, *3*, 100085. [CrossRef]

89. Hoffmann, T.G.; de Souza, C.K.; Sonawane, A.D.; Praeger, U.; Büchele, F.; Neuwald, D.A.; Jedermann, R.; Linke, M.; Sturm, B.; Mahajan, P.V. Challenges and future perspectives in postharvest cold storage: Technological review on sustainable and efficient cold storage of fresh produce. *Food Res. Int.* **2025**, *221*, 117406. [CrossRef]
90. Bombiński, S.; Kossakowska-Skajster, J.; Jemielniak, K. New developments and future prospects in commercial tool condition monitoring systems. *Measurement* **2025**, *255*, 118037. [CrossRef]
91. Rahman, Z.U.; Asaari, M.S.M.; Ibrahim, H. Advancing animal farming with deep learning: A systematic review. *Comput. Electron. Agric.* **2025**, *237*, 110674. [CrossRef]
92. Mohan, A.; Manitha, P.V.; Subramaniam, U. A comprehensive review on the integration of air quality monitoring systems with hybrid electric vehicles for emission control in smart cities. *Sci. Total Environ.* **2025**, *994*, 180022. [CrossRef]
93. Kolawole, F.O.; Kolawole, I.D.; Sanni-manuel, B.A.; Kolawole, G.O.; Bello, S.A.; Kolade, O.S.; Oni, K.; Kolawole, S.K.; Kolawole, V.A. Organic fertilizers synthesized from domestic food waste: A green sustainable approach—A review. *Bioresour. Technol. Rep.* **2025**, *31*, 102231. [CrossRef]
94. Semercioz-Oduncuoglu, A.S.; Luning, P.A. Industry 4.0 technologies in quality and safety control systems in food manufacturing: A systematic techno-managerial analysis on benefits and barriers. *Trends Food Sci. Technol.* **2025**, *163*, 105144. [CrossRef]
95. Eren, H.; Karaduman, Ö.; Gençoğlu, M.T. Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Appl. Sci.* **2025**, *15*, 8704. [CrossRef]
96. Prasath, B.; Akila, M.; Mohan, M. A Comprehensive Survey on IoT-Aided Pest Detection and Classification in Agriculture Using Different Image Processing Techniques. *Int. J. Image Graph.* **2025**, *25*, 2550040. [CrossRef]
97. Ali, M.; Ahmad, I.; Geun, I.; Hamza, S.A.; Ijaz, U.; Jang, Y.; Koo, J.; Kim, Y.G.; Kim, H.D. A Comprehensive Review of Advanced Sensor Technologies for Fire Detection with a Focus on Gasistor-Based Sensors. *Chemosensors* **2025**, *13*, 230. [CrossRef]
98. Kypraiou, C.; Varzakas, T. Evolution and Evaluation of Ultra-Low Temperature Freezers: A Comprehensive Literature Review. *Foods* **2025**, *14*, 2298. [CrossRef]
99. Dębowski, M.; Kazimierowicz, J.; Zieliński, M. Multi-Sensing Monitoring of the Microalgae Biomass Cultivation Systems for Biofuels and Added Value Products Synthesis—Challenges and Opportunities. *Appl. Sci.* **2025**, *15*, 7324. [CrossRef]
100. Sardar, R.; Anees, T.; Al-Shamayleh, A.S.; Mehmood, E.; Khalil, W.; Akhunzada, A.; Shaikh, F.S. Challenges in detecting security threats in WoT: A systematic literature review. *Artif. Intell. Rev.* **2025**, *58*, 196. [CrossRef]
101. Gupta, A.; Misra, D.D.C. A Systematic Review on Enhancing IoT Security with Deep Learning and Big Data Analytics. *J. Theor. Appl. Inf. Technol.* **2025**, *103*, 4565–4587.
102. Nugroho, H.Y.S.H.; Basuki, T.M.; Savitri, E.; Supangat, A.B.; Putra, P.B.; Wahyuningrum, N.; Adi, R.N.; Setiawan, O.; Nandini, R.; Cahyono, S.A.; et al. Advancing air quality monitoring systems towards sustainable green development: Insight for metropolitan cities in Indonesia. *Environ. Sustain. Indic.* **2025**, *26*, 100649. [CrossRef]
103. da Costa Filho, P.E.; Marques, L.A.D.A.; Lima, I.D.S.F.D.; Sousa, E.L.D.; Kreutz, M.E.; Neto, A.V.; Cunha, E.N.; Vieira, D. Machine-Learning-Based Classification of Electronic Devices Using an IoT Smart Meter. *Informatics* **2025**, *12*, 48. [CrossRef]
104. Le Roux, R.; Sepehri, M.; Khaksar, S.; Murray, I. Slope Stability Monitoring Methods and Technologies for Open-Pit Mining: A Systematic Review. *Mining* **2025**, *5*, 32. [CrossRef]
105. Gotte, M.; Rama Sreekanth, P.S. Integrating artificial intelligence with piezoelectric nanogenerators: A review on advancements in smart energy harvesting technologies. *J. Mater. Sci.* **2025**, *60*, 8253–8284. [CrossRef]
106. Jusoh, M.F.; Abd Kharim, M.N.; Kayat, F.; Abu, T.H.S.A.T.; Idris, A.A.; Muttalib, M.F.A.; Abdullah, F.A.; Löytty, T. Discovering Research Landscape and Emerging Trends of Compost Implementation with the Internet of Things via Bibliometric Analysis. *J. Adv. Res. Des.* **2025**, *128*, 100–115. [CrossRef]
107. Ngwenya, B.; Paepae, T.; Bokoro, P.N. Monitoring ambient water quality using machine learning and IoT: A review and recommendations for advancing SDG indicator 6.3.2. *J. Water Process Eng.* **2025**, *73*, 107664. [CrossRef]
108. Chen, W.; Hou, J.; Hao, S.; Zhu, Y.; Yu, M. Mapping knowledge structure and themes trends of corrosion detection of steel: A bibliometric analysis. *Comput. Mater. Sci.* **2025**, *253*, 113889. [CrossRef]
109. Su, S.; Ma, K.; Zhou, T.; Yao, Y.; Xin, H. Advancing methodologies for assessing the impact of land use changes on water quality: A comprehensive review and recommendations. *Environ. Geochem. Health* **2025**, *47*, 101. [CrossRef]
110. Soegoto, E.S.; Rafdhi, A.A.; Abduh, A.; Rosmaladewi, R.; Haristiani, N. Emerging applications of iot, machine learning, virtual reality, augmented reality and artificial intelligent in monitoring systems: A comprehensive review and analysis. *J. Eng. Sci. Technol.* **2025**, *20*, 404–426.
111. Singh, A.; Yasheshwar; Kaushik, N.K.; Kala, D.; Nagraik, R.; Gupta, S.; Kaushal, A.; Walia, Y.; Dhir, S.; Noorani, M.S. Conventional and cutting-edge advances in plant virus detection: Emerging trends and techniques. *3 Biotech* **2025**, *15*, 100. [CrossRef] [PubMed]
112. Waseem, M.; Lakshmi, G.S.; Amir, M.; Ahmad, M.; Suhaib, M. Advancement in battery health monitoring methods for electric vehicles: Battery modelling, state estimation, and internet-of-things based methods. *J. Power Sources* **2025**, *633*, 236414. [CrossRef]

113. Rashid, M.R.A.; Al Rafi, A.; Islam, M.A.; Sharkar, S.U.; Rafi, Z.H.; Hasan, M.; Ali, M.S.; Khan, M.S.H. Enhancing land management policy in Bangladesh: A blockchain-based framework for transparent and efficient land management. *Land Use Policy* **2025**, *150*, 107436. [CrossRef]
114. Bukhari, S.A.S.; Shafi, I.; Ahmad, J.; Villar, S.G.; Villena, E.G.; Khurshaid, T.; Ashraf, I. Review of flood monitoring and prevention approaches: A data analytic perspective. *Nat. Hazards* **2025**, *121*, 5103–5128. [CrossRef]
115. Singh, R.; Nickhil, C.; Nisha, R.; Upendar, K.; Jithender, B.; Deka, S.C. A Comprehensive Review of Advanced Deep Learning Approaches for Food Freshness Detection. *Food Eng. Rev.* **2025**, *17*, 127–160. [CrossRef]
116. Miller, T.; Durlik, I.; Kostecka, E.; Kozlovska, P.; Łobodzińska, A.; Sokołowska, S.; Nowy, A. Integrating Artificial Intelligence Agents with the Internet of Things for Enhanced Environmental Monitoring: Applications in Water Quality and Climate Data. *Electronics* **2025**, *14*, 696. [CrossRef]
117. Kotama, I.N.D.; Funabiki, N.; Panduman, Y.Y.F.; Brata, K.C.; Pradhana, A.A.S.; Noprianto; Desnanjaya, I.G.M.N. Implementation of Sensor Input Setup Assistance Service Using Generative AI for SEMAR IoT Application Server Platform. *Information* **2025**, *16*, 108. [CrossRef]
118. Sylvestrin, G.R.; Maciel, J.N.; Amorim, M.L.M.; Carmo, J.P.; Afonso, J.A.; Lopes, S.F.; Ando Junior, O.H. State of the Art in Electric Batteries' State-of-Health (SoH) Estimation with Machine Learning: A Review. *Energies* **2025**, *18*, 746. [CrossRef]
119. Bignami, E.G.; Panizzi, M.; Bezzi, F.; Mion, M.; Bagnoli, M.; Bellini, V. Wearable devices as part of postoperative early warning score systems: A scoping review. *J. Clin. Monit. Comput.* **2025**, *39*, 233–244. [CrossRef]
120. Liu, Y.; Wang, B. Advanced applications in chronic disease monitoring using IoT mobile sensing device data, machine learning algorithms and frame theory: A systematic review. *Front. Public Health* **2025**, *13*, 1510456. [CrossRef]
121. Li, L. A Comprehensive Survey of Fire Weather Index (FWI) Systems and IoT Applications in Peatland Fire Management. *IEEE Access* **2025**, *13*, 33579–33598. [CrossRef]
122. Visconti, P.; Rausa, G.; Del-Valle-Soto, C.; Velázquez, R.; Cafagna, D.; De Fazio, R. Innovative Driver Monitoring Systems and On-Board-Vehicle Devices in a Smart-Road Scenario Based on the Internet of Vehicle Paradigm: A Literature and Commercial Solutions Overview. *Sensors* **2025**, *25*, 562. [CrossRef]
123. Selvam, A.P.; Al-Humairi, S.N.S. Environmental impact evaluation using smart real-time weather monitoring systems: A systematic review. *Innov. Infrastruct. Solut.* **2025**, *10*, 13. [CrossRef]
124. Khoshafa, M.H.; Maraqa, O.; Moualeu, J.M.; Aboagye, S.; Ngatched, T.M.N.; Ahmed, M.H.; Gadallah, Y.; Di Renzo, M. RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communication Systems: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 2156–2203. [CrossRef]
125. Shamroukh, M.; Natapov, A.; Larimian, T. Reliability and Scalability of Pedestrian Monitoring Practices: A Systematic Review. *IEEE Access* **2025**, *13*, 147679–147688. [CrossRef]
126. Mithal, A.; Thankachan, B. A Comprehensive Review on Blockchain-based Systems for Groundwater Conservation and Wastewater Management. *Environ. Manag.* **2025**, *75*, 2225–2243. [CrossRef]
127. Modak, M.; Pritom, M.M.; Banik, S.C.; Rabbi, M.S. Internet of Things-Based Health Surveillance Systems for Livestock: A Review of Recent Advances and Challenges. *IET Wirel. Sens. Syst.* **2025**, *15*, e7f0013. [CrossRef]
128. Aryffin, H.A.K.; Sahbudin, M.A.B.; Pitchay, S.A.; Abhalim, A.H.; Sahbudin, I. Technological trends in epidemic intelligence for infectious disease surveillance: A systematic literature review. *PeerJ Comput. Sci.* **2025**, *11*, e2874. [CrossRef] [PubMed]
129. Lakshmipriya, T.; Gopinath, S.C. Internet of Medical Things (IoMT) for Alzheimer Patient's Outcome. *CNS Neurol. Disord. Drug Targets* **2025**, *24*, 491–493. [CrossRef] [PubMed]
130. Alaoui, M.L.T.; Belhiah, M.; Ziti, S. IoT-Enabled Waste Management in Smart Cities: A Systematic Literature Review. *Int. J. Adv. Comput. Sci. Appl.* **2025**, *16*, 131–138. [CrossRef]
131. Lai, C.Y.; Lo, Y.W.; Chow, C.F.; Chan, C.C.; Mung, S.W. Smart Food Area–Weight System for Dietary and Nutritional Monitoring. *IEEE Sens. J.* **2025**, *25*, 44522–44534. [CrossRef]
132. Ma, L.; Li, Z.; Yang, S.; Wang, J. A Review on Vibration Sensor: Key Parameters, Fundamental Principles, and Recent Progress on Industrial Monitoring Applications. *Vibration* **2025**, *8*, 56. [CrossRef]
133. Alterkawi, L.; Dib, F.K. Federated Learning for Smart Cities: A Thematic Review of Challenges and Approaches. *Future Internet* **2025**, *17*, 545. [CrossRef]
134. Aldehim, G.; Shahzad, T.; Khan, M.A.; Ghadi, Y.Y.; Jiang, W.; Mazhar, T.; Hamam, H. Balancing sustainability and security: A review of 5G and IoT in smart cities. *Digit. Commun. Netw.* **2025**, *11*, 1722–1737. [CrossRef]
135. da Silva, A.H.M.C.; da Silva, M.K.; Santos, A.; Gómez-Malagón, L.A. A Systematic Review for Ammonia Monitoring Systems Based on the Internet of Things. *Internet Things* **2025**, *6*, 66. [CrossRef]
136. Bakhronova, D.; Saipova, M.; Tursunov, D.; Jaynaqov, M.; Khurramova, R.; Nurmukhamedova, D.; Yuldashova, N.; Berdiev, K. Security and Privacy Frameworks for Mobile Internet Services in Ubiquitous Computing Environments for Smart Classrooms in Educational Institutions. *J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl.* **2025**, *16*, 674–688. [CrossRef]

137. Essien, D.; Neethirajan, S. Multimodal AI systems for enhanced laying hen welfare assessment and productivity optimization. *Smart Agric. Technol.* **2025**, *12*, 101564. [CrossRef]
138. De, S.; Jalajamony, H.M.; Adhinarayanan, S.; Joshi, S.; Upadhyay, H.; Fernandez, R. Multimedia Transmission over LoRa Networks for IoT Applications: A Survey of Strategies, Deployments, and Open Challenges. *Sensors* **2025**, *25*, 7128. [CrossRef]
139. Hassan, S.R.; Hassan, A.; Maqsood, A.; Hijab, S. A survey on intelligent secure and distributed frameworks for Healthcare 5.0. *Discov. Artif. Intell.* **2025**, *5*, 286. [CrossRef]
140. Pandiselvam, R.; Rajbongshi, B.; Deepali, D.; Akoijam, T.; Nickhil, C.; Arputharaj, A.; Süfer, Ö. Advances in non-invasive techniques for enhancing cottonseed oil quality and shelf life: A sustainable approach. *J. Food Meas. Charact.* **2025**, *19*, 9354–9381. [CrossRef]
141. Yu, J.; Pu, H.; Sun, D.W. Intelligent non-invasive testing of food quality: Advancing accuracy and efficiency powered by artificial intelligence. *Trends Food Sci. Technol.* **2025**, *166*, 105357. [CrossRef]
142. Bereda, G. Emerging technologies and strategies for food contaminant detection and control: A global narrative review. *J. Food Compos. Anal.* **2025**, *148*, 108303. [CrossRef]
143. Ding, X.; Xu, Y.; Zheng, M.; Kang, W.; Xiahou, X. Digital Technology Integration in Risk Management of Human–Robot Collaboration Within Intelligent Construction—A Systematic Review and Future Research Directions. *Systems* **2025**, *13*, 974. [CrossRef]
144. Zvîncă, A.M.; Petruc, S.I.; Bogdan, R.; Marcu, M.; Popa, M. TreeHelper: A Wood Transport Authorization and Monitoring System. *Sensors* **2025**, *25*, 6713. [CrossRef]
145. Khan, M.U.S.; Battamo, A.Y.; Ravindar, R.; Salauddin, M. The Role of Artificial Intelligence in Bathing Water Quality Assessment: Trends, Challenges, and Opportunities. *Water* **2025**, *17*, 3176. [CrossRef]
146. Parween, G.; Al-Anbuky, A.; Mawston, G.; Lowe, A. Digital Twin Prospects in IoT-Based Human Movement Monitoring Model. *Sensors* **2025**, *25*, 6674. [CrossRef] [PubMed]
147. Manekar, K.; Kulkarni, M.B.; Hasamnis, M.A. Smart sensing for cholesterol quantification: Integrating AI, IoT, and emerging technologies. *Microchem. J.* **2025**, *218*, 115469. [CrossRef]
148. Letsoalo, E.; Mathonsi, T.; Tshilongamulenzhe, T.; du Duplesis, D. Systematic Literature Review of Reactive Jamming Attacks Mitigation Techniques in Internet of Things Networks. *Int. J. Adv. Comput. Sci. Appl.* **2025**, *16*, 1083–1090. [CrossRef]
149. Ikubanni, P.P.; Ejalonibu, D.; Abioye, O.M.; Alhassan, E.A.; Faloye, O.T.; Adeleke, A.A. Recent Advances of Artificial Intelligence in the Agricultural Sector: A Review. *NIPES J. Sci. Technol. Res.* **2025**, *7*, 219–226. [CrossRef]
150. Xie, A.; Wu, W. Emerging nanosensor technologies for the rapid detection of heavy metal contaminants in agricultural soils. *Anal. Methods* **2025**, *17*, 7846–7862. [CrossRef] [PubMed]
151. Nkwocha, C.L.; Chandel, A.K. Towards an End-to-End Digital Framework for Precision Crop Disease Diagnosis and Management Based on Emerging Sensing and Computing Technologies: State over Past Decade and Prospects. *Computers* **2025**, *14*, 443. [CrossRef]
152. Lim, K.S.; Ooi, S.Y.; Sayeed, M.S.; Chew, Y.J.; Ahmad, N.M. Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses. *Electronics* **2025**, *14*, 3972. [CrossRef]
153. Lima, M.; Viana, C.; Santos, W.R.; Neves, F.; Campos, J.R.; Aires, F. Toward using cyber threat intelligence with machine and deep learning for IoT security: A comprehensive study. *J. Supercomput.* **2025**, *81*, 1404. [CrossRef]
154. Chikatimalla, R.; Trivedi, Y.V.; Chigurupati, H.D.; Faheem, M.S.B.; Naveed, M.A.; Sattar, Y.; Rana, J.S.; Neppala, S. From prediction to precision: Artificial intelligence and emerging technologies in cardiopulmonary resuscitation. *Prog. Cardiovasc. Dis.* **2025**, *92*, 97–107. [CrossRef]
155. Barath, A.; Selvakumar, S.; Ravikumar, V.; Sivakumar, U.; Boomiraj, K. Integrating traditional and emerging technologies for enhanced water quality monitoring and sustainable resource management. *Plant Sci. Today* **2025**, *12*, 1–10. [CrossRef]
156. Amrita, C.M.; Balasubramanian, K. Precise aquaculture development: Overview of unmanned system technologies and its application to monitoring and management in aquaculture farms. *J. Environ. Prot. Ecol.* **2025**, *26*, 2501–2513.
157. Singh, R.P.; Gill, J. In-Field Crop Health Monitoring Using Intelligent Image Processing over Internet of Things Framework: A Comprehensive Review. *Int. J. Image Graph.* **2025**, 2750084. [CrossRef]
158. Ravisankar, T.; Prasanna, K.P.; Geetha, R.; Sairam, C.V.; Kumaran, M.; Muralidhar, M.; Ananda, R.R.; Kavibharathi, S.M.; Testimona, A.; Venkateswarlu, P.; et al. Transforming risk into resilience: A review of insurance strategies for sustainable shrimp aquaculture in India and beyond. *Front. Sustain. Food Syst.* **2025**, *9*, 1663329. [CrossRef]
159. Chen, J.; Yang, B.; Peng, C.; Yang, B.; Zhou, L.; Jiang, Z.; Liu, Z.; Liu, Y.; Tang, L. Recent advances of non-invasive sensors for smart wearable respiratory monitoring. *VIEW* **2025**, *7*, 20250162. [CrossRef]
160. Saeed, A.M.; Alagrash, Y.H.; Jeme, M.; Said, L. A systematic review of Healthcare Monitoring System: Methods, applications, and challenges. *J. Theor. Appl. Inf. Technol.* **2025**, *103*, 8764–8781.

161. Cai, L.; Li, Y.; Liu, Y.; Ma, G.; Zhang, Q.; Li, X.; Li, N. Endotracheal intubation-related oral mucosal membrane pressure injuries: A narrative review of biomechanical insights, biomaterial optimization, and intelligent monitoring. *Front. Med. Technol.* **2025**, *7*, 1667748. [CrossRef] [PubMed]
162. Yan, J.; Wu, H.; Diao, Z.; Miao, Y.; Zhang, B.; Zhao, C. Recent Developments and Applications of Crop Disease Detection, Prediction, and Early Warning: A review. *Engineering* **2025**. [CrossRef]
163. Gong, Z.; Cheng, Y.; Wei, X.; Zhang, Y.; Cheng, W.; Sun, T.; Liang, S.; Wang, X. Digital technologies in psoriasis management: From precision diagnosis to therapeutic innovation and holistic care. *Front. Digit. Health* **2025**, *7*, 1656585. [CrossRef] [PubMed]
164. Amoran, A.E.; Bismor, D. Review of Microphone-Based Contactless Vital Signs Monitoring Systems. *Arch. Acoust.* **2025**, *50*, 525–541. [CrossRef]
165. Soni, G.; Sharma, M.; Kumar, N. Free Space Optical Communication and its Implementation Using Diffractive Optical Elements Using Artificial Intelligence (AI). *Recent Pat. Eng.* **2025**, *19*, E230724232156. [CrossRef]
166. Pise, P.S.; Patil, R.N. A Review of Patient Health Care Monitoring System Based on Internet of Things. *J. Inst. Eng. India Ser. B* **2025**, *107*, 373–392. [CrossRef]
167. Krishnamoorthy, P.S.; Venugopal, P. Enhancing Public Transportation Through Advanced Technologies: A Comprehensive Review. *IEEE Access* **2025**, *13*, 185533–185557. [CrossRef]
168. Khan, I.U.; Khan, F.M.; Haider, Z.A.; Alturise, F. Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework. *Comput. Mater. Contin.* **2025**, *85*, 4307–4344. [CrossRef]
169. Al Khatib, I.; Awad, M.; Shamayleh, A. Navigating Pharma 4.0: Real-Time Monitoring and Traceability in the Middle East Pharmaceutical Industry—A Systematic Review. *Int. J. Serv. Sci. Manag. Eng. Technol.* **2025**, *16*, 35. [CrossRef]
170. Ibarra-Esparza, J.; Ibarra-Esparza, F.E.; González-López, M.E.; Garcia-Gonzalez, A.; Gradilla-Hernández, M.S. Instrumentation and Continuous Monitoring for the Anaerobic Digestion Process: A Systematic Review. *IEEE Access* **2025**, *13*, 193820–193837. [CrossRef]
171. Fiza, S.; Shafi, S.; Pradhan, R.; Riat, A.K. Recent advances in insect pest management strategies emphasizing on Artificial intelligence: A overview. *J. Appl. Nat. Sci.* **2025**, *17*, 1409–1419. [CrossRef]
172. Yasarathna, T.L.; Liyanage, M.; Le-Khac, N.A. Deep Learning-Based Autonomous Anomaly Detection for Security in SDN-IoT Networks. *IEEE Open J. Commun. Soc.* **2025**, *6*, 8007–8048. [CrossRef]
173. Zhang, F.; Cui, Y.; Yu, J.; Li, J.; Li, L.; Cui, G.; Li, Q.; Shi, K. Advances in Attack-Defense Game Models for IIoT: A Review. *IEEE Internet Things J.* **2025**, *12*, 46417–46430. [CrossRef]
174. Elghaish, F.; Mohandes, S.R.; Rahimian, F.; Abrishami, S.; Hosseini, M.R. Predictive digital monitoring of construction resources: An integrated digital twin solution. *Eng. Constr. Archit. Manag.* **2025**. [CrossRef]
175. Ametefe, D.S.; Sarnin, S.S.; Ali, D.M.; Muhamad, W.N.W.; Ametefe, G.D.; John, D.; Aliu, A.A. Enhancing Fingerprint Authentication: A Systematic Review of Liveness Detection Methods Against Presentation Attacks. *J. Inst. Eng. India Ser. B* **2024**, *105*, 1451–1467. [CrossRef]
176. Harbi, Y.; Medani, K.; Gherbi, C.; Aliouat, Z.; Harous, S. Roadmap of Adversarial Machine Learning in Internet of Things—Enabled Security Systems. *Sensors* **2024**, *24*, 5150. [CrossRef]
177. Nnabuife, S.G.; Udemu, C.; Hamzat, A.K.; Darko, C.K.; Quainoo, K.A. Smart monitoring and control systems for hydrogen fuel cells using AI. *Int. J. Hydrogen Energy* **2024**, *110*, 704–726. [CrossRef]
178. Kumi, L.; Jeong, J.; Jeong, J. State-of-the-Art review of blockchain applications for construction safety: Opportunities, challenges, and future directions. *Saf. Sci.* **2025**, *191*, 106966. [CrossRef]
179. Hernández-Torres, G.A.; Sánchez-DelaCruz, E. Challenges and opportunities of ambient intelligence (AmI) in the 21st century: A historical review. *Evol. Intell.* **2025**, *18*, 80. [CrossRef]
180. Ojo, K.E.; Saha, A.K.; Srivastava, V.M. Review of Advances in Renewable Energy-Based Microgrid Systems: Control Strategies, Emerging Trends, and Future Possibilities. *Energies* **2025**, *18*, 3704. [CrossRef]
181. Abbood, I.K.; Idrees, A.K. Data reduction techniques for wireless multimedia sensor networks: A systematic literature review. *J. Supercomput.* **2024**, *80*, 10044–10089. [CrossRef]
182. Garcia, A.; Saez, Y.; Harris, I.; Huang, X.; Collado, E. Advancements in air quality monitoring: A systematic review of IoT-based air quality monitoring and AI technologies. *Artif. Intell. Rev.* **2025**, *58*, 275. [CrossRef]
183. Alqurashi, I.; Alver, N.; Bagci, U.; Catbas, F.N. A review of ultrasonic testing and evaluation methods with applications in civil NDT/E. *J. Nondestruct. Eval.* **2025**, *44*, 53. [CrossRef]
184. Cabanillas-Carbonell, M.; Sallari Rivera, J.; Santivañez Muñoz, J. Artificial intelligence in video surveillance systems for suspicious activity detection and incident response: A systematic review. *Adv. Sci. Technol. Res. J.* **2025**, *19*, 389–405. [CrossRef]
185. Mallidi, S.K.R.; Ramisetty, R.R. Optimizing Intrusion Detection for IoT: A Systematic Review of Machine Learning and Deep Learning Approaches with Feature Selection and Data Balancing. *WIREs Data Min. Knowl. Discov.* **2025**, *15*, e70008. [CrossRef]
186. Kaveh, H.; Alhajj, R. Advancing civil infrastructure with Digital Twins: A review of applications and challenges. *J. Civ. Eng. Manag.* **2025**, *31*, 24921. [CrossRef]

187. Muhammad, R.; Sagara, M.S.A.; Teluma, Y.M.; Wicaksana, F.A. AI as Modern Technology for Home Security Systems: A Systematic Literature Review. *Eng. Proc.* **2025**, *107*, 35. [CrossRef]
188. Boucif, O.H.; Lahouaou, A.M.; Boubiche, D.E.; Toral-Cruz, H. Artificial intelligence of things for solar energy monitoring and control. *Appl. Sci.* **2025**, *15*, 6019. [CrossRef]
189. Marangis, D.; Tziolis, G.; Livera, A.; Makrides, G.; Kyprianou, A.; Georghiou, G.E. Intelligent Maintenance Approaches for Improving Photovoltaic System Performance and Reliability. *Sol. RRL* **2025**, *9*, 2500289. [CrossRef]
190. Parida, L.; Banerjee, S.; Moharana, S. Current status and future challenges on performance evaluation of reinforcement-concrete bond and the interfacial deterioration using piezo impedance-based SHM (PISHM). *Struct. Concr.* **2025**, *26*, 8255–8291. [CrossRef]
191. Popescu, S.M.; Mansoor, S.; Wani, O.A.; Kumar, S.S.; Sharma, V.; Sharma, A.; Arya, V.M.; Kirkham, M.B.; Hou, D.; Bolan, N.; et al. Artificial intelligence and IoT driven technologies for environmental pollution monitoring and management. *Front. Environ. Sci.* **2024**, *12*, 1336088. [CrossRef]
192. Mahadik, S.S.; Pawar, P.M.; Muthalagu, R. Heterogeneous IoT (HetIoT) security: Techniques, challenges and open issues. *Multimed. Tools Appl.* **2024**, *83*, 35371–35412. [CrossRef]
193. Forlesi, M.; Esposito, A.; Zyrianoff, I.; Marzani, A.; Leonardi, G.; Di Felice, M. Crack Detection and Monitoring: Review and Comparison of IoT and Image-Based Methods [Roadmap for Measurement and Applications]. *IEEE Instrum. Meas. Mag.* **2025**, *28*, 26–35. [CrossRef]
194. Al-Yaseri, A.M.; Al-Hadithy, L.K. Advances in the structural performance of reinforced concrete flat plate column connections under gravity and seismic loads. *J. Build. Pathol. Rehabil.* **2025**, *10*, 58. [CrossRef]
195. Habibovic, I.; Almisreb, A.; Hodzic, M.; Turaev, S.; Cantelli-Forti, A. Machine Learning Algorithms and Sensor Technologies for Aging-in-Place Applications: A Review. *IEEE Sens. J.* **2025**, *25*, 34326–34347. [CrossRef]
196. Qasim Flayyih, H.; Waleed, J.; Ibrahim, A.M. IoT-based AI Methods for Indoor Air Quality Monitoring Systems: A Systematic Review. *Int. J. Comput. Digit. Syst.* **2024**, *16*, 813–826. [CrossRef] [PubMed]