

Article

Research Communities in Smart Homes Security: A Systematic Mapping Study

Fazeleh Dehghani Ashkezari ^{1,2,*} , Andreas Jacobsson ^{1,2} , Kayode S. Adewole ^{1,2} , Klara Svalin ³  and Martin Höst ^{1,2} 

- ¹ Department of Computer Science and Media Technology, Malmö University, 211 19 Malmö, Sweden; andreas.jacobsson@mau.se (A.J.); kayode.adewole@mau.se (K.S.A.); martin.host@mau.se (M.H.)
² Sustainable Digitalisation Research Center, Malmö University, 211 19 Malmö, Sweden
³ Department of Criminology, Malmö University, 211 19 Malmö, Sweden; klara.svalin@mau.se
* Correspondence: fazeleh.dehghaniashkezari@mau.se

Abstract

Smart homes are becoming increasingly common, bringing convenience to users but also raising serious security concerns. As the number of connected devices grows, so does the research interest in securing smart homes. However, the literature is broad, making it difficult to understand the main research directions and how they are connected. Given the scope and diversity of existing research, a systematic mapping study was chosen to provide a high-level overview of smart home security research by mapping research communities, identifying dominant themes, and examining their evolution over time. We retrieved articles from the Scopus database published between 2000 and April 2025, resulting in approximately 13,600 articles. After filtering out unrelated domains such as smart vehicles, smart industry, and general IoT, a final set of 6313 publications specifically focused on smart home security was used for analysis. We applied a citation-based network analysis approach, constructed an author citation graph, and used the Louvain community detection algorithm to identify 12 main research communities. Each community was further analyzed based on its keywords, most-cited publications, leading authors, and institutions. Our results provide a structured overview of the field, highlighting its key themes and evolution over time. This work can help researchers better navigate the smart home security landscape and identify future research opportunities.

Keywords: smart homes; security; community detection; literature review; systematic mapping study; scopus



Academic Editor: Amiya Nayak

Received: 23 December 2025

Revised: 31 January 2026

Accepted: 6 February 2026

Published: 11 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article

distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

A smart home is a residence equipped with internet-connected devices that enable remote monitoring, automation, and control of home functions such as lighting, temperature, appliances, and security systems [1]. These capabilities rely on Internet of Things (IoT) technologies, which offers interaction among devices and enhances user comfort and energy efficiency [2,3]. However, the integration of these technologies also introduces a range of security and privacy risks.

Smart home devices are often manufactured by different vendors with heterogeneous architectures and limited built-in security features [4]. Moreover, many users lack basic awareness of security and privacy risks, and devices are frequently deployed with weak default configuration, which makes smart homes easy targets for attacks such as malware infections, data breaches, surveillance, and denial of service [5,6].

Multiple studies have documented the evolving landscape of smart home threats and proposed mitigation strategies, including secure communication protocols, encryption mechanisms, user awareness, and machine learning-based intrusion detection systems [7–9]. Despite these efforts, the literature remains fragmented across disciplines and application domains, such as energy, health, and entertainment. As Solaimani et al. [10] observe, many studies focus on isolated components of smart homes without offering a comprehensive or integrated understanding of the broader research field. Similarly, Marikyan et al. [11] found that existing reviews tend to adopt a single technology or single domain viewpoint, neglecting the complex interplay between smart home systems, user behaviors, and security threats.

Several literature reviews have listed vulnerabilities and countermeasures in smart homes, such as the works by [5,12,13]. However, as noted by Plachkinova et al. and Arabo [14,15], there is a lack of structured understanding of how the research field itself is organized: its key communities, thematic clusters, and the underlying structure of the research landscape over time.

To address this gap, we conducted a systematic mapping study (SMS) complemented by bibliometric and network analysis to uncover the structure, themes, and evolution of research communities in smart home security. We retrieved a large body of relevant publications, constructed an author citation network, and applied the Louvain community detection algorithm [16] to identify cohesive research clusters and thematic areas.

In this study, we aim to map the main research communities in smart home security, analyze how these communities have evolved over time, examine the leading contributors and publication venues, and characterize the dominant research topics and themes within each community, as well as their relationships across communities. Through this analysis, we provide a data-driven map of the smart home security research landscape, highlighting key research themes, collaboration patterns, and emerging areas.

2. Related Work

Research on smart home security spans several areas, including technical vulnerabilities, application-level risks, usability challenges, and broader social and ethical concerns. The literature contains different types of reviews and analyses, each contributing a specific perspective on how security issues in smart homes are understood and addressed. In this section, we summarize these contributions and highlight how our study differs in scope and methodology.

Many existing studies use the systematic literature review (SLR) methodology to investigate specific aspects of smart home security, yet their focus and coverage vary considerably.

One stream of such research concentrates on technical risks and device-level vulnerabilities within smart home environments. For example, Khan et al. discuss threats such as unauthorized access, data breaches, and device malfunction, drawing attention to the need for stronger security-by-design practices [17]. Vera-Mundaca and Aquino-Trujillo [18] categorize prevalent threats and outline a range of mitigation strategies for IoT-based residential settings. Although Liao et al. [19] review IoT devices in mobile computing environments, their analysis of attack vectors and defense mechanisms is also applicable to smart homes, given the common use of embedded and mobile devices in domestic systems. These studies provide in-depth technical insight but typically focus on specific threat categories or system components rather than the structure of the research field as a whole.

In addition to device-level vulnerabilities, some studies focus on security challenges related to smart home applications and system interfaces. For instance, Ansari et al. [20]

outline weaknesses in smart home controlling applications and categorize different attack paths. Complementing this perspective, Tampubolon et al. [21] discuss the tension between security requirements and user accessibility, showing how security measures can introduce usability challenges and influence system design decisions.

A smaller body of work explores the broader social and ethical dimensions of smart home technologies. A representative study in this area is by Olabode et al. [22], who identify issues such as surveillance, exclusion, and algorithmic bias. Their findings show that risks in smart homes extend beyond technical failures and involve questions of fairness, privacy, and user rights. However, these perspectives are often reviewed separately from technical security research, reinforcing the fragmented nature of the literature.

Although these studies contribute valuable insights, they also reveal that the smart home security literature is fragmented across technical, social, and application domains. Most existing reviews rely on manual synthesis and predefined categories, which limits their ability to capture how the research field is structured overall or how different topics evolve over time.

To address such limitations, prior works, such as those by Katsikeas et al. [23] and Heiding et al. [24] in their review studies on security and vulnerability assessment, have shown the usefulness of data-driven bibliometric approaches for mapping large and complex research landscapes. These studies show that network-based methods can uncover research communities and linkages that remain hidden in traditional reviews. However, these approaches have not yet been systematically applied to smart home security research. Taking inspiration from the structure and approach of these works, our study applies a large-scale bibliometric and community detection method to smart home security. Despite rapid growth in this field, no mapping effort has systematically analyzed its research communities, topic clusters, and structural evolution. Our work addresses this gap by combining an SMS methodology with author citation network analysis to provide a comprehensive, data-driven overview of the field.

3. Methodology

To explore the structure and evolution of research in smart home security, this study follows the established process for an SMS as outlined by Petersen et al. [25] and Kitchenham and Charters [26]. The SMS methodology provides a structured and reproducible approach for identifying, screening, classifying, and mapping the literature. Accordingly, we conducted a systematic search, applied inclusion and exclusion criteria, and extracted structured metadata. To support large-scale classification and mapping, we complement the traditional SMS process with citation-based bibliometric techniques inspired by prior studies [23,24]. Instead of manually classifying studies according to a procedure defined by [25] for conducting an SMS, we identified research communities by constructing an author citation network and applying the Louvain community detection algorithm [16]. The resulting communities were interpreted and given descriptive names through a combination of manual review of keywords from the most cited publications and a data-driven analysis of keyword usage across each community.

The combination of the SMS methodology and the citation-based bibliometric analysis enables a structure for methodological rigor and a scalable map of the research trends in smart home security. While SMS provides a structured framework for literature identification and selection, bibliometric network analysis supports large-scale, data-driven classification and the identification of emergent research structures. This integration informs the interpretation of the results and underpins the methodological choices described in the following sections, with remaining limitations discussed later in this paper.

3.1. Review Protocol

This study follows a review protocol to ensure transparency and reproducibility, in accordance with guidelines for SMSs [25,26]. The protocol organizes this review into a sequence of automated and analysis-driven phases, covering literature identification, study selection, data extraction, and classification.

As illustrated in Figure 1, the protocol begins with an iterative keyword refinement and query design, which supports systematic literature identification. The resulting query is used in an automated data collection phase to retrieve publications and apply relevance-based filtering on bibliometric metadata, producing the study dataset used in subsequent analysis. In the second phase shown in Figure 1, the protocol focuses on large-scale classification and mapping of the selected literature. Citation-based network analysis is used to detect research communities, followed by sub-community detection to reveal more specific research themes within each community. This phase enables an overview of how research in smart home security is organized and how key topics are interconnected.

A detailed description of each phase of the review protocol is provided in the following subsections.

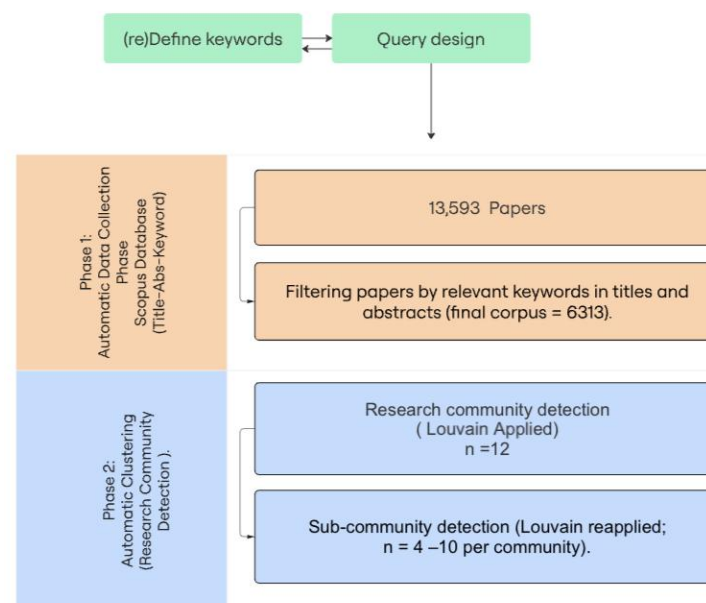


Figure 1. Methodological workflow of this study, illustrating the automated pipeline for data collection and community detection.

3.2. Search Strategy

Following SMS guidelines, the search process included selecting an appropriate data source and designing and refining the search query. To support large-scale mapping and bibliometric analysis, we additionally retrieved and exported structured metadata for all relevant publications. The full search procedure ensures a clearly defined scope and a consistent, reproducible retrieval process.

3.3. Data Source Selection

Scopus (<https://www.scopus.com>, accessed on 25 April 2025) was selected as the primary data source due to its extensive indexing of peer-reviewed journals and conference proceedings in computing, engineering, and security. Scopus also provides a stable API with structured metadata fields, enabling the large-scale and automated data extraction required for this study.

3.4. Query Design

The search query was developed using an iterative process conducted prior to final execution, in alignment with the SMS requirement for transparent and reproducible search procedures [25,26]. To construct the search query, we first identified terminology associated with the smart home domain, including expressions such as “smart home,” “home automation,” “connected home,” “domotics,” “residential IoT,” and “intelligent home.” We then compiled security-related terminology, covering both general concepts, such as “security,” “privacy,” and “risk”, and more specific threats and techniques, including “malware,” “ransomware,” “phishing,” “access control,” “encryption,” and “anomaly detection.”

These terms were selected based on their relevance in the literature and their prevalence in prior review studies. The final query was formulated using TITLE-ABS-KEY fields in Scopus and combined the smart home and security term sets using Boolean AND/OR operators to ensure that only publications addressing both domains were retrieved. The complete search query is provided in the Zenodo repository (<https://zenodo.org/records/18538858>, accessed on 5 February 2026).

3.5. Article Retrieval

The final query was executed through the Scopus Search API using a Python-based automated script (Python 3.12.12). To avoid retrieval biases and ensure consistent coverage, the search was performed year by year. Because of API pagination constraints, results were downloaded in batches of 25 records, and a short delay was introduced between consecutive API calls to comply with Scopus rate limits. For each retrieved publication, the script collected a full set of metadata, including the title, abstract, author names and their Scopus Author IDs, author affiliations, keywords, citation counts, publication year, source title (journal or conference), and unique identifiers such as EIDs and DOIs. The Python script used for this automated retrieval process is publicly available in the Zenodo repository (<https://zenodo.org/records/18538858>, accessed on 5 February 2026) provided with this study. In total, the retrieval process resulted in 13,593 publications, with the final extraction carried out on 25 April 2025.

3.6. Study Selection and Screening

A publication was included in this study if it met the conditions defined in the search query and was indexed between January 2000 and April 2025. Publications before 2000 were excluded because smart home devices were not yet widely Internet-connected, and security-related discussions of smart homes were minimal. This date range reflects the emergence and evolution of modern smart home technologies. These constraints were implemented in the code script during the article retrieval phase.

Publications were excluded through a two-stage automated screening procedure. First, duplicate records were identified using Scopus EIDs and removed to ensure uniqueness, resulting in the elimination of 2592 entries. Second, a relevance filter was applied to the title and keyword fields of the dataset to remove studies unrelated to smart home security. This filter excluded records containing any of the following domain-specific terms: “smart vehicles,” “smart car,” “smart farming,” “smart cities,” “smart healthcare,” “smart phone,” and “smart factory.” These terms were used in the filtering script and led to the removal of 4690 publications. Additional exclusions were applied to records lacking essential bibliometric metadata (such as author identifiers or citation information), as these could not support subsequent network-based analysis. Surveys and review papers were intentionally retained in the analysis. While such papers are often broad in scope, they typically synthesize prior work and are widely cited across multiple research areas. In a citation-based analysis, this makes them important structural connectors that link related

research communities. Excluding these papers could therefore hide some relationships in the research landscape. Following this selection process, 6311 publications (out of 13,593) remained. This final dataset was saved as a CSV file and used in later stages to build the author graph and perform bibliometric analysis.

3.7. Author Graph Construction

To uncover the structure of research communities in the domain, we built an author citation graph. In this graph, each node represents a unique author (identified via their Scopus Author ID) and edges show citation links between authors. Since authors do not directly cite each other, we inferred these links from article-level citation data. We began with a dataset of citing-cited paper pairs (based on Scopus EIDs) and then extracted the full list of authors for each paper. For each citing–cited paper pair, the citation is projected to the author level by creating directed links between all authors of the citing paper and all authors of the cited paper. These links are represented as unweighted edges, so repeated citation events between the same authors do not increase edge strength. This design allows patterns of citation relationships across multiple publications to shape the network structure while limiting the influence of individual highly collaborative papers. An edge exists between two authors if at least one of them cited the other in their papers. This process produced a directed network showing how citations flow from authors of citing papers to authors of cited papers. To reduce noise, we kept only authors with at least 10 total citations (in-degree plus out-degree) (see Figure 2).



Figure 2. Author citation graph with community detection. Each node represents an author; node size corresponds to citation volume. Colors indicate communities. Edges were removed for more clarity. For better view of the figure, the reader is referred to the web version of this article.

For better interpretation and visual clarity, we hid edges in the final graph layout. Node size represents the author’s citation count measured as the total number of incoming and outgoing citation links (node degree), while node color indicates the research community to which the author is assigned, as identified through the community detection procedure described in the following subsection (Section 3.8).

3.8. Community Detection

To identify groups of researchers working on related topics within the field of smart homes security, we applied the Louvain community detection algorithm, introduced by Blondel et al. [16], to the constructed author citation graph. The Louvain method is a hierarchical, greedy optimization technique that seeks to maximize modularity, a scalar value that quantifies the strength of division of a network into communities, which makes it useful for the study at hand [27].

Modularity is calculated using the following equation:

$$Q = \frac{1}{2m} \sum_{i,j} \left[A_{ij} - \frac{k_i k_j}{2m} \right] \delta(c_i, c_j)$$

where

- A_{ij} represents the edge weight between nodes i and j . Here the edge weights are the number of in-degree plus out-degree citations.
- k_i and k_j are the sum of A_{ij} (weights of edges) attached to nodes i and j .
- m is the total number of edge weights in the graph.
- c_i and c_j are the communities assigned to nodes i and j , respectively.
- $\delta(c_i, c_j)$ is 1 if c_i and c_j are equal and 0 otherwise.

In simpler terms, this algorithm helps uncover clusters of authors who are more closely connected to each other, based on citation behavior, than to the rest of the network. It operates in two main phases: First, it assigns each author to their own community, which means each author is a community, then iteratively merges communities if doing so increases modularity. Once no further improvements can be made, it aggregates communities into single nodes and repeats the process, further refining the structure. This allows the algorithm to work efficiently even on large networks, detecting meaningful and well-separated communities without requiring any manual input or predefined labels [16].

Using this approach, each author in the graph is assigned to the community where they have the most citation connections. This helps reveal how the research landscape is organized, highlights key contributors, and shows which topics are drawing the most attention. Although some authors may work across different themes, the Louvain method places them in the group where their influence is strongest.

3.9. Community Graph Visualization

To visually represent the structural relationships between research communities in smart home security, we constructed a community-level graph based on the results of our author-level citation network and Louvain clustering.

Each node in the graph corresponds to a distinct community identified by the Louvain algorithm. The size of each node reflects the total number of authors in that community (i.e., its population), while node color serves as a visual cue to distinguish individual communities. For clarity, only inter-community relationships were considered in this layout.

The layout of the graph was generated using the spring-layout algorithm from the Python NetworkX library (<https://networkx.org/en/> (accessed on 20 June 2025)), which simulates a force-directed placement of nodes. This approach positions communities with stronger inter-community citation coupling closer together, offering an intuitive overview of thematic proximities in the field.

Since the Louvain algorithm functions entirely based on structural patterns in the citation graph, it does not provide semantic descriptions or topic labels for the communities it detects. As a result, community labeling was performed as a separate step to describe the dominant research focus of each group rather than to strictly classify individual papers.

This labeling process combined manual inspection and data-driven validation. Initially, the themes were determined through a manual review of the top keywords associated with the five most influential authors in each community. These interpretations were later validated using an automated keyword frequency and distinctiveness analysis, ensuring that the assigned names accurately reflected the underlying research focus. Figure 3 illustrates the resulting community graph.

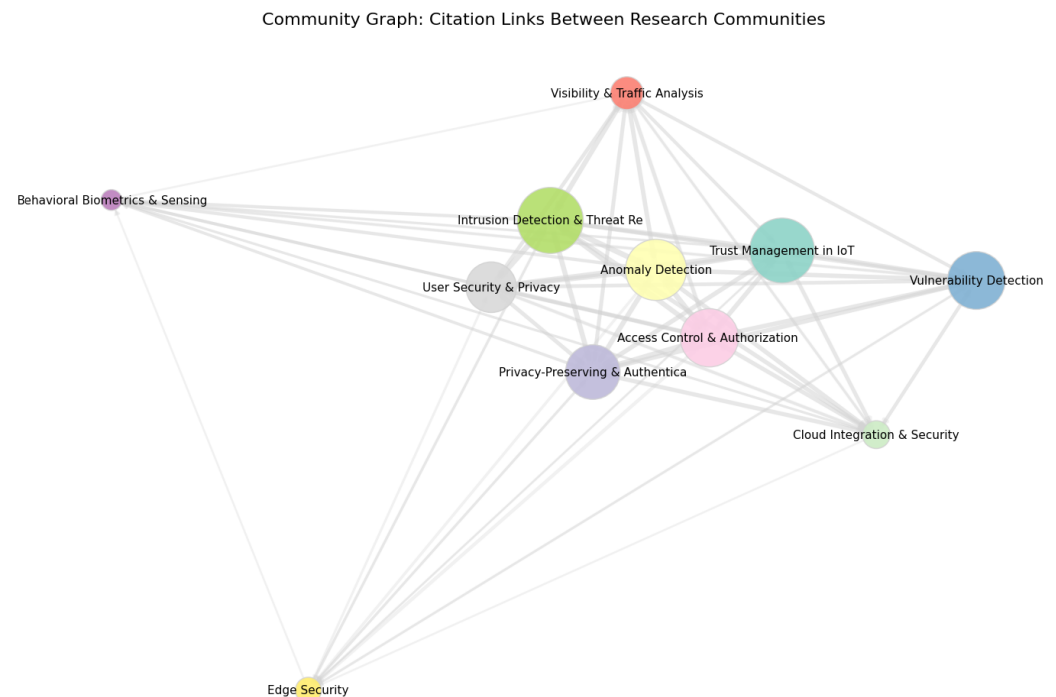


Figure 3. Connections between main research communities in smart home security. Nodes represent research communities, with node size proportional to the number of authors in each community. An edge between two nodes indicates the existence of a citation connection between the corresponding communities, and edge thickness reflects the volume of inter-community citations.

3.10. Sub-Community Analysis

An initial review of the detected communities indicated that some large clusters covered multiple research topics. Sub-community detection was therefore used to reveal finer thematic distinctions that could not be identified at the community level. To examine the internal structure of each research community, we conducted a sub-community analysis by reapplying the Louvain algorithm within each previously detected community. For each community, we built a local author-level citation graph and identified sub-communities based on citation interactions between authors belonging to the same community. This process allowed us to uncover fine-grained clusters of authors that represent more specialized research themes within their broader associated fields.

Sub-community labels are assigned afterward to summarize the dominant research focus reflected in the publications within each group, rather than to impose a uniform technical taxonomy. As a result, some sub-communities are characterized by specific security-related mechanisms, while others are defined by recurring application contexts.

3.11. Threats to Validity

Several factors may affect the validity of this study. While care was taken throughout the study design and execution to reduce potential threats to validity, some limitations remain and should be considered when interpreting the results.

First, the study relies on the Scopus database as the sole data source. Although Scopus provides broad coverage of peer-reviewed literature and a well-documented API that supports large-scale automated analysis, relevant studies indexed in other databases may not be included. This may affect the completeness of the dataset but is unlikely to substantially alter the overall structure of the research landscape identified.

Second, the selection and filtering process depends on the quality of bibliographic metadata and on keyword-based matching applied to titles and keywords. As a result, relevant studies using alternative terminology or containing incomplete metadata may be excluded. In addition, the high degree of automation reduces manual inspection at the individual-study level, which may limit opportunities for human judgment and quality assurance. Given the size of the dataset and the focus on high-level patterns rather than individual studies, the impact of these limitations is expected to be limited.

Finally, the citation-based measures used to construct author networks and identify research communities may introduce bias, as older publications tend to accumulate more citations over time regardless of their current relevance. While this may affect how prominent some communities appear, it is unlikely to change the main thematic structure of the field. These limitations should therefore be kept in mind when interpreting the findings of this study.

4. Results

As mentioned before, all data were retrieved from the Scopus database in April 2025 and a total of 6311 papers, after filtering out the irrelevant keywords, were included in the final analysis. These publications were authored by 18,156 individuals and received 103,082 citations in total. Table 1 presents the ten most cited publications within the final dataset, based on total citation count.

Although not all titles explicitly reference “smart home security”, these works have significantly influenced the field through their focus on key enabling technologies such as edge computing, fog computing, blockchain security, intrusion detection, and IoT device classification, which are core components of contemporary smart home.

Table 1. Top 10 Most Cited Publications in the Smart Home Security Dataset. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Edge Computing: Vision and Challenges [28]	Shi W. et al. (2016)
Blockchain for IoT Security and Privacy: The Case Study of a Smart Home [29]	Dorri A. et al. (2017)
Exploiting Smart e-Health Gateways at the Edge of Healthcare Internet-of-Things: A Fog Computing Approach [30]	Rahmani A.M. et al. (2018)
A Survey of Intrusion Detection in Internet of Things [31]	Zarpelão B.B. et al. (2017)
Towards an Optimized Blockchain for IoT [32]	Dorri A. et al. (2017)
IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices [33]	Meneghello F. et al. (2019)
Security Analysis of Emerging Smart Home Applications [34]	Fernandes E. et al. (2016)
Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics [35]	Sivanathan A. et al. (2019)
Securing Fog Computing for Internet of Things Applications: Challenges and Solutions [36]	Ni J. et al. (2018)
DIoT: A Federated Self-learning Anomaly Detection System for IoT [37]	Nguyen T.D. et al. (2019)

The top 10 countries that conducted research in smart home security include India, China, and the United States as the leading contributors, with 2098, 1589, and 1406 publications respectively. These are followed by the United Kingdom (518), Germany (424), South Korea (351), Canada (287), Saudi Arabia (246), Australia (238), and Italy (226). This

distribution reflects a strong global interest in enhancing the security of smart home environments, with particularly high research activity in Asia and North America. The Louvain community detection algorithm identified a total of 12 distinct author communities within the citation network. Figure 3 visualizes these key communities. In addition, top twenty most frequently used keywords in the area of focus in this field, particularly relevant to smart home security, are shown in Figure 4.

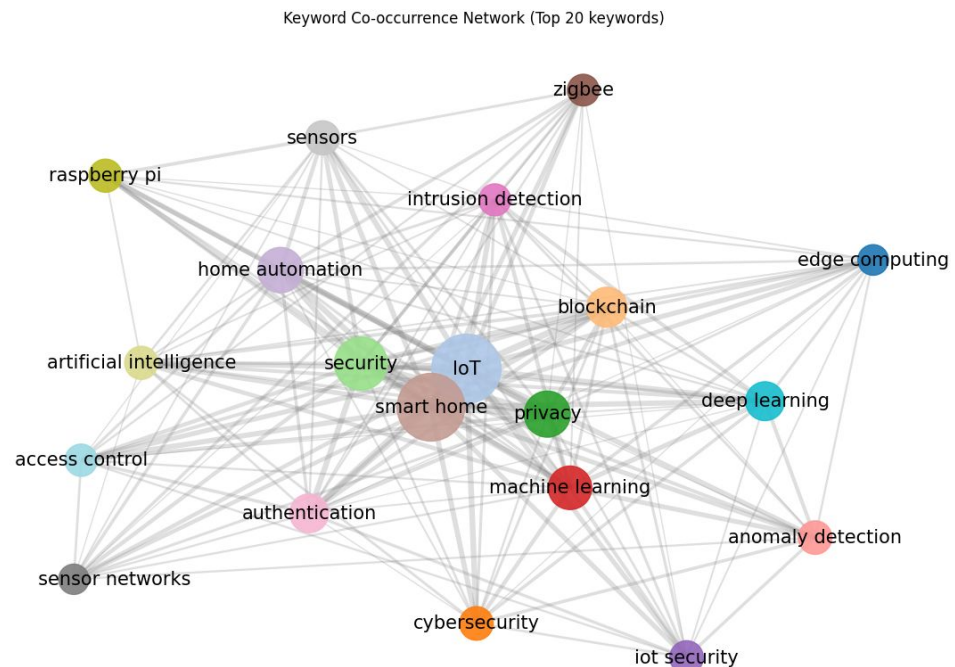


Figure 4. Keyword Co-occurrence Network of the Top 20 Keywords: Node size reflects keyword frequency and edge thickness indicates how often two keywords appear together in the same paper.

The key research communities in security in the smart home, ranked by the number of published articles, are shown in Table 2. It is worth noting that these communities are not completely disjointed; there is some overlap between them. In practice, certain authors or papers may appear to be part of multiple communities, reflecting the interdisciplinary nature of research in this field.

Table 2. Communities sorted by number of papers in descending order. Row shading is used to improve readability and does not convey additional information.

Community Name	No. of Papers
Intrusion Detection and Threat Response	1719
Anomaly Detection	1292
Trust Management in IoT	1263
Access Control and Authorization	1078
Vulnerability Detection	1010
Privacy Preserving and Authentication	1118
User Security and Privacy	952
Visibility and Traffic Analysis	368
Edge-Based Localization and Recognition	274
Cloud Integration and Security	234
Behavioral Biometrics and Sensing	82
Hardware-Accelerated AIoT Security	2

Table 3 presents the top ten publication venues contributing to the smart home security literature analyzed in this study, showing their distribution across the twelve identified re-

search communities discussed in Sections 4.1–4.12. The annual publication graph (Figure 5) shows the number of smart home security publications per community, illustrating the overall growth of research activity over time. Table 4 lists the top ten institutional affiliations in smart home security research, ranked by number of publications. It highlights where most research activity is concentrated and shows that leading contributions come from universities across Asia and Europe.

Table 3. Occurrences of the Top 10 Leading Publication Venues Across Research Communities in Smart Home Security Literature. Each column corresponds to one research community discussed in Sections 4.1–4.12. Row shading is used to improve readability and does not convey additional information.

Source Title	Section 4.1	Section 4.2	Section 4.3	Section 4.4	Section 4.5	Section 4.6	Section 4.7	Section 4.8	Section 4.9	Section 4.10	Section 4.11	Section 4.12
Sensors (Journal)	7	41	21	33	48	55	8	5	18	4	1	0
IEEE Access (Journal)	18	18	23	57	5	70	2	4	8	4	0	0
IEEE Internet of Things (Journal)	48	28	1	42	0	57	2	8	13	0	0	0
ACM International Conference Proceeding Series	31	11	4	3	11	8	45	10	0	1	0	1
Lecture Notes in Networks and Systems	1	14	23	3	10	4	1	0	0	5	0	0
Communications in Computer and Information Science	2	15	2	0	4	7	2	1	5	0	0	0
Lecture Notes in Computer Science (including subseries LNAI and LNBI)	0	0	24	3	0	0	0	0	0	0	0	0
Lecture Notes in Electrical Engineering	5	1	0	0	14	0	3	0	0	0	0	0
AIP Conference Proceedings	0	6	6	0	11	0	0	0	0	0	0	0
Advances in Intelligent Systems and Computing	0	4	4	5	2	3	0	0	0	0	0	0

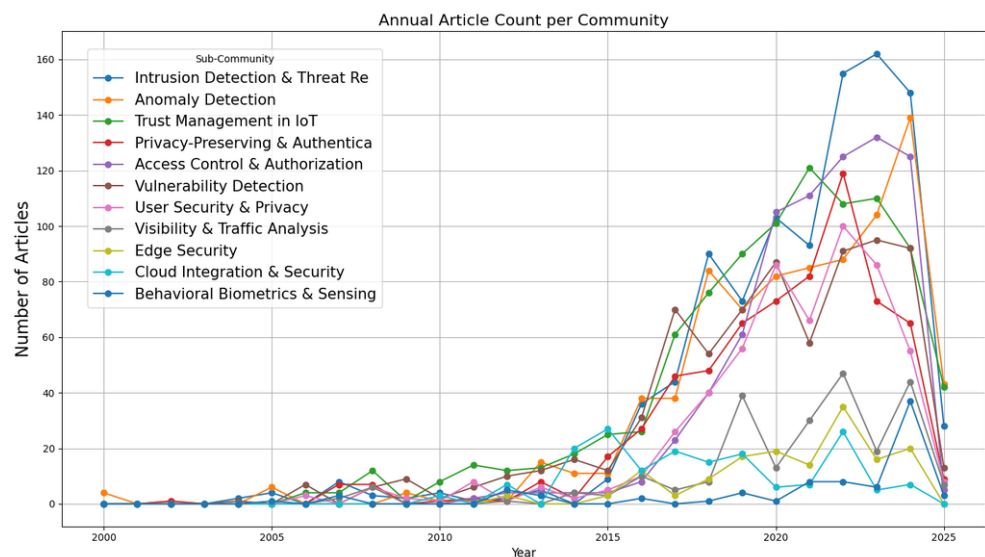


Figure 5. Annual article count per community in smart home security research. The figure illustrates the overall publication trends across major research communities, showing their growth and temporal evolution.

Table 4. Top 10 Affiliations in Smart Home Security Research (up to April 2025). Row shading is used to improve readability and does not convey additional information.

Rank	Affiliation	Country	Publications
1	Vellore Institute of Technology	India	45
2	University of Oxford	United Kingdom	20
3	K L Deemed to be University, Vaddeswaram	India	19
4	Malmö University	Sweden	15
5	Vellore Institute of Technology, Chennai	India	15
6	Chongqing University of Posts and Telecommunications	China	14
7	Amity University	India	14
8	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH Aachen University)	Germany	12
9	Ontario Tech University	Canada	12
10	Bina Nusantara University	Indonesia	11

In the remainder of this section, we show the 12 main communities along with their smaller sub-communities (see Appendix A). We describe the main topics of each community and highlight the most common research themes, citing one or two representative papers from that sub-community. In addition, annual graphs depicting each community and its sub-communities are available in Appendix B. These graphs offer detailed insights into growth trends and publication counts per year across all sub-communities. While the Louvain algorithm clusters authors based on citation relationships, this method does not perfectly reflect research areas, since authors can work on different topics and sometimes cite papers that are not directly related to their main field. However, this method often shows clear patterns and shared interests, making it useful to understand what topics are popular or important.

4.1. Intrusion Detection and Threat Response

Intrusion Detection and Threat Response is the largest community, reflecting its central role in securing smart home environments. This community includes 1719 papers from 2004 to 2025. This study identified 10 sub-communities within it, as shown in Figure A1. The top five most cited articles in this community are presented in Table 5.

Research in this community focuses on detecting unauthorized access, identifying abnormal system behavior, and coordinating defensive responses across heterogeneous IoT devices. Publication activity has steadily increased since 2016, possibly driven by the rise of connected consumer devices and more complex home networks. **Smart Platform Security** in smart homes focuses on securing the platforms that integrate devices, applications, and cloud services in smart homes. Research emphasizes enforcing appropriate permissions, limiting over-privileged applications, and preventing cross-app interference that could expose users to security risks. Recent work also explores privacy-preserving techniques, such as federated learning, to detect platform-level threats without sharing sensitive household data [34,38].

Behavioral Traffic Analysis focuses on examining network traffic patterns to detect suspicious or malicious behaviors. Research in this sub-community highlights traffic profiling and distinguishing normal from abnormal device activity to identify potential attack vectors [39,40]. This area has grown rapidly, becoming the most prominent sub-community in 2022 with more than 55 publications, which is higher than any other sub-community in a single year (see Figure A12). **Federated Intrusion Detection** focuses on distributed and collaborative intrusion detection across devices or systems. It leverages federated learning and decentralized architectures to improve threat detection without sharing raw data [37]. **Behavioral Intrusion Analysis** uses behavioral models of users or devices to spot intrusions. For this goal, it applies machine learning and pattern recognition to differentiate legitimate behavior from threats [41,42]. The sub-community of **Threat Modeling and Benchmarking** systematically identifies potential threats and evaluates defense effectiveness. The papers in this sub-community introduce frameworks for categorizing attacks, analyzing attack scenarios and benchmarking detection systems [43,44]. **The Privacy-Aware Threat Control** sub-community is about ensuring that smart home systems protect user data while maintaining secure control of devices. Research here explores how to design access control policies, prevent over-privileged or malicious applications, and strengthen communication security [45,46]. **Identity-Driven Threat Prevention** centers on using identity as the foundation for securing smart homes. Research in this category explores how trusted identities of devices, users, data, and applications can be enforced to block unauthorized access and stop threats at their source [47]. **Federated Intrusion Response** focuses on how smart home systems can coordinate defense actions once a threat is detected. Unlike Federated Intrusion Detection, which concentrates on identifying anomalies, this sub-community

develops mechanisms for privacy-preserving response, adaptive access control, and insider threat mitigation across distributed devices [48]. The **Contactless Authentication** sub-community develops techniques to secure smart homes by verifying users without relying on traditional passwords or touch-based inputs. Research here leverages modalities such as mmWave radar [49], voice liveness detection [50], and gesture-based authentication [51] to defend against spoofing and impersonation attacks while preserving usability. **Risk and Threat Modeling (Ecosystem-Oriented)** looks at risks that come from the whole smart home ecosystem, where many devices, services, and users interact. Research in this area builds broad threat models and case-based analyses to show how these complex settings can create new vulnerabilities [52].

Table 5. Top Cited Publications in the Intrusion Detection and Threat Response community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Edge Computing: Vision and Challenges [28]	Shi W. et al. (2016)
Security Analysis of Emerging Smart Home Applications [34]	Fernandes E. et al. (2016)
Securing Fog Computing for Internet of Things Applications: Challenges and Solutions [36]	Ni J. et al. (2018)
D ² IoT: A Federated Self-learning Anomaly Detection System for IoT [37]	Nguyen T.D. et al. (2019)
The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved [45]	Zhou W. et al. (2018)

4.2. Anomaly Detection

The second largest community is Anomaly Detection, comprising 1292 papers written by 827 authors. These papers are clustered into nine sub-communities (see Figure A2). The top most cited works in this community are summarized in Table 6.

Since 2016, the Machine Learning-based Intrusion Detection Systems (**ML-based IDS**) have shown the strongest growth within smart home anomaly detection research (see Figure A13). While IDS concepts were outlined earlier, this sub-community specifically investigates how machine learning improves detection by learning normal device behavior and identifying deviations that may signal threats. Supervised, unsupervised, and self-learning models enable IDSs to handle complex traffic patterns and evolving attack strategies in dynamic household environments [53,54].

Studies on the Anomaly Detection sub-community focus on categorizing the evolving scope of security threats, protocols, and countermeasures within the IoT and particularly smart homes. These studies play a pivotal role in identifying common vulnerabilities across protocols such as Zigbee and 6LoWPAN and highlighting the limitations of current security practices in resource-constrained environments. They also show gaps between theoretical security models and practical deployment challenges [31,33]. As illustrated in Figure A2, the Anomaly Detection sub-community has a central position and connects to multiple technical sub-communities. It reflects the role of survey papers as citation hubs that link related research areas. The articles within the **Vulnerability Analysis** sub-community cover the identification, categorization, and experimental validation of weaknesses in smart home systems, with a particular focus on IoT devices and protocols. These works examine vulnerabilities across different layers and applications of smart home infrastructure [55,56].

The **Threat Modeling** sub-community examines cyber and physical risks within specific smart home systems, focusing on how these risks create the conditions under which anomalies arise. This work builds structured views of critical assets, vulnerabilities, and potential attack paths, enabling researchers to understand where abnormal behavior is

likely to occur and how it can be detected early. Studies in this area highlight recurring issues such as software and configuration weaknesses, user-driven risks, and unprotected communication surfaces, emphasizing the need for systematic risk identification and mitigation within smart home environments [57,58].

Behavioral Anomaly Detection focuses on identifying unusual traffic or user activity patterns in smart homes by distinguishing normal from abnormal behavior. Research in this sub-community often applies machine learning, traffic profiling, and behavioral modeling to detect hidden threats that traditional methods may miss [59,60]. **Device Security** in smart homes centers on ensuring that IoT devices and appliances are reliable, protected, and resilient against misuse or failure. Research in this sub-community often ties into anomaly detection by monitoring device behavior, traffic patterns, and sensor outputs to spot deviations that may indicate compromise or malfunction. These works emphasize secure communication, dependable device operation, and mechanisms that prevent unauthorized actions through continuous behavioral monitoring [61,62].

Network Forensics sub-community focuses on capturing, analyzing, and preserving digital evidence from IoT traffic to investigate abnormal activities and potential attacks. Research in this area develops methods for advanced traffic analysis [63], tamper-resistant evidence preservation [64], and automated forensics investigations tailored to smart home environments [65]. Within smart home anomaly detection, the **Privacy and access control** sub-community focuses on protecting household data and restricting device interactions that could interfere with detection processes. Research highlights that unsecured sensor information can reveal sensitive patterns, showing the need for confidentiality and authenticated communication in detection pipelines [66]. Lightweight security mechanisms also contribute by enforcing access control and integrity protection on constrained devices, reducing opportunities for unauthorized actions that may trigger or mask anomalies [67]. **Consumer IoT** addresses the security of connected devices and systems in everyday smart home environments. Within the anomaly detection context, research emphasizes traffic flow monitoring at the network layer and device behavior analysis to identify irregularities and detect emerging threats in consumer IoT systems [68,69].

Table 6. Top Cited Publications in the Anomaly Detection community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
A survey of intrusion detection in Internet of Things [31]	Zarapelão et al. (2017)
IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices [33]	Meneghello et al. (2019)
A Supervised Intrusion Detection System for Smart Home IoT Devices [53]	Anthi et al. (2019)
Flexible technologies and smart clothing for citizen medicine, home healthcare, and disease prevention [70]	Axisa T.D. et al. (2005)
IoT privacy and security challenges for smart home environments [66]	Lin H., Bergmann N.W. (2016)

4.3. Trust Management in the IoT

The third largest community is trust management in the IoT, with 1263 papers written by 938 authors from 2006 to the time of fetching these data (April 2025). As shown in Figure A3, six sub-communities are detected for this community. The top most cited works in this community are summarized in Table 7.

Trust and Adoption Barriers is the largest sub-community and examines how non-technical factors influence the acceptance of smart home systems. Research in this domain highlights that users' trust, privacy concerns, and perceptions of usefulness strongly shape

whether they choose to adopt smart home technologies. Studies consistently show that worries about data exposure, loss of control, and uncertainty about service providers can limit adoption, underscoring the importance of designing smart homes that are transparent, respectful of user concerns, and easy to trust [71,72].

The **Elder Security and Monitoring** and **Smart Assistive Healthcare** sub-communities collectively explore how smart home technologies support the safety, health, and independence of older adults and individuals with chronic conditions. Research in this area examines sensor-based systems, such as fall detectors, motion sensors, and unobtrusive activity monitors, that help users live securely at home or in assisted care settings. Studies highlight that acceptance of these technologies depends on factors like privacy, usability, and perceived personal need, while health-oriented applications emphasize long-term monitoring, improved daily activity tracking, and early detection of potential health issues [73,74]. The **Trust and Privacy** sub-community focuses on how the collection and monitoring practices in smart homes shape users' sense of safety, control, and acceptance. Research in this area highlight growing concerns about surveillance, unauthorized data sharing, and the potential misuse of personal information, which can reduce trust and affect adoption decisions [75,76].

The **Ethical and Inclusive Trust Design** sub-community examines how smart home technologies can be developed in ways that respect users' identities, abilities, and values. Research highlights that experiences with smart homes vary across gender, disability, and cultural backgrounds, shaping perceptions of trust, usability, and fairness. Studies point to the importance of inclusive and equitable design practices to ensure that smart homes support diverse users without reproducing existing social or accessibility barriers [77].

The **Multimodal Monitoring and Security** sub-community investigates how smart home systems combine several types of sensor inputs to improve reliability, reduce false alarms, and support privacy-aware incident detection. Research in this area examines how heterogeneous devices can cross-check each other's signals, coordinate responses to unusual events, and maintain strong privacy safeguards while enabling dependable safety automation [78,79].

Table 7. Top Cited Publications in the Trust Management in IoT sub-community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Social barriers to the adoption of smart homes [80]	Balta-Ozkan et al. (2013)
Benefits and risks of smart home technologies [71]	Wilson C. et al. (2017)
Technologies for an aging society: a systematic review of “smart home” applications [81]	Demiris G., Hensel B.K. (2008)
Senior residents' perceived need of and preferences for “smart home” sensor technologies [73]	Demiris G. et al. (2008)
User acceptance of smart home services: An extension of the theory of planned behavior [72]	Yang H., Lee H., Zo H. (2017)

4.4. Access Control and Authorization

The Access Control and Authorization community comprises 1078 papers authored by 753 individuals. These articles were published between 2011 and the date of this study. Seven sub-communities are detected for this community (see Figure A4). The top articles based on the amount of citations are given in Table 8.

Articles in the sub-community of **Anomaly-Based Access Control** focus on detecting unauthorized or abnormal behaviors by modeling legitimate device or network activity and identifying deviations that may indicate threats. Research in this area develops

adaptive, lightweight access control mechanisms suitable for the dynamic and resource-constrained nature of smart home environments, using network-traffic monitoring and behavior-based intrusion detection frameworks designed for IoT contexts [82]. Among the sub-communities of this field, **Blockchain Access Control** appears to be the most trending topic (see Figure A15). This sub-community explores decentralized approaches for managing identity, authorization, and data integrity in smart home environments. Research in this area uses blockchain to create tamper-resistant and privacy-preserving access control mechanisms that operate without relying on a centralized authority. These systems aim to improve trust, prevent data manipulation, and support secure device interactions in heterogeneous smart home settings [29,83].

Table 8. Top Cited Publications in Access Control and Authorization sub-community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Blockchain for IoT security and privacy: The case study of a smart home [29]	Dorri et al. (2017)
Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices [84]	Zhao et al. (2020)
Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices [85]	Eskandari et al. (2020)
Network-level security and privacy control for smart-home IoT devices [86]	Sivaraman et al. (2015)
A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow [82]	Nobakht et al. (2016)

The **Blockchain Cryptography** subcommunity explores how blockchain can help create lightweight and scalable security methods for IoT devices with limited resources. Research in this area focuses on decentralized and certificate-free ways of managing keys and controlling access, aiming to improve security while supporting the diverse and low-power devices found in smart home environments [87,88].

Blockchain Coordination has emerged as a distinct sub-community that examines how blockchain can be used to coordinate access control and authorization across smart home devices. Research in this area focuses on decentralized and secure frameworks that manage device identity, user permissions, and data exchange without relying on a central authority. These approaches aim to improve trust, scalability, and resilience against malicious activity in heterogeneous smart home environments [89]. Studies in the **Sensing and Control** sub-community examine how smart home systems interpret sensing data to understand household context and trigger appropriate automated responses. This work focuses on enabling reliable, unobtrusive automation that aligns with user routines and supports secure system behavior [90]. Articles in the sub-community of **Secure System Integration** are about making the whole smart home secure as one system, so sensors, gateways, edge devices, and cloud services all follow the same access rules end-to-end. In practice, this work locks down home gateways and control apps; pushes more decision-making to the edge for quicker, more private responses; and strengthens back-end storage, often in ways that ensure data stays protected and every access can be audited [91,92].

The **Intrusion Detection** sub-community within access control and authorization is the smallest in this field and focuses on detecting abnormal or unauthorized activities that directly affect permission enforcement. Unlike broader intrusion detection efforts that analyze network-wide behavior, this work concentrates on identifying threats at the device or edge level so that suspicious actions can be blocked before they escalate. These

approaches help prevent unauthorized operations before they compromise the integrity of smart home systems [85].

4.5. Vulnerability Detection

The Vulnerability Detection community comprises 1010 papers authored by 742 researchers since 2004. Six sub-communities are identified for this community (see Figure A5). An overview of the most cited works in this domain is provided in Table 9.

The **Sensor Networks** sub-community examines how smart homes use networks of sensors and wireless communication methods to operate securely and reliably. Research in this area focuses on creating low-power and dependable sensing systems that keep data transmission stable, allow many devices to work together smoothly, and support continuous monitoring across different types of smart home technologies [93,94].

The **Microcontroller-Based Authentication Systems** sub-community, as the second largest sub-community within this domain, focuses on hardware-driven approaches to securing smart homes. Research in this area leverages low-cost microcontroller platforms to support lightweight authentication and access control, often using biometric or sensor-based verification methods suitable for devices with limited processing power [95,96]. Research in the **Energy-Efficient Architectures** sub-community focuses on smart home systems that aim to reduce energy consumption while incorporating lightweight security features. Recent work reflects a growing interest in hardware-aware designs that balance performance, sustainability, and protection for resource-constrained devices in smart homes [97].

Under the **Authentication and Sensing** sub-community, researchers investigate how biometric and behavioral cues captured through smart home sensing systems can help identify vulnerabilities and detect unauthorized access. Research in this area focuses on unobtrusive, continuous authentication methods that rely on users' natural interaction patterns to distinguish legitimate occupants from intruders, offering more resilient alternatives to traditional password-based approaches [98,99]. Articles in the **Lightweight Communication Protocols** sub-community examine how low-power messaging methods used in smart homes can introduce security vulnerabilities and how these communication channels can be strengthened. Research highlights challenges in securing device interactions, detecting misuse, and preventing unauthorized access while keeping systems simple and efficient [100,101]. The **Trends and Risks in Smart Buildings** sub-community takes a broad view of how emerging smart building technologies introduce new security and privacy challenges. Research in this area highlights issues related to rapid adoption, increasing system complexity, and the expansion of connected services, which can widen the attack surface and expose vulnerabilities if not properly managed [102,103].

Table 9. Top Cited Publications in Vulnerability Detection Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
A ZigBee-based home automation system [93]	Gill et al. (2009)
Deep learning enabled smart mats as a scalable floor monitoring system [98]	Shi et al. (2020)
IoT based smart security and home automation system [104]	Kodali et al. (2017)
A novel secure IoT-based smart home automation system using a wireless sensor network [97]	Pirbhulal et al. (2017)
Raspberry Pi as a Sensor Web node for home automation [105]	Vujović V. and Maksimović M. (2015)

4.6. Privacy-Preserving and Authentication

The Privacy-Preserving and Authentication community contains 1118 articles published from 2002 to 2025 divided across 7 sub-communities, as seen in Figure A6. An overview of the most cited works in this domain is provided in Table 10.

The **Wireless Authentication and Protocols** sub-community, the largest in this community, focuses on lightweight methods that enable smart home devices to authenticate each other securely while preserving user privacy. Research in this sub-community explores mutual authentication and key-establishment techniques designed to work on low-power devices and within dynamic home networks. Many approaches use intermediary gateways or privacy-enhancing mechanisms to limit identity exposure and reduce the risk of unauthorized access [106,107].

The **IoT Systems Privacy** sub-community focuses on protecting sensitive data and securing communication within smart home IoT environments. Research in this area develops lightweight and energy-efficient privacy mechanisms that limit data exposure, reduce the risk of traffic analysis, and support secure device communication under resource constraints. These approaches often emphasize simple key-management strategies and privacy-enhancing designs that can operate effectively on low-power devices [108,109].

Works in the **IoT Permissions** sub-community develop privacy-aware authentication and communication models for smart homes, aiming to support secure device interactions while preserving user privacy. They have proposed decentralized or blockchain-based mutual authentication schemes and privacy-preserving communication protocols that seek to protect device identity and data confidentiality without central trust dependencies [110,111]. The **Authentication and ECC** sub-community investigates lightweight authentication mechanisms that rely on elliptic-curve cryptography (ECC), a public-key technique that provides strong security with minimal processing requirements. This makes ECC suitable for smart home devices with limited resources. Research in this area focuses on securing device interactions, protecting user privacy, and resisting common attacks while keeping authentication efficient and scalable [112,113].

The **Anti-Tracking and Key Management**, **Activity Recognition**, and **Gateway Privacy** sub-communities all address how to limit data exposure and protect user privacy in resource-constrained smart home environments. The first focuses on preventing linkability and securing key establishment so devices cannot be tracked across sessions (e.g., [114]). The second explores non-intrusive sensing methods that infer activities while keeping behavioral data local and confidential (e.g., [115]). The third strengthens privacy at the network boundary by enforcing strict access controls on the home gateway and reducing unnecessary external communication (e.g., [116]). Together, these efforts form a coordinated approach to minimizing what external parties can learn about users and their households.

Table 10. Top Cited Publications in Privacy-Preserving and Authentication Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes [108]	Song et al. (2017)
A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) [117]	Almusaylim Z.A. and Zaman N. (2019)
Securing IoT for smart home system [106]	Santoso F. and Vun N. (2015)
Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments [118]	Kumar et al. (2015)
HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes [111]	Lin et al. (2019)

4.7. User Security and Privacy

The User Security and Privacy community contains 952 papers authored by 567 researchers from 2006 to 2025 and is divided into five distinct sub-communities (Figure A7). Table 11 summarizes the leading contributions shaping research in this field.

The Home Automation Threats sub-community examines the security and privacy risks that emerge when smart home technologies are embedded into everyday domestic life. Research in this area highlights how system design, shared household environments, and long-term monitoring can create tensions around autonomy, control, and data exposure for different types of users [119,120]. Studies in this field consistently show that while home automation promises convenience and support, it also introduces new social and technical vulnerabilities that must be addressed to ensure safe and equitable adoption.

Table 11. Top Cited Publications in User Security and Privacy Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home) [121]	Kepuska V. and Bohouta G. (2018)
User perceptions of smart home IoT privacy [122]	Zheng et al. (2018)
Home automation in the wild: Challenges and opportunities [119]	Brush et al. (2011)
Music, Search, and IoT: How people (really) use voice assistants [123]	Ammari et al. (2019)
End user security and privacy concerns with smart homes [124]	Zeng et al. (2019)

The Virtual Personal Assistants (VPAs) and Privacy sub-community examines the security and privacy risks that emerge as voice-driven assistants become embedded in everyday smart home routines. Research in this area highlights how features like always-on listening and cloud-based processing can create uncertainty about what data is collected, how it is used, and who ultimately has access (e.g., [121]). Studies also show that many users hold incomplete or overly optimistic assumptions about how these systems work, often underestimating the extent of data exposure and overestimating device protections [125].

The IoT Sensing Threats sub-community examines the privacy and security risks that arise from the growing use of sensing technologies in smart homes. While sensors can provide benefits such as safety, healthcare support, and convenience, research shows that they also create concerns about surveillance, profiling, and loss of personal control over what is observed or inferred. Within this sub-community, studies highlight that acceptance often depends on how intrusive different types of sensors feel, and that the increasing complexity of sensing systems can make it difficult for users to understand or manage the data being collected [126,127]. Broader work in this area also points to social tensions, showing how sensing technologies may reinforce or amplify existing household inequalities and privacy expectations, particularly when they intersect with caregiving roles or control dynamics (e.g., [128,129]).

The Non-user Privacy Threats sub-community examines the risks faced by bystanders in smart homes: individuals such as guests, children, tenants, and domestic workers who are present in these environments but are not primary users. Research shows that bystanders often have limited awareness, agency, or control over the data collected about them, creating privacy vulnerabilities that differ from those of device owners. Studies highlight recurring issues around consent, visibility, and power imbalances, where bystanders may be monitored without clear knowledge or meaningful ability to object (such as [130,131]). The last sub-community of this community, named **Device security and Privacy Notices**, focuses on how smart home devices communicate security risks, data

practices, and protective measures to users. Research highlights that many devices still rely on weak or unclear communication, leaving users uncertain about how their data is handled or shared [132]. Other studies show that the design of privacy notices, which is about how information is presented and when it appears, shapes how users interpret a device's data practices (e.g., [133]). Overall, this sub-community stresses that privacy notices should offer transparent and timely explanations of how smart home devices handle data.

4.8. Visibility and Traffic Analysis

The Visibility and Traffic Analysis community comprises 368 papers authored by 238 researchers beginning in 2007 and organized into seven sub-communities (Figure A8). Table 12 summarizes the most cited works in this field.

Within the Visibility and Traffic Analysis community, **Traffic Classification** is the predominant sub-community. It focuses on methods for identifying IoT devices and inferring their behavior from observable network traffic patterns, even when the traffic is encrypted. Recent work explores ML-based approaches that analyze flow characteristics to distinguish between devices and applications, supporting better monitoring and anomaly detection in smart home environments [35,134].

Table 12. Top Cited Publications in Visibility and Traffic Analysis Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics [35]	Sivanathan et al. (2019)
Ensemble machine learning approach for classification of IoT devices in smart home [135]	Cvitić et al. (2021)
DEFT: A Distributed IoT Fingerprinting Technique [136]	Thangavelu et al. (2019)
An Efficient Spam Detection Technique for IoT Devices Using Machine Learning [137]	Makkar et al. (2021)
Identifying IoT devices and events based on packet length from encrypted traffic [134]	Pinheiro et al. (2019)

The **Forensics** sub-community examines how smart home assistants, such as voice-controlled devices, can be analyzed in digital investigations. Research in this area highlights both the security vulnerabilities of these systems and the potential of device logs and interaction traces to reconstruct user activities or identify malicious behavior [138,139]. Complementing this perspective, the **Privacy in Network** sub-community focuses on mitigating information leakage from IoT traffic, recognizing that even encrypted communications can reveal sensitive behavioral details [140,141]. Studies in this area explore adaptive encryption and traffic obfuscation to limit what can be inferred from network observations while maintaining communication efficiency.

The smaller sub-communities within this community address complementary aspects of securing IoT networks. **Smart Home Resilience** research explores mechanisms that help home services remain reliable during disruptions or cyber attacks [142], while **Threat Intelligence** studies examine how IoT threats can be contextualized and tracked to uncover vulnerabilities and support proactive defenses [143]. In parallel, work on **Deep Learning for IoT Attack Detection** applies neural models to identify malicious behaviors from traffic patterns [144], while the **ML-based IoT Security** sub-community uses traditional machine-learning techniques for broader detection and classification tasks in smart home networks [137]. Together, these efforts reflect a broader trend toward data-driven methods that strengthen visibility, resilience, and adaptive defense in IoT environments.

4.9. Edge-Based Localization and Recognition

This community examines the security and reliability of wireless sensing technologies deployed in smart environments. It emphasizes device-free localization, occupancy detection, gesture recognition, and human activity recognition (HAR), which collectively enable non-intrusive sensing for security and automation within smart homes. This community includes 274 papers published between 2012 and 2024, grouped into six sub-communities (see Figure A9). Table 13 highlights the most cited works in this field.

Table 13. Top Cited Publications in Edge-Based Localization and Recognition Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review [145]	Majid et al. (2022)
Dynamic-MUSIC: Accurate device-free indoor localization [146]	Li et al. (2016)
Device-Free Occupant Activity Sensing Using WiFi-Enabled IoT Devices for Smart Homes [147]	Yang et al. (2018)
RASID: A robust WLAN device-free passive motion detection system [148]	Kosba et al. (2012)
Continuous Authentication through Finger Gesture Interaction for Smart Homes Using WiFi [149]	Kong et al. (2021)

Angle-of-Arrival (AoA) Localization uses directional signal information to estimate where transmissions originate. This technology can enable location-aware security functions [150]. **Channel State Information (CSI) Occupancy Sensing** detects human presence by observing variations in WiFi signals and supports presence-aware access control [147]. **Device-Free Localization** extends this approach by estimating a person's position or movement without requiring wearables or cameras [148]. Building on these capabilities, **WiFi-based Human Activity Recognition (HAR)** identifies common daily activities for safety and behavioral monitoring [151], while **CSI Gesture Recognition** focuses on recognizing hand and body gestures for touchless interaction and authentication [152]. The final sub-community of this community, **Cross-Person HAR**, focuses on recognizing activities in a way that works for new users without needing extra setup or training for each person, often combining with practical deployment on low-cost hardware (e.g., Raspberry Pi) [153]. Together, these sub-communities show how edge-based wireless sensing, through localization and recognition, can offer low-cost, non-intrusive, and privacy-aware security features in smart homes.

4.10. Cloud Integration and Security

The cloud integration and security community examines how cloud and fog infrastructures support secure data processing, communication, and service delivery in smart home environments. This community is divided into six sub-communities (Figure A10) and includes 234 papers published between 2010 and 2024. Table 14 summarizes the most influential studies shaping research in cloud-integrated smart home security.

Remote Health Monitoring sub-community examines how cloud and fog infrastructures support secure, real-time health monitoring in smart homes, with work focusing on continuous sensing, emergency alerts and resilient architectures for medical IoT data [154]. **Fog and Healthcare Gateways** is one of the most active sub-communities and explores fog-based gateways that process health and sensor data close to the user, such as body sensors, to reduce latency and strengthen privacy protections (e.g., [30]). The third sub-community, **Threat Analysis Frameworks**, develops structured tools for identifying risks

in cloud-connected smart homes. Research here includes modeling techniques that help evaluate attack paths and system vulnerabilities [155]. In **Protocol Security and Privacy** sub-community, weaknesses in communication protocols within cloud-connected smart homes are investigated. Studies propose approaches to secure data exchange while preserving user privacy [156]).

The **Energy-aware Monitoring** sub-community focuses on how cloud integration can support energy-efficient and context-aware smart home systems. Research has highlighted the role of adaptive sensing and cloud-based processing in balancing security, performance, and sustainability [157]. The last and smallest sub-community within this community is the **Fog Security Reviews** sub-community, with only two papers. It provides high-level examinations of how fog architectures can address security and latency challenges in smart homes [158,159].

Table 14. Top Cited Publications in Cloud Integration and Security Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach [30]	Rahmani et al. (2018)
Securing Fog Computing for Internet of Things Applications: Challenges and Solutions [36]	Ni et al. (2017)
Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems [160]	Rahmani et al. (2015)
SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways [161]	Moosavi et al. (2015)
Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review [154]	Talal et al. (2019)

4.11. Behavioral Biometrics and Sensing

The Behavioral Biometrics and Sensing community examines how smart homes leverage behavioral patterns, sensing techniques, and embedded technologies to support secure and adaptive interaction. This community consists of 82 publications (2005–present), which the Louvain algorithm groups into four sub-communities (see Figure A11). In addition, Table 15 summarizes the most influential publications contributing to the Behavioral Biometrics and Sensing community.

The **Automation Platforms** sub-community looks at how IoT platforms integrate devices, data flows, and services into unified smart home environments. Research in this field provides the foundations for secure and adaptable operation [162]. The focus of studies in the **Embedded Resilience** sub-community shifts to the embedded devices that quietly power smart home infrastructures. Core concepts among the studies include strengthening the security of sensors, micro-controllers, and other embedded components through vulnerability analysis and cybersecurity-by-design practices [163].

The **Biometric Protocols** sub-community, on the other hand, emphasizes securing smart homes through behavioral and biometric authentication methods. Key approaches include continuous user verification, gesture-based recognition, and activity-driven identity confirmation. Studies in this area demonstrate how authentication can move beyond passwords and tokens to enhance both security and user experience [149,164]. Finally, **Non-invasive Sensing** is about monitoring or collecting information without requiring direct contact with sensors. In smart homes, this technology can be used for activity recognition. The papers within this sub-community explore the use of radar, WiFi, and other wireless signals to capture motion patterns in a privacy-preserving manner [165,166]. While closely

related to contactless authentication techniques (Section 4.1), the focus here is on interpreting daily behaviors and well-being rather than verifying identity and access control.

Table 15. Top Cited Publications in Behavioral Biometrics and Sensing Community. Row shading is used to improve readability and does not convey additional information.

Title	Authors (Year)
Continuous Authentication through Finger Gesture Interaction for Smart Homes Using WiFi [149]	Kong et al. (2021)
Noninvasive Human Activity Recognition Using Millimeter-Wave Radar [165]	Yu et al. (2022)
A new framework architecture for next generation e-health services [167]	Fengou et al. (2012)
Human Activity Recognition (HAR) Using Deep Learning: Review, Methodologies, Progress and Future Research Directions [168]	Kumar et al. (2024)
Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends [169]	Aldahmani et al. (2023)

4.12. Hardware-Accelerated AIoT Security

The Hardware-Accelerated AIoT Security sub-community is a small and highly specialized cluster represented by two closely related papers, one with 36 and the other one with 32 authors, originating from the VEDLIoT project [170,171]. These works focus on designing energy-efficient and secure cryptographic mechanisms tailored to AIoT hardware, with an emphasis on combining high-performance machine learning with lightweight security techniques. Because these studies are tightly connected and do not intersect with the broader smart home security landscape, this sub-community appears isolated from other research areas in the smart home security field.

5. Discussion

The purpose of this study was to demonstrate how research on smart home security has evolved and organized itself into research communities and identify the main thematic directions shaping the field. The analysis shows that the field does not form one unified line of work but is divided into several distinct directions. Technical topics, such as intrusion detection, access control, and device-level vulnerabilities, form the most internally connected groups, reflecting consistent methods and shared terminology across studies. In contrast, work related to user behavior, privacy practices, and broader socio-technical issues is more distributed across communities, indicating a wider variety of approaches and less direct cross-citation among authors.

The annual publication trend shows a steady increase in research activity beginning in the early 2010s and accelerating sharply after 2015. This growth can be interpreted in light of the widespread adoption of consumer IoT devices, increased connectivity within home environments, the ability of smart home technologies to reduce living costs through improved energy and heating efficiency, and growing awareness of security and privacy risks, all of which have expanded the attack surface of smart homes. As smart home deployments became more common and technically complex, the need for scalable and automated security mechanisms became more apparent, particularly in environments with heterogeneous devices and communication patterns. The expansion is reflected most strongly in technical research streams, which form the largest and most cohesive communities in the dataset. These clusters, centered on intrusion detection, access control, and device-level vulnerability analysis, show consistent development over time, with sustained publication activity

and dense citation patterns. In particular, the prominence of data-driven and machine learning-based approaches aligns with advances in edge computing and the increased availability of network traffic datasets, which enable the practical experimentation and deployment of such techniques.

The results of this study align with several observations made in earlier reviews. Solaimani et al. [10] and Marikyan et al. [11] noted that smart home research is fragmented and that technical studies dominate the field; the community structure in our analysis provides quantitative support for this pattern, with large, cohesive technical clusters and smaller, more dispersed socio-technical ones. Consistent with these observations, Arabo [15] and Plachkinova et al. [14] reported limited integration of privacy and user-centered work into mainstream security research, which is reflected in the weak citation links between these themes across communities in the community graph (see Figure 3). Beyond differences in research focus, the structure of the community graph suggests practical relationships between research areas, where studies on network visibility and traffic analysis provide the basis for later work on anomaly detection and intrusion response. This pattern is also visible in the dominance of a small group of active researchers and established publication venues within the largest technical communities. In addition, in several large technical communities, sub-community analysis highlights the presence of multiple distinct methodological approaches that are not apparent at the community level alone, such as different intrusion detection techniques, authentication mechanisms, and privacy-focused methods.

Within the technical communities, ML-based intrusion detection remains one of the most active directions, reflecting continued methodological development and sustained citation activity (see Figure A13). More broadly, several sub-communities indicate an increasing reliance on data-driven and AI-based approaches for threat detection, anomaly identification, and adaptive security mechanisms, particularly in more recent publications. Another area showing growing visibility is the use of blockchain-based techniques for access control, cryptography, and coordination within the smart home context (see Figure A15). Although still smaller than intrusion detection-focused work, these topics indicate increasing interest in decentralized security mechanisms for smart home environments. Privacy-preserving methods and user-centered security models are likewise gaining attention, particularly within socio-technical communities (see Figures A17 and A18). However, despite this growth, these areas remain comparatively small and less interconnected across communities than the dominant technical clusters (e.g., see Figure A7). Some degree of overlap between closely related communities is therefore expected, as areas such as intrusion detection, anomaly detection, and traffic analysis often share methods, datasets, and citation practices. Rather than indicating unclear boundaries, this overlap reflects the interconnected and interdisciplinary nature of smart home security research, with communities representing dominant research directions rather than exclusive classifications.

From a practical point of view, the identified research communities show that smart home security research has mainly focused on detection-based solutions such as intrusion and anomaly detection. While these approaches are important, the weaker connection with user-centered and privacy-related communities suggests that current solutions do not always fully consider how people use smart home systems. This highlights opportunities for practitioners, policymakers, and applied researchers to develop security solutions that better combine technical protection with usability and privacy concerns.

6. Conclusions and Future Work

In this study, we addressed the fragmented nature of smart home security research by providing a systematic, data-driven overview of how the field has evolved and organized itself in research communities. By combining SMS methodology with citation-based bibliometric analysis, we applied a scalable approach for mapping the research landscape and identifying its main thematic structures.

The findings show that smart home security research can be described in a set of research communities that represent the main thematic directions of the field. These communities reflect how security challenges, methods, and application contexts are conceptually structured within the literature. The analysis also indicates that these research communities have evolved over time, with noticeable shifts in focus and increasing interaction between research areas. Together, these patterns highlight a dynamic and interconnected research landscape rather than separate and isolated lines of work.

The findings also suggest opportunities for closer integration between technical security solutions and user behavior in smart homes. Greater attention to the combined design of usability, security, and privacy may help address practical deployment challenges and bridge the gap between technical and socio-technical research streams. One important direction for future work is the explicit study of Trigger–Action IoT platforms, which enable user-defined automation across devices and services and introduce distinct security and privacy challenges. While aspects of these systems appear across multiple studies, they are often not examined as a clearly defined research focus in existing smart home security surveys. A second direction concerns Technology-Facilitated Abuse (TFA) in smart home environments, where connected devices and automation may be misused to monitor, control, or harm users. Although related issues are discussed indirectly in privacy and user-centered security research, TFA itself remains underexplored as an explicit security concern in the smart home literature. Overall, this study provides a consolidated view of the smart home security research field that can support future studies by clarifying its structure, evolution, and interconnections and demonstrates that the methodological approach presented here is applicable to other research domains characterized by large and evolving bodies of literature.

Author Contributions: Conceptualization, F.D.A., A.J., K.S.A. and M.H.; Methodology, F.D.A., A.J., K.S.A., K.S. and M.H.; Software, F.D.A. and K.S.A.; Validation, F.D.A., A.J., K.S.A., K.S. and M.H.; Formal analysis, F.D.A., K.S.A. and M.H.; Investigation, F.D.A., A.J., K.S.A., K.S. and M.H.; Resources, F.D.A., K.S.A. and A.J.; Data curation, F.D.A. and K.S.A.; Writing—original draft preparation, F.D.A.; Writing—review and editing, F.D.A., K.S.A., A.J., K.S. and M.H.; Visualization, F.D.A., K.S.A., A.J., M.H. and K.S.; Supervision, A.J., K.S.A., M.H. and K.S.; Project administration, F.D.A.; Funding acquisition, A.J. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The datasets, queries, and source code supporting the findings of this study are available in a public repository at <https://zenodo.org/records/18538858> (accessed on 5 February 2026).

Acknowledgments: During the preparation of this manuscript, the authors used AI-assisted tools for language and grammar polishing. The authors reviewed and edited the output and take full responsibility for the content of this publication.

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

Appendix A. Smart Home Security Sub-Community Graphs

Each figure illustrates a distinct community in this research area and its corresponding sub-communities' connections.

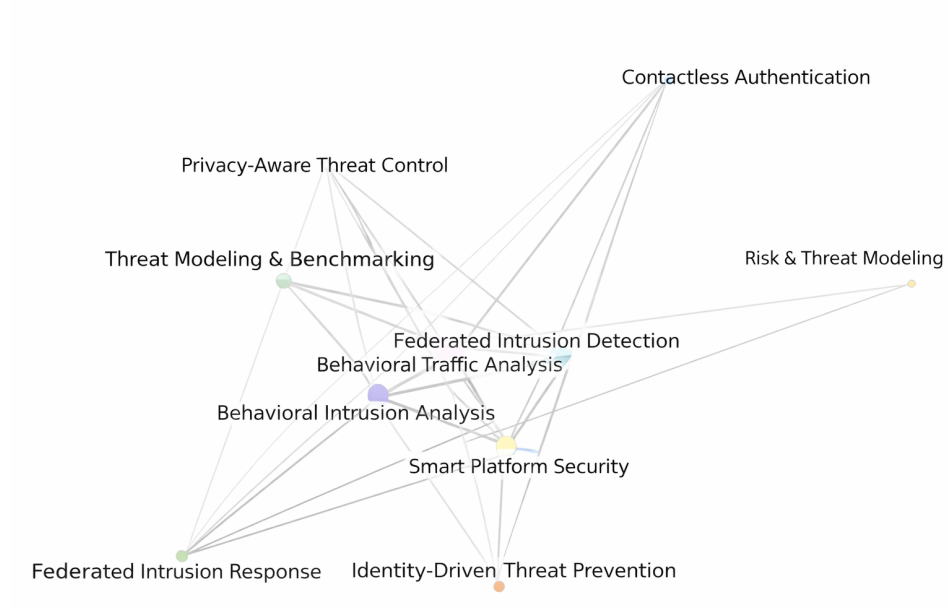


Figure A1. Intrusion Detection and Threat Response.

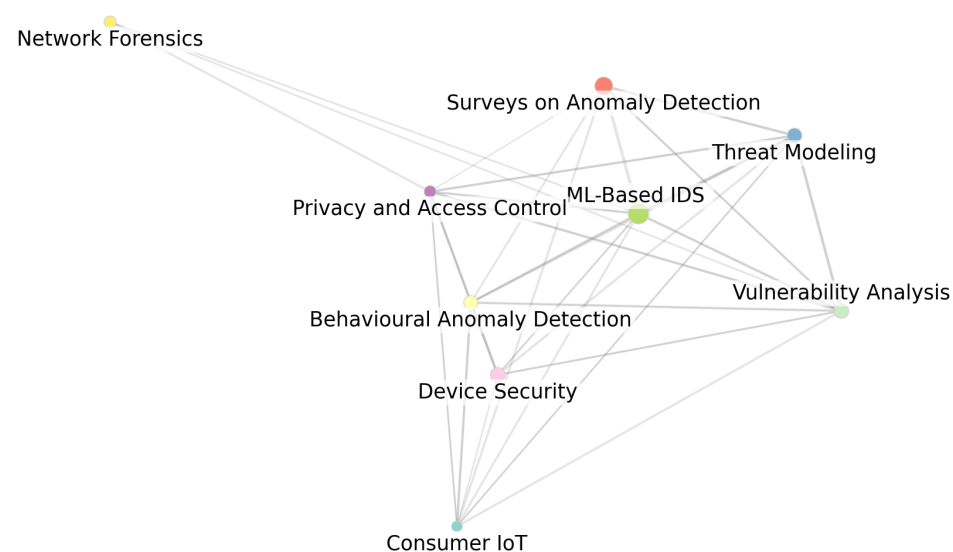


Figure A2. Anomaly Detection.

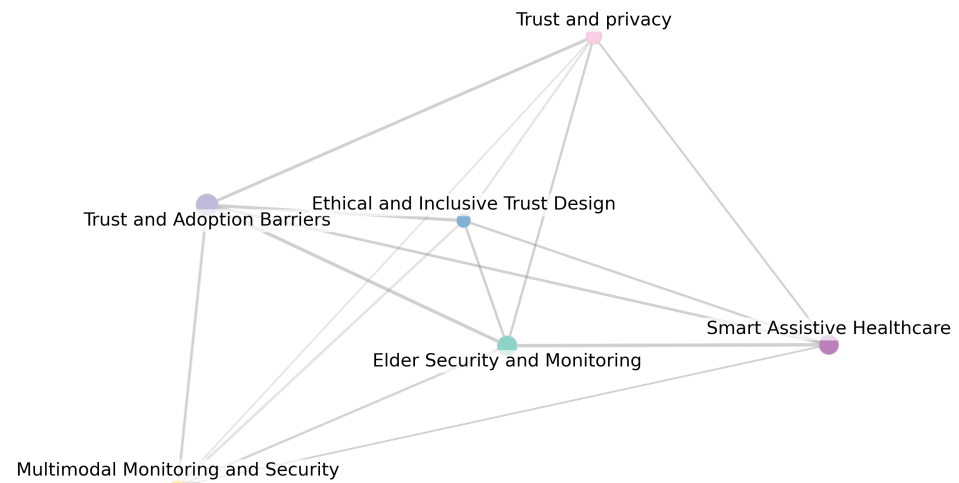


Figure A3. Trust Management in IoT.

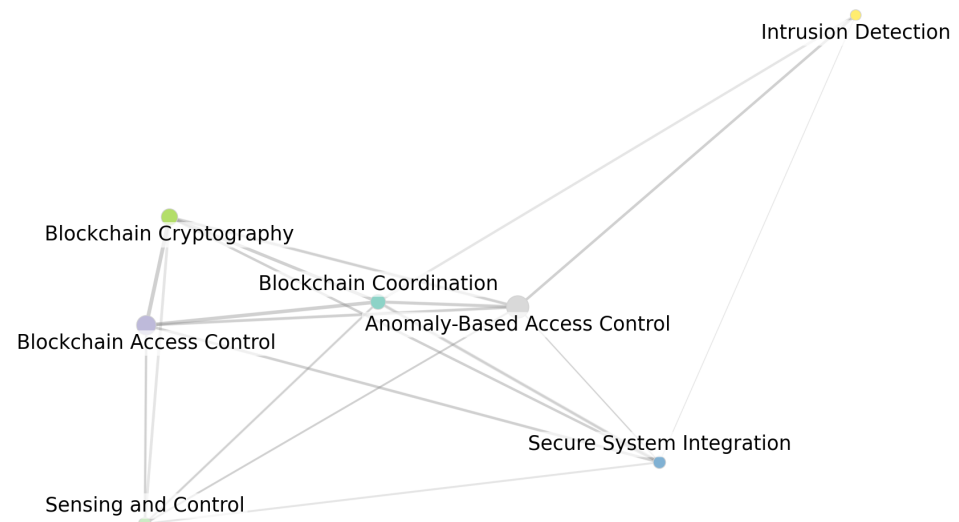


Figure A4. Access Control and Authorization.

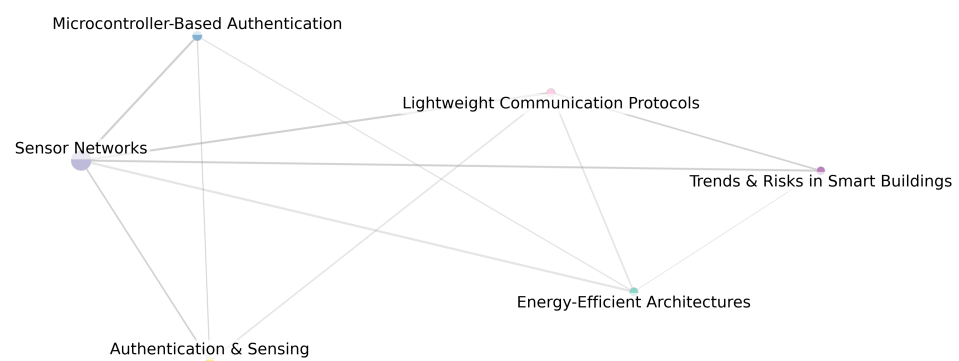


Figure A5. Vulnerability Detection.

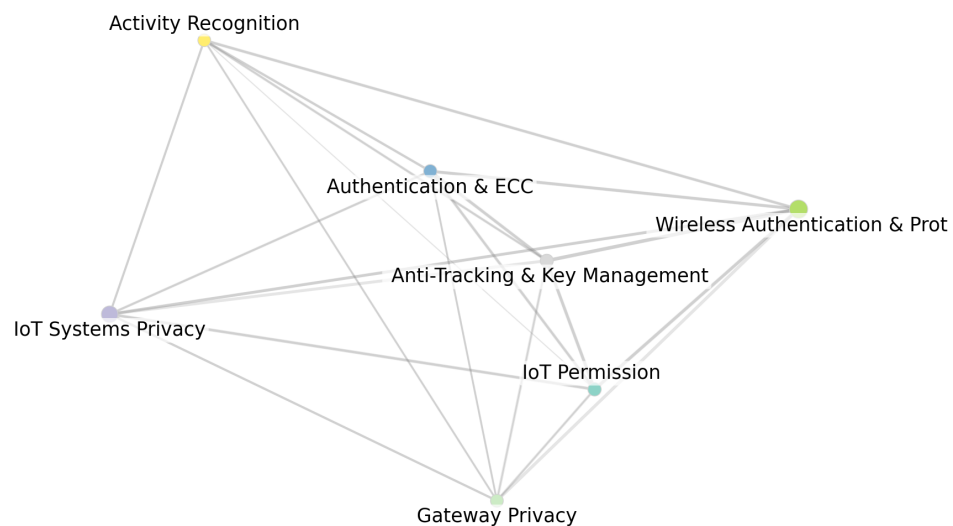


Figure A6. Privacy-Preserving and Authentication.

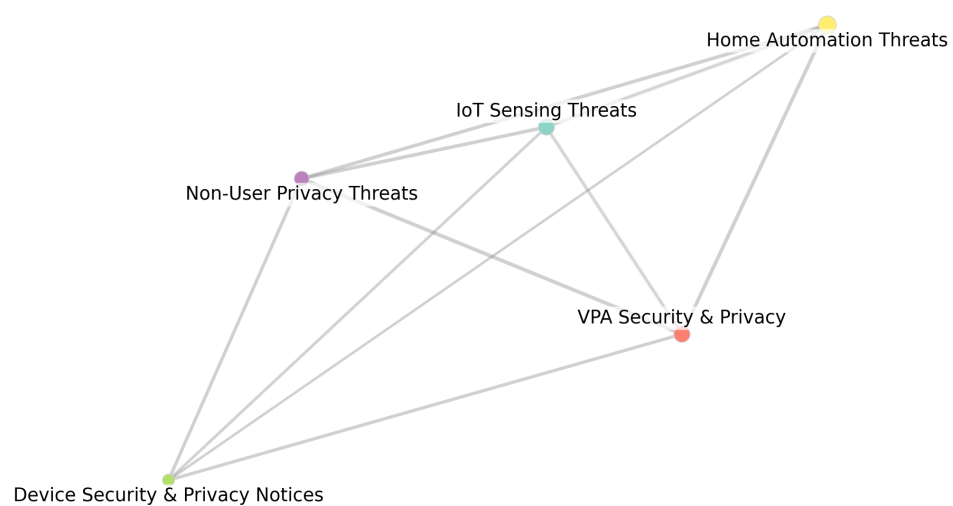


Figure A7. User Security and Privacy.

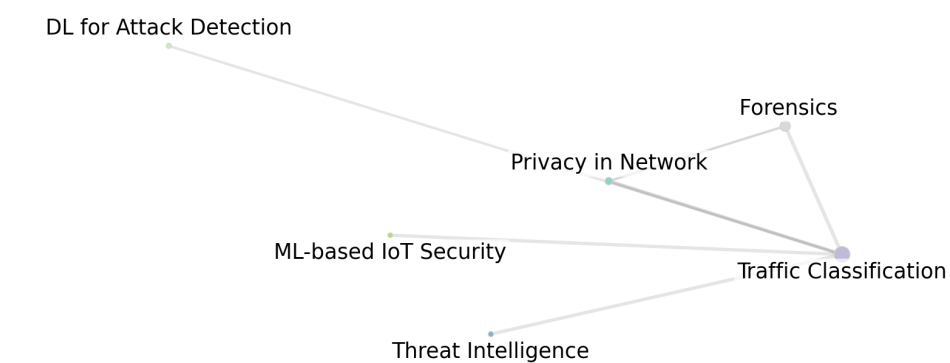


Figure A8. Visibility and Traffic Analysis.

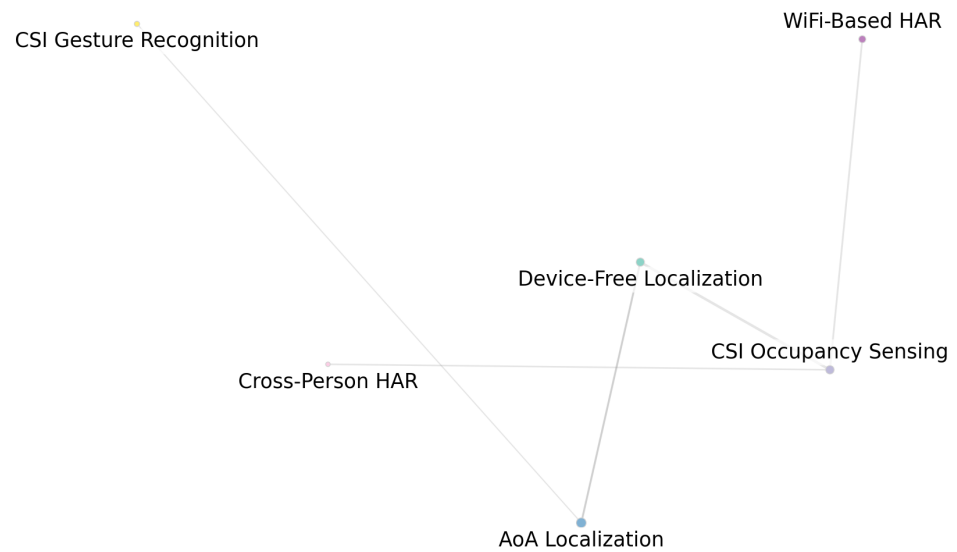


Figure A9. Edge-Based Localization and Recognition.

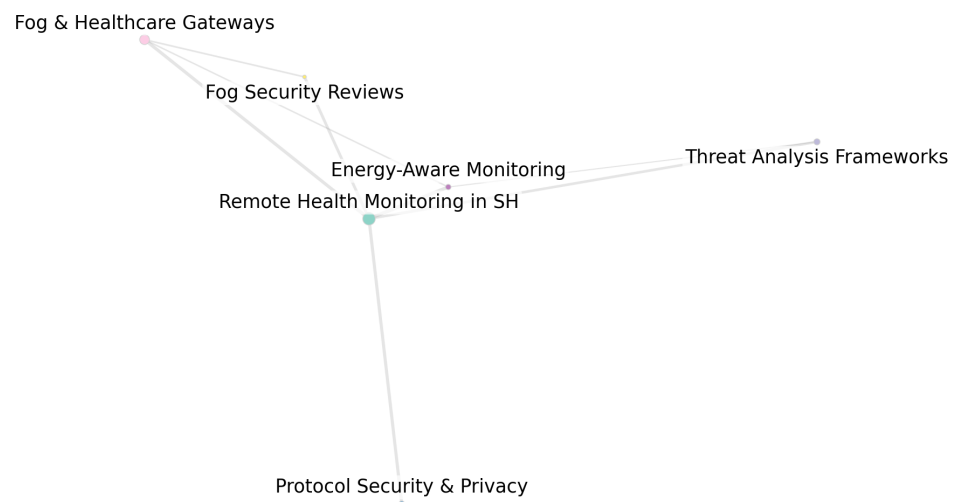


Figure A10. Cloud Integration and Security.

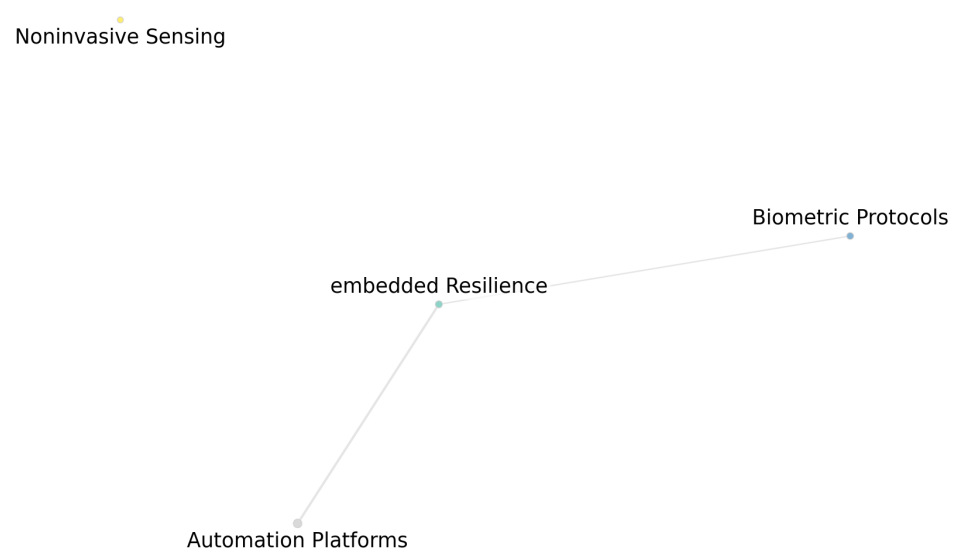


Figure A11. Behavioral Biometrics and Sensing.

Appendix B. Annual Sub-Community Graphs for Smart Home Security

Each figure represents a distinct community and its annual publication count per sub-community.

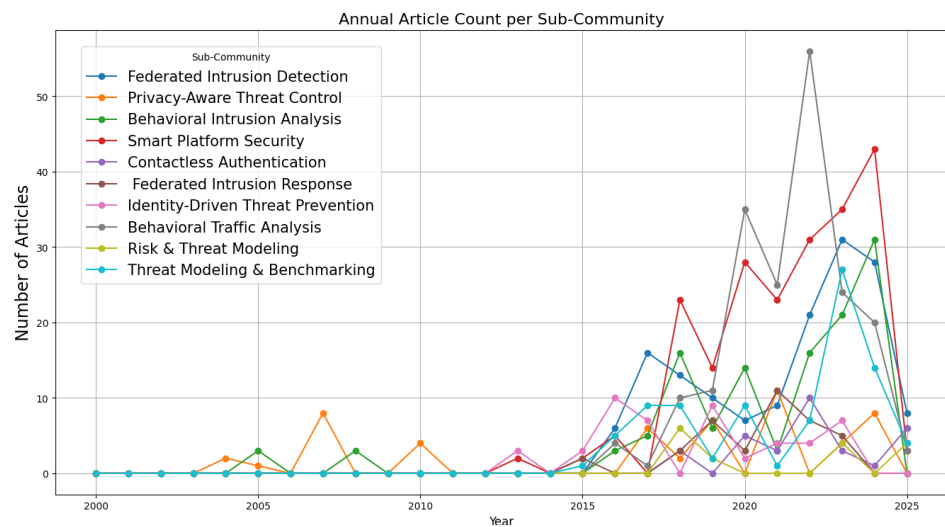


Figure A12. Intrusion Detection and Threat Response.

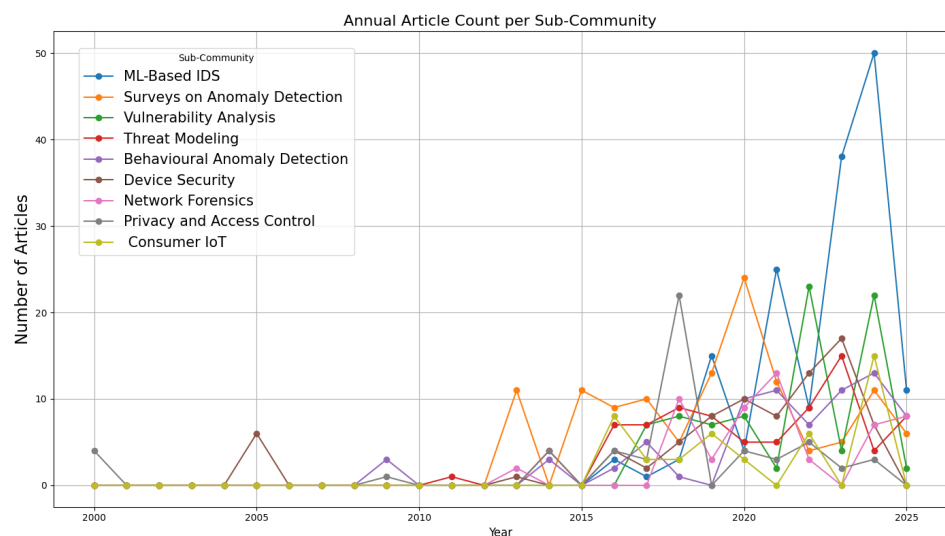


Figure A13. Anomaly Detection.

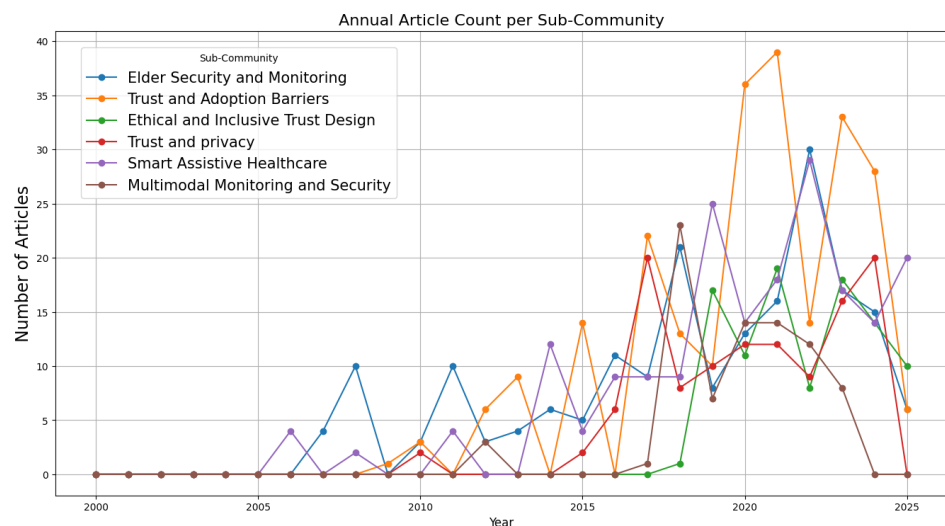


Figure A14. Trust Management.

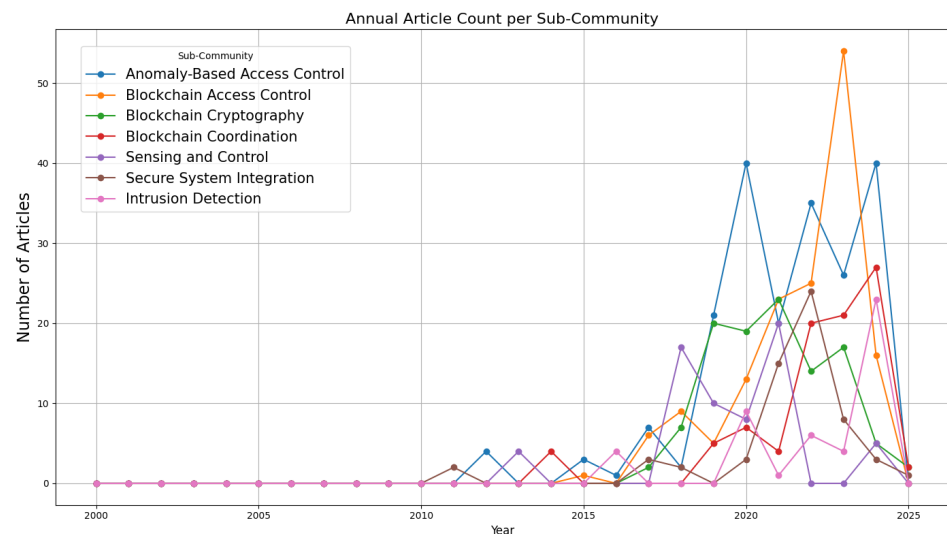


Figure A15. Access Control and Authorization.

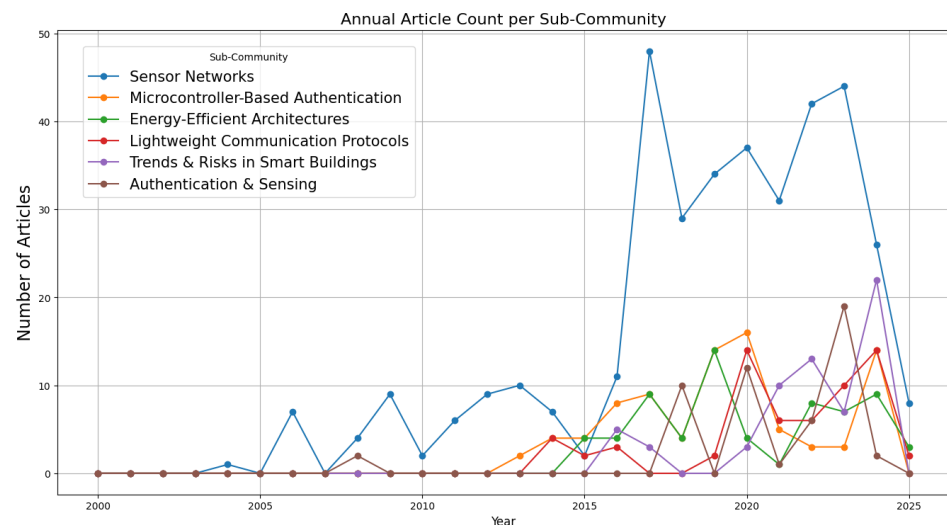


Figure A16. Vulnerability Detection—annual evolution.

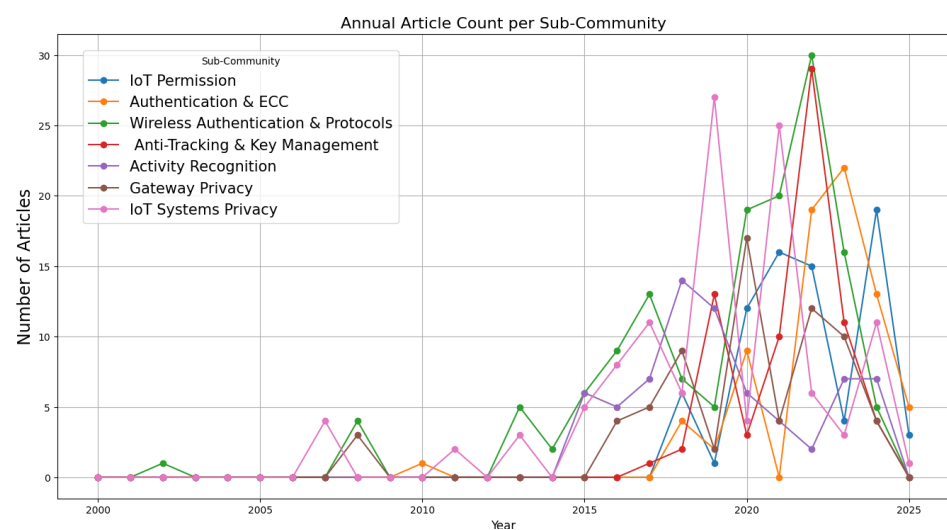


Figure A17. Privacy-Preserving and Authentication—annual evolution.

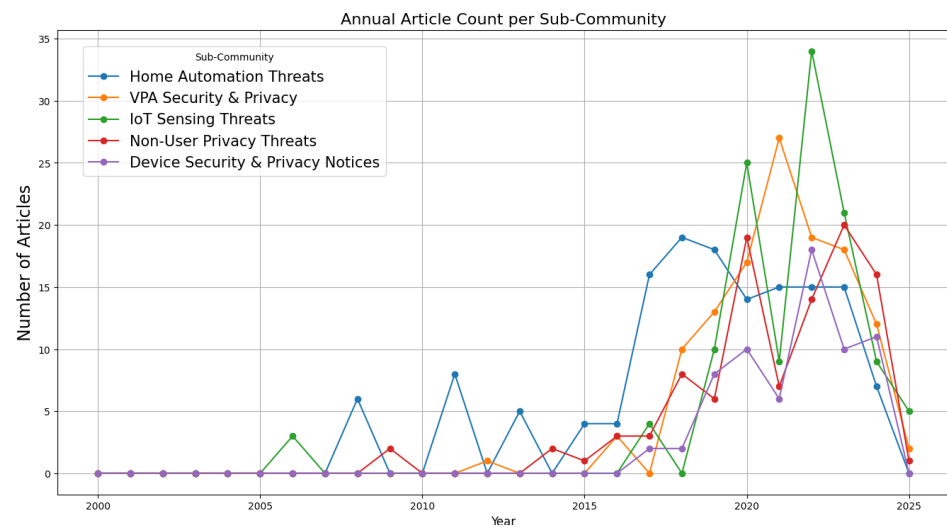


Figure A18. User Security and Privacy—annual evolution.

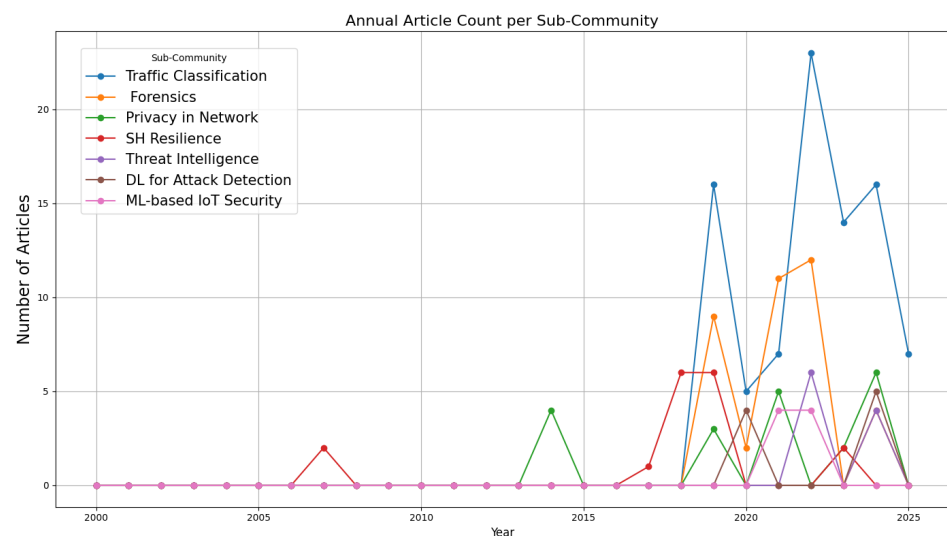


Figure A19. Visibility and Traffic Analysis—annual evolution.

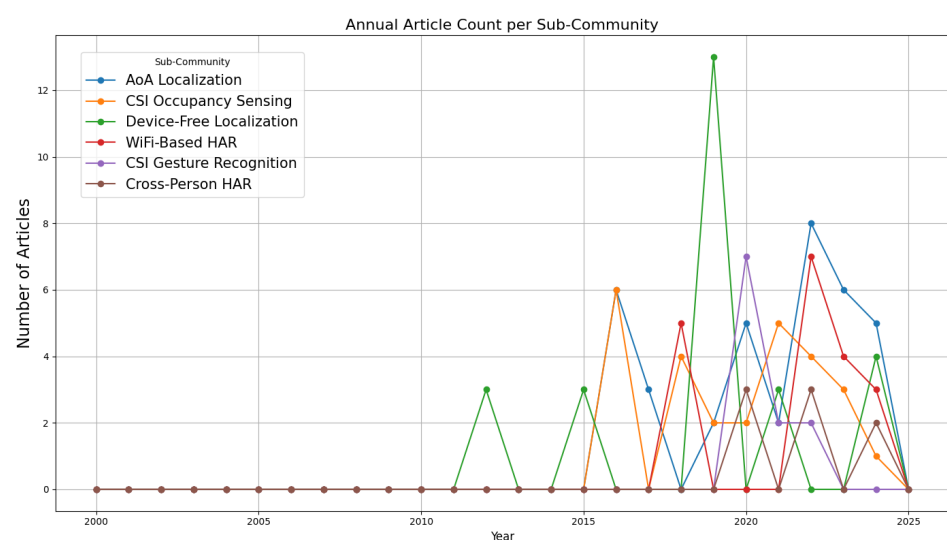


Figure A20. Edge Security—annual evolution.

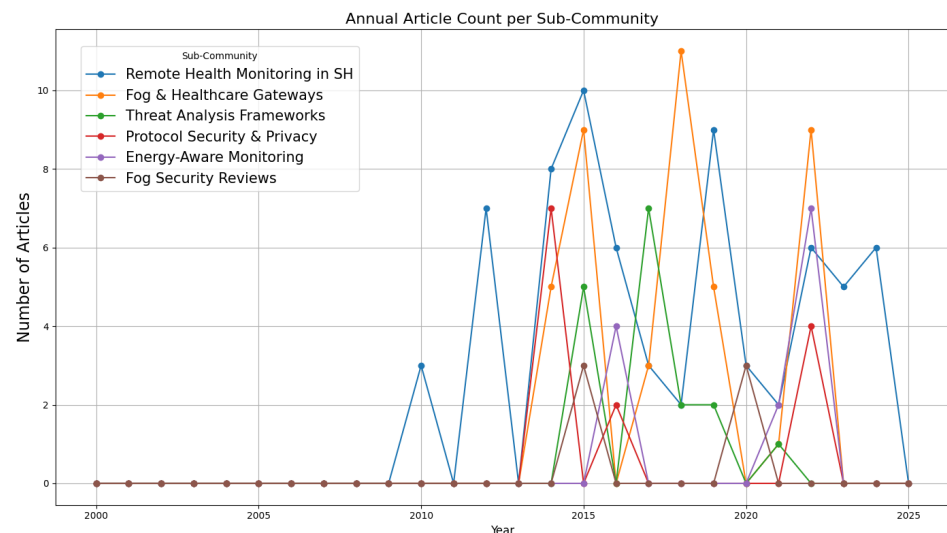


Figure A21. Cloud Integration and Security—annual evolution.

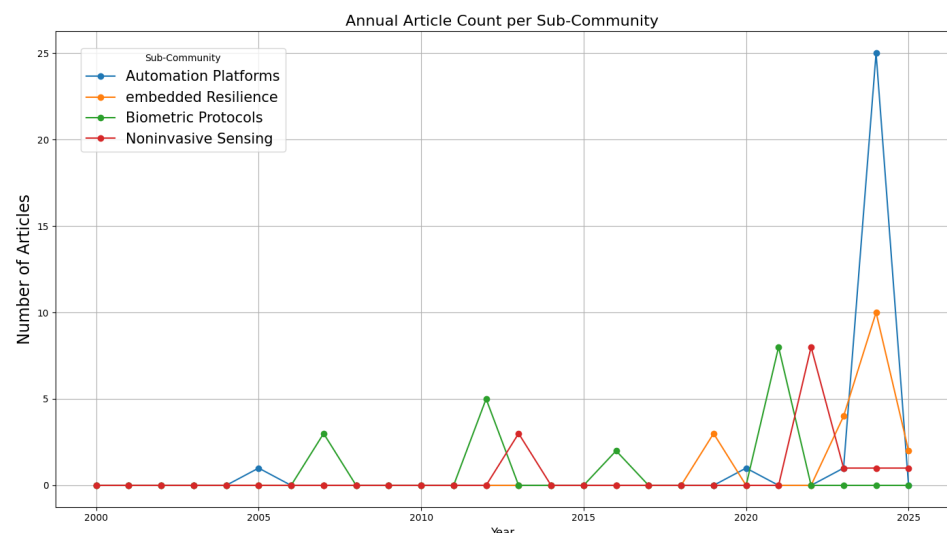


Figure A22. Behavioral Biometrics and Sensing—annual evolution.

References

1. Bugeja, J.; Jacobsson, A.; Davidsson, P. Smart connected homes. In *Internet of Things A to Z: Technologies and Applications*; Wiley: Hoboken, NJ, USA, 2018; pp. 359–384.
2. Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A review of smart homes: Past, present, and future. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* **2012**, *42*, 1190–1203. <https://doi.org/10.1109/TSMCC.2012.2189204>.
3. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035.
4. Batalla, J.M.; Vasilakos, A.; Gajewski, M. Secure smart homes: Opportunities and challenges. *ACM Comput. Surv.* **2017**, *50*, 1–32.
5. Hammi, B.; Zeadally, S.; Khatoun, R.; Nebhen, J. Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Comput. Secur.* **2022**, *117*, 102677.
6. Zhao, K.; Zhong, J.; Ye, J. Smart Home Security Based on the Internet of Things. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 1283, pp. 388–393. https://doi.org/10.1007/978-3-030-62746-1_57.
7. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues, and solutions at different IoT layers. *J. Supercomput.* **2021**, *77*, 14053–14089. <https://doi.org/10.1007/s11227-021-03825-1>.
8. Aldridge, A.A. Examining the security essences of Internet of Things (IoT) devices in smart homes: Challenges, vulnerabilities, and countermeasures. *Issues Inf. Syst.* **2024**, *25*, 279–292. https://doi.org/10.48009/1_iis_2024_123.
9. Allafi, R.; Alzahrani, I.R. Enhancing cybersecurity in the Internet of Things environment using artificial orca algorithm and ensemble learning model. *IEEE Access* **2024**, *12*, 63282–63291. <https://doi.org/10.1109/ACCESS.2024.3390093>.
10. Solaimani, S.; Keijzer-Broers, W.; Bouwman, H. What we do—and don't—know about the smart home: An analysis of the smart home literature. *Indoor Built Environ.* **2015**, *24*, 370–383.

11. Marikyan, D.; Papagiannidis, S.; Alamanos, E. A systematic review of the smart home literature: A user perspective. *Technol. Forecast. Soc. Chang.* **2019**, *138*, 139–154.
12. Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of smart-home security using the Internet of Things. *Electronics* **2024**, *13*, 3343. <https://doi.org/10.3390/electronics13163343>.
13. Khatoun, R. *Cybersecurity in Smart Homes: Architectures, Solutions and Technologies*; Wiley: Hoboken, NJ, USA, 2022; pp. 1–290. <https://doi.org/10.1002/9781119987451>.
14. Plachkinova, M.; Vo, A.; Alluhaidan, A. Emerging trends in smart home security, privacy, and digital forensics. In Proceedings of the AMCIS 2016: 22nd Americas Conference on Information Systems, San Diego, CA, USA, 11–14 August 2016.
15. Arabo, A. Cyber security challenges within the connected home ecosystem futures. *Procedia Comput. Sci.* **2015**, *61*, 227–232. <https://doi.org/10.1016/j.procs.2015.09.201>.
16. Blondel, V.D.; Guillaume, J.L.; Lambiotte, R.; Lefebvre, E. Fast unfolding of communities in large networks. *J. Stat. Mech. Theory Exp.* **2008**, *2008*, P10008.
17. Khan, H.U.; Alomari, M.K.; Khan, S.; Nazir, S.; Gill, A.Q.; Al-Maadid, A.A.; Abu-Shawish, Z.K.; Hassan, M.K. Systematic analysis of safety and security risks in smart homes. *Comput. Mater. Contin.* **2021**, *68*, 1409–1428. <https://doi.org/10.32604/cmc.2021.016058>.
18. Vera-Mundaca, V.G.; Aquino-Trujillo, J.Y. Cybersecurity strategies for smart homes: A systematic review of threats and mitigation approaches in IoT environments. In Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology, San José, Costa Rica, 17–19 July 2024. <https://doi.org/10.18687/LEIRD2024.1.1.307>.
19. Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security analysis of IoT devices by using mobile computing: A systematic literature review. *IEEE Access* **2020**, *8*, 120331–120350. <https://doi.org/10.1109/ACCESS.2020.3006358>.
20. Ansari, A.M.; Nazir, M.; Mustafa, K. Smart homes app vulnerabilities, threats, and solutions: A systematic literature review. *J. Netw. Syst. Manag.* **2024**, *32*, 29. <https://doi.org/10.1007/s10922-024-09803-1>.
21. Tampubolon, D.G.; Widodo, G.N.; Margaretha, J.S.; Gunawan, A.A.S.; Edbert, I.S. A systematic literature review: Challenges of security optimization while maintaining good accessibility in the Internet of Things. In Proceedings of the 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS 2023): Responsible Technology for Sustainable Humanity, Yogyakarta, Indonesia, 9–10 August 2023; pp. 153–157. <https://doi.org/10.1109/ICE3IS59323.2023.10335260>.
22. Olabode, S.; Owens, R.; Zhang, V.N.; Copilah-Ali, J.; Kolomeets, M.; Wu, H.; Malviya, S.; Markeviciute, K.; Spiliotopoulos, T.; Neesham, C.; et al. Complex online harms and the smart home: A scoping review. *Future Gener. Comput. Syst.* **2023**, *149*, 664–678. <https://doi.org/10.1016/j.future.2023.08.019>.
23. Katsikeas, S.; Johnson, P.; Ekstedt, M.; Lagerström, R. Research communities in cyber security: A comprehensive literature review. *Comput. Sci. Rev.* **2021**, *42*, 100431.
24. Heiding, F.; Katsikeas, S.; Lagerström, R. Research communities in cyber security vulnerability assessments: A comprehensive literature review. *Comput. Sci. Rev.* **2023**, *48*, 100551.
25. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic mapping studies in software engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), Bari, Italy, 26–27 June 2008.
26. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report; EBSE-2007-01; Keele University: Keele, UK; Durham University: Durham, UK, 2007.
27. Lee, Y.; Lee, Y.; Seong, J.; Stanescu, A.; Hwang, C.S. A comparison of network clustering algorithms in keyword network analysis: A case study with geography conference presentations. *Int. J. Geospat. Environ. Res.* **2020**, *7*, 1–16.
28. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646.
29. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
30. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M.; Liljeberg, P. Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Gener. Comput. Syst.* **2018**, *78*, 641–658.
31. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; De Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37.
32. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the 2nd International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
33. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201.
34. Fernandes, E.; Jung, J.; Prakash, A. Security analysis of emerging smart home applications. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 636–654.
35. Sivanathan, A.; Gharakheili, H.H.; Loi, F.; Radford, A.; Wijenayake, C.; Vishwanath, A.; Sivaraman, V. Classifying IoT devices in smart environments using network traffic characteristics. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1745–1759.

36. Ni, J.; Zhang, K.; Lin, X.; Shen, X. Securing fog computing for Internet of Things applications: Challenges and solutions. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 601–628.
37. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.R. D²IoT: A federated self-learning anomaly detection system for IoT. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 756–767.
38. Yu, T.; Li, T.; Sun, Y.; Nanda, S.; Smith, V.; Sekar, V.; Seshan, S. Learning context-aware policies from multiple smart homes via federated multi-task learning. In Proceedings of the 2020 IEEE/ACM 5th International Conference on Internet-of-Things Design and Implementation (IoTDI), Los Angeles, CA, USA, 21–24 April 2020; pp. 104–115.
39. O'Connor, T.J.; Mohamed, R.; Miettinen, M.; Enck, W.; Reaves, B.; Sadeghi, A.R. HomeSnitch: Behavior transparency and control for smart home IoT devices. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 128–138.
40. Zhang, W.; Meng, Y.; Liu, Y.; Zhang, X.; Zhang, Y.; Zhu, H. Homonit: Monitoring smart home apps from encrypted traffic. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1074–1088.
41. Srinivasan, V.; Stankovic, J.; Whitehouse, K. Protecting your daily in-home activity information from a wireless snooping attack. In Proceedings of the 10th International Conference on Ubiquitous Computing, Seoul, Republic of Korea, 21–24 September 2008; pp. 202–211.
42. Fu, C.; Zeng, Q.; Du, X. HAWatcher: Semantics-aware anomaly detection for appified smart homes. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Virtual Conference, 11–13 August 2021; pp. 4223–4240.
43. Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O.B. Internet of Things (IoT): Taxonomy of security attacks. In Proceedings of the 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 11–12 August 2016; pp. 321–326.
44. Lonsetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in Bluetooth technology as used in IoT. *J. Sens. Actuator Netw.* **2018**, *7*, 28.
45. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616.
46. Liu, H.; Li, C.; Jin, X.; Li, J.; Zhang, Y.; Gu, D. Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, 30 October 2017; pp. 13–18.
47. Shang, W.; Bannis, A.; Liang, T.; Wang, Z.; Yu, Y.; Afanasyev, A.; Thompson, J.; Burke, J.; Zhang, B.; Zhang, L. Named data networking of things. In Proceedings of the 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany, 4–7 April 2016; pp. 117–128.
48. Ghosh, N.; Chandra, S.; Sachidananda, V.; Elovici, Y. SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT. *IEEE Internet Things J.* **2019**, *6*, 10773–10785.
49. Dong, Y.; Yao, Y.D. Secure mmWave-radar-based speaker verification for IoT smart home. *IEEE Internet Things J.* **2021**, *8*, 3500–3511.
50. Meng, Y.; Li, J.; Pillari, M.; Deopujari, A.; Brennan, L.; Shamsie, H.; Zhu, H.; Tian, Y. Your microphone array retains your identity: A robust voice liveness detection system for smart speakers. In Proceedings of the 31st USENIX Security Symposium (USENIX Security 22), Boston, MA, USA, 10–12 August 2022; pp. 1077–1094.
51. Zhang, S.; Das, A. HandLock: Enabling 2-FA for smart home voice assistants using inaudible acoustic signal. In Proceedings of the the 24th International Symposium on Research in Attacks, Intrusions and Defenses, San Sebastián, Spain, 6–8 October 2021; pp. 251–265.
52. Ryoo, J.; Kim, S.; Cho, J.; Kim, H.; Tjoa, S.; DeRobertis, C. IoE security threats and you. In *2017 International Conference on Software Security and Assurance (ICSSA)*; IEEE: Piscataway, NJ, USA, 2017; pp. 13–19.
53. Anthi, E.; Williams, L.; Słowińska, M.; Theodorakopoulos, G.; Burnap, P. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet Things J.* **2019**, *6*, 9042–9053.
54. Heartfield, R.; Loukas, G.; Bezemskij, A.; Panaousis, E. Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1720–1735.
55. Davis, B.D.; Mason, J.C.; Anwar, M. Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet Things J.* **2020**, *7*, 10102–10110.
56. Bugeja, J.; Jönsson, D.; Jacobsson, A. An investigation of vulnerabilities in smart connected cameras. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 537–542.
57. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733.
58. Ali, B.; Awad, A.I. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817.

59. Capellupo, M.; Liranzo, J.; Bhuiyan, M.Z.A.; Hayajneh, T.; Wang, G. Security and attack vector analysis of IoT devices. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 593–606.
60. Anthi, E.; Williams, L.; Javed, A.; Burnap, P. Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *Comput. Secur.* **2021**, *108*, 102352.
61. Li, K.F. Smart home technology for telemedicine and emergency management. *J. Ambient Intell. Humaniz. Comput.* **2013**, *4*, 535–546.
62. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future smart connected communities to fight COVID-19 outbreak. *Internet Things* **2021**, *13*, 100342.
63. Koroniotis, N.; Moustafa, N.; Sitnikova, E. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Gener. Comput. Syst.* **2020**, *110*, 91–106.
64. Brotsis, S.; Limnitis, K.; Bendiab, G.; Kolokotronis, N.; Shiaeles, S. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Comput. Netw.* **2021**, *191*, 108005.
65. Oriwoh, E.; Sant, P. The forensics edge management system: A concept and design. In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*; IEEE: Piscataway, NJ, USA, 2013; pp. 544–550.
66. Lin, H.; Bergmann, N.W. IoT privacy and security challenges for smart home environments. *Information* **2016**, *7*, 44.
67. Al-Muhtadi, J.; Anand, M.; Mickunas, M.D.; Campbell, R. Secure smart homes using Jini and UIUC SESAME. In *16th Annual Computer Security Applications Conference (ACSAC'00)*; IEEE: Piscataway, NJ, USA, 2000; pp. 77–85.
68. Serror, M.; Henze, M.; Hack, S.; Schuba, M.; Wehrle, K. Towards in-network security for smart homes. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg, Germany, 27–30 August 2018; pp. 1–8.
69. Pătru, I.I.; Carabaș, M.; Bărbulescu, M.; Gheorghe, L. Smart home IoT system. In *2016 15th RoEduNet Conference: Networking in Education and Research*; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
70. Axisa, F.; Schmitt, P.M.; Gehin, C.; Delhomme, G.; McAdams, E.; Dittmar, A. Flexible technologies and smart clothing for citizen medicine, home healthcare, and disease prevention. *IEEE Trans. Inf. Technol. Biomed.* **2005**, *9*, 325–336.
71. Wilson, C.; Hargreaves, T.; Hauxwell-Baldwin, R. Benefits and risks of smart home technologies. *Energy Policy* **2017**, *103*, 72–83.
72. Yang, H.; Lee, H.; Zo, H. User acceptance of smart home services: An extension of the theory of planned behavior. *Ind. Manag. Data Syst.* **2017**, *117*, 68–89.
73. Demiris, G.; Hensel, B.K.; Skubic, M.; Rantz, M. Senior residents' perceived need of and preferences for smart home sensor technologies. *Int. J. Technol. Assess. Health Care* **2008**, *24*, 120–124.
74. Gochoo, M.; Tan, T.H.; Liu, S.H.; Jean, F.R.; Alnajjar, F.S.; Huang, S.C. Unobtrusive activity recognition of elderly people living alone using anonymous binary sensors and DCNN. *IEEE J. Biomed. Health Inform.* **2019**, *23*, 693–702.
75. Guhr, N.; Werth, O.; Blacha, P.P.H.; Breitner, M.H. Privacy concerns in the smart home context. *SN Appl. Sci.* **2020**, *2*, 247.
76. Dahmen, J.; Cook, D.J.; Wang, X.; Wang, H. Smart secure homes: A survey of smart home technologies that sense, assess, and respond to security threats. *J. Reliab. Intell. Environ.* **2017**, *3*, 83–98.
77. Jamwal, R.; Jarman, H.K.; Roseingrave, E.; Douglas, J.; Winkler, D. Smart home and communication technology for people with disability: A scoping review. *Disabil. Rehabil. Assist. Technol.* **2022**, *17*, 624–644.
78. Iqbal, A.; Ullah, F.; Anwar, H.; Kwak, K.S.; Imran, M.; Jamal, W.; ur Rahman, A. Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud. *Sustain. Cities Soc.* **2018**, *38*, 636–646.
79. De Silva, L.C.; Morikawa, C.; Petra, I.M. State of the art of smart homes. *Eng. Appl. Artif. Intell.* **2012**, *25*, 1313–1321.
80. Balta-Ozkan, N.; Davidson, R.; Bicket, M.; Whitmarsh, L. Social barriers to the adoption of smart homes. *Energy Policy* **2013**, *63*, 363–374.
81. Demiris, G.; Hensel, B.K. Technologies for an aging society: A systematic review of smart home applications. *Yearb. Med. Inform.* **2008**, *17*, 33–40.
82. Nobakht, M.; Sivaraman, V.; Boreli, R. A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, 31 August–2 September 2016; pp. 147–156.
83. Lee, Y.; Rathore, S.; Park, J.H.; Park, J.H. A blockchain-based smart home gateway architecture for preventing data forgery. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 9.
84. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet Things J.* **2021**, *8*, 1817–1829.
85. Eskandari, M.; Janjua, Z.H.; Vecchio, M.; Antonelli, F. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet Things J.* **2020**, *7*, 6882–6897.

86. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; pp. 163–167.
87. Tao, M.; Zuo, J.; Liu, Z.; Castiglione, A.; Palmieri, F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Gener. Comput. Syst.* **2018**, *78*, 1040–1051.
88. Mohanty, S.N.; Ramya, K.C.; Rani, S.S.; Gupta, D.; Shankar, K.; Lakshmanaprabu, S.K.; Khanna, A. An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. *Future Gener. Comput. Syst.* **2020**, *102*, 1027–1037.
89. Singh, S.; Ra, I.H.; Meng, W.; Kaur, M.; Cho, G.H. SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719844159.
90. Jiang, H.; Cai, C.; Ma, X.; Yang, Y.; Liu, J. Smart home based on WiFi sensing: A survey. *IEEE Access* **2018**, *6*, 13317–13325.
91. Nasir, M.; Muhammad, K.; Ullah, A.; Ahmad, J.; Baik, S.W.; Sajjad, M. Enabling automation and edge intelligence over resource-constrained IoT devices for smart home. *Neurocomputing* **2022**, *491*, 494–506.
92. Ren, Y.; Leng, Y.; Qi, J.; Sharma, P.K.; Wang, J.; Almakhadmeh, Z.; Tolba, A. Multiple cloud storage mechanism based on blockchain in smart homes. *Future Gener. Comput. Syst.* **2021**, *115*, 304–313.
93. Gill, K.; Yang, S.H.; Yao, F.; Lu, X. A ZigBee-based home automation system. *IEEE Trans. Consum. Electron.* **2009**, *55*, 422–430.
94. Froiz-Míguez, I.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Castedo, L. Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes. *Sensors* **2018**, *18*, 2660.
95. Sahani, M.; Nanda, C.; Sahu, A.K.; Pattnaik, B. Web-based online embedded door access control and home security system based on face recognition. In Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 19–20 March 2015; pp. 1–6.
96. Adriansyah, A.; Dani, A.W. Design of small smart home system based on Arduino. In Proceedings of the 2014 Electrical Power, Electronics, Communications, Control and Informatics Seminar (EECCIS), Malang, East Java, Indonesia, 26–27 August 2014; pp. 121–125.
97. Pirbhulal, S.; Zhang, H.; Alahi, M.E.E.; Ghayvat, H.; Mukhopadhyay, S.C.; Zhang, Y.T.; Wu, W. A novel secure IoT-based smart home automation system using a wireless sensor network. *Sensors* **2017**, *17*, 69.
98. Shi, Q.; Zhang, Z.; He, T.; Sun, Z.; Wang, B.; Feng, Y.; Shan, X.; Salam, B.; Lee, C. Deep learning enabled smart mats as a scalable floor monitoring system. *Nat. Commun.* **2020**, *11*, 4609.
99. 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.
100. Upadhyay, Y.; Borole, A.; Dileepan, D. MQTT-based secured home automation system. In Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 18–19 March 2016; pp. 1–4.
101. Majeed, R.; Abdullah, N.A.; Ashraf, I.; Zikria, Y.B.; Mushtaq, M.F.; Umer, M. An intelligent, secure, and smart home automation system. *Sci. Program.* **2020**, *2020*, 4579291.
102. Venkatraman, S.; Overmars, A.; Thong, M. Smart home automation: Use cases of a secure and integrated voice-control system. *Systems* **2021**, *9*, 77.
103. Celebre, A.M.D.; Dubouzet, A.Z.D.; Medina, I.B.A.; Surposa, A.N.M.; Gustilo, R.C. Home automation using Raspberry Pi through Siri enabled mobile devices. In *2015 International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM)*; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.
104. Kodali, R.K.; Jain, V.; Bose, S.; Boppana, L. IoT-based smart security and home automation system. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29–30 April 2016; pp. 1286–1289.
105. Vujović, V.; Maksimović, M. Raspberry Pi as a sensor Web node for home automation. *Comput. Electr. Eng.* **2015**, *44*, 153–171.
106. Santoso, F.K.; Vun, N.C.H. Securing IoT for smart home system. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 1–2.
107. Kumar, P.; Braeken, A.; Gurtov, A.; Iinatti, J.; Ha, P.H. Anonymous secure framework in connected smart home environments. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 968–979.
108. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy-preserving communication protocol for IoT applications in smart homes. *IEEE Internet Things J.* **2017**, *4*, 1844–1852.
109. Al Salami, S.; Baek, J.; Salah, K.; Damiani, E. Lightweight encryption for smart home. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 382–388.
110. Poh, G.S.; Gope, P.; Ning, J. PrivHome: Privacy-preserving authenticated communication in smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1095–1107.
111. Lin, C.; He, D.; Kumar, N.; Huang, X.; Vijayakumar, P.; Choo, K.K.R. HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet Things J.* **2019**, *7*, 818–829.

112. Liu, Z.; Seo, H. IoT-NUMS: Evaluating NUMS elliptic curve cryptography for IoT platforms. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 720–729.
113. Lohachab, A. ECC-based inter-device authentication and authorization scheme using MQTT for IoT networks. *J. Inf. Secur. Appl.* **2019**, *46*, 1–12.
114. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146.
115. Shin, D.; Yun, K.; Kim, J.; Astillo, P.V.; Kim, J.N.; You, I. A security protocol for route optimization in DMM-based smart home IoT networks. *IEEE Access* **2019**, *7*, 142531–142550.
116. Luo, H.; Wang, C.; Luo, H.; Zhang, F.; Lin, F.; Xu, G. G2F: A secure user authentication for rapid smart home IoT management. *IEEE Internet Things J.* **2021**, *8*, 10884–10895.
117. Almusaylim, Z.A.; Zaman, N. A review on smart home present state and challenges: Linked to context-awareness Internet of Things (IoT). *Wirel. Netw.* **2019**, *25*, 3193–3204.
118. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2015**, *16*, 254–264.
119. Brush, A.J.B.; Lee, B.; Mahajan, R.; Agarwal, S.; Saroiu, S.; Dixon, C. Home automation in the wild: Challenges and opportunities. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada, 7–12 May 2011; pp. 2115–2124.
120. Geeng, C.; Roesner, F. Who's in control? Interactions in multi-user smart homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019; pp. 1–13.
121. Kepuska, V.; Bohouta, G. Next generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home). In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 99–103.
122. Zheng, S.; Aphorpe, N.; Chetty, M.; Feamster, N. User perceptions of smart home IoT privacy. In *Proceedings of the ACM on Human-Computer Interaction*; Association for Computing Machinery: New York, NY, USA, 2018; Volume 2, pp. 1–20.
123. Ammari, T.; Kaye, J.; Tsai, J.Y.; Bentley, F. Music, search, and IoT: How people really use voice assistants. *ACM Trans. Comput.-Hum. Interact.* **2019**, *26*, 1–28.
124. Zeng, E.; Mare, S.; Roesner, F. End user security and privacy concerns with smart homes. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA, 12–14 July 2017; pp. 65–80.
125. Tabassum, M.; Kosinski, T.; Lipford, H.R. I don't own the data: End user perceptions of smart home device data practices and risks. In Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, USA, 24–26 July 2019; pp. 435–450.
126. Caine, K.E.; Fisk, A.D.; Rogers, W.A. Benefits and privacy concerns of a home equipped with a visual sensing system: A perspective from older adults. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, San Francisco, CA, USA, 16–20 October 2006; Volume 50, pp. 180–184.
127. Laput, G.; Zhang, Y.; Harrison, C. Synthetic sensors: Towards general-purpose sensing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 6–11 May 2017; pp. 3986–3999.
128. Strengers, Y.; Kennedy, J.; Arcari, P.; Nicholls, L.; Gregg, M. Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019; pp. 1–13.
129. Leitão, R. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In Proceedings of the 2019 on Designing Interactive Systems Conference, San Diego, CA, USA, 23–28 June 2019; pp. 527–539.
130. Marky, K.; Prange, S.; Krell, F.; Mühlhäuser, M.; Alt, F. You just can't know about everything: Privacy perceptions of smart home visitors. In Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia, Virtual Conference, 22–25 November 2020; pp. 83–95.
131. Yao, Y.; Basdeo, J.R.; McDonough, O.R.; Wang, Y. Privacy perceptions and designs of bystanders in smart homes. In *Proceedings of the ACM on Human-Computer Interaction*; Association for Computing Machinery: New York, NY, USA, 2019; Volume 3, pp. 1–24.
132. Huang, D.Y.; Aphorpe, N.; Li, F.; Acar, G.; Feamster, N. IoT Inspector: Crowdsourcing labeled network traffic from smart home devices at scale. In *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*; ACM: New York, NY, USA, 2020; Volume 4; pp. 1–21.
133. Schaub, F.; Balebako, R.; Durity, A.L.; Cranor, L.F. A design space for effective privacy notices. In Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), Ottawa, ON, Canada, 22–24 July 2015; pp. 1–17.
134. Pinheiro, A.J.; Bezerra, J.d.M.; Burgardt, C.A.P.; Campelo, D.R. Identifying IoT devices and events based on packet length from encrypted traffic. *Comput. Commun.* **2019**, *144*, 8–17.
135. Cvitić, I.; Peraković, D.; Periša, M.; Gupta, B. Ensemble machine learning approach for classification of IoT devices in smart homes. *Int. J. Mach. Learn. Cybern.* **2021**, *12*, 3179–3202.

136. Thangavelu, V.; Divakaran, D.M.; Sairam, R.; Bhunia, S.S.; Gurusamy, M. DEFT: A distributed IoT fingerprinting technique. *IEEE Internet Things J.* **2019**, *6*, 940–952.
137. Makkar, A.; Garg, S.; Kumar, N.; Hossain, M.S.; Ghoneim, A.; Alrashoud, M. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans. Ind. Inform.* **2021**, *17*, 903–912.
138. Yıldırım, İ.; Bostancı, E.; Güzel, M.S. Forensic analysis with anti-forensic case studies on Amazon Alexa and Google Assistant built-in smart home speakers. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 1–3.
139. Pathak, S.; Islam, S.A.; Jiang, H.; Xu, L.; Tomai, E. A survey on security analysis of Amazon Echo devices. *High-Confid. Comput.* **2022**, *2*, 100087.
140. Hafeez, I.; Antikainen, M.; Tarkoma, S. Protecting IoT-environments against traffic analysis attacks with traffic morphing. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*; IEEE: Piscataway, NJ, USA, 2019; pp. 196–201.
141. Pinheiro, A.J.; de Araujo-Filho, P.F.; Bezerra, J.d.M.; Campelo, D.R. Adaptive packet padding approach for smart home networks: A tradeoff between privacy and performance. *IEEE Internet Things J.* **2021**, *8*, 3930–3938.
142. Kabir, S.; Gope, P.; Mohanty, S.P. A security-enabled safety assurance framework for IoT-based smart homes. *IEEE Trans. Ind. Appl.* **2022**, *59*, 6–14.
143. Tagliaro, C.; Komsic, M.; Continella, A.; Borgolte, K.; Lindorfer, M. Large-scale security analysis of real-world backend deployments speaking IoT-focused protocols. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses, Padua, Italy, 14–16 October 2024; pp. 561–578.
144. Sham, S.N.S.A.; Ishak, K.K.; Razali, N.A.M.; Noor, N.M.; Hasbullah, N.A. IoT attack detection using machine learning and deep learning in smart home. *JOIV Int. J. Inform. Vis.* **2024**, *8*, 510–519.
145. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. *Sensors* **2022**, *22*, 2087.
146. Li, X.; Li, S.; Zhang, D.; Xiong, J.; Wang, Y.; Mei, H. Dynamic-MUSIC: Accurate Device-Free Indoor Localization. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 196–207.
147. Yang, J.; Zou, H.; Jiang, H.; Xie, L. Device-Free Occupant Activity Sensing Using WiFi-Enabled IoT Devices for Smart Homes. *IEEE Internet Things J.* **2018**, *5*, 3991–4002.
148. Kosba, A.E.; Saeed, A.; Youssef, M. RASID: A Robust WLAN Device-Free Passive Motion Detection System. In *2012 IEEE International Conference on Pervasive Computing and Communications*; IEEE: Piscataway, NJ, USA, 2012; pp. 180–189.
149. Kong, H.; Lu, L.; Yu, J.; Chen, Y.; Tang, F. Continuous Authentication Through Finger Gesture Interaction for Smart Homes Using WiFi. *IEEE Trans. Mob. Comput.* **2020**, *20*, 3148–3162.
150. Peng, R.; Sichitiu, M.L. Angle of Arrival Localization for Wireless Sensor Networks. In *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*; IEEE: Piscataway, NJ, USA, 2006; Volume 1, pp. 374–382.
151. Guo, L.; Wang, L.; Liu, J.; Zhou, W.; Lu, B. HuAc: Human Activity Recognition Using Crowdsourced WiFi Signals and Skeleton Data. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 6163475.
152. Dang, X.; Bai, Y.; Hao, Z.; Liu, G. Wi-GC: A deep spatiotemporal gesture recognition method based on Wi-Fi signal. *Appl. Sci.* **2022**, *12*, 10425.
153. Forbes, G.; Massie, S.; Craw, S. WiFi-based human activity recognition using Raspberry Pi. In Proceedings of the 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI), Virtual Conference, 9–11 November 2020; pp. 722–730.
154. Talal, M.; Zaidan, A.; Zaidan, B.; Albahri, A.S.; Alamoodi, A.H.; Albahri, O.S.; Alsalem, M.; Lim, C.K.; Tan, K.L.; Shir, W.; et al. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *J. Med Syst.* **2019**, *43*, 42.
155. Ge, M.; Hong, J.B.; Guttman, W.; Kim, D.S. A framework for automating security analysis of the Internet of Things. *J. Netw. Comput. Appl.* **2017**, *83*, 12–27.
156. Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*; IEEE: Piscataway, NJ, USA, 2016; pp. 1–7.
157. Khan, M.; Silva, B.N.; Han, K. Internet of Things Based Energy Aware Smart Home Control System. *IEEE Access* **2016**, *4*, 7556–7566.
158. Rahimi, M.; Songhorabadi, M.; Kashani, M.H. Fog-Based Smart Homes: A Systematic Review. *J. Netw. Comput. Appl.* **2020**, *153*, 102531.
159. Gaikwad, P.P.; Gabhane, J.P.; Golait, S.S. A Survey Based on Smart Homes System Using Internet-of-Things. In *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*; IEEE: Piscataway, NJ, USA, 2015; pp. 330–335.

160. Rahmani, A.M.; Thanigaivelan, N.K.; Gia, T.N.; Granados, J.; Negash, B.; Liljeberg, P.; Tenhunen, H. Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*; IEEE: Piscataway, NJ, USA, 2015; pp. 826–834.
161. Moosavi, S.R.; Gia, T.N.; Rahmani, A.M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459.
162. Xu, Z.; Ansari, S.; Abdulghani, A.M.; Imran, M.A.; Abbasi, Q.H. IoT-enabled smart security framework for 3D-printed smart home. In *Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Beijing, China, 14–16 August 2020; pp. 117–123.
163. Siddhanti, P.; Aspiron, P.M.; Schneider, B. Cybersecurity by design for smart home environments. In *Proceedings of the 21st International Conference on Enterprise Information Systems (ICEIS)*, Heraklion, Crete, Greece, 3–5 May 2019; pp. 587–595.
164. Ul Rehman, S.; Manickam, S. A study of smart home environment and its security threats. *Int. J. Reliab. Qual. Saf. Eng.* **2016**, *23*, 1640005.
165. Yu, C.; Xu, Z.; Yan, K.; Chien, Y.R.; Fang, S.H.; Wu, H.C. Noninvasive human activity recognition using millimeter-wave radar. *IEEE Syst. J.* **2022**, *16*, 3036–3047.
166. Wang, Z.; Ren, A.; Zhang, Q.; Zahid, A.; Abbasi, Q.H. Recognition of approximate motions of humans based on micro-Doppler features. *IEEE Sens. J.* **2023**, *23*, 12388–12397.
167. Fengou, M.A.; Mantas, G.; Lymberopoulos, D.; Komninos, N.; Fengos, S.; Lazarou, N. A new framework architecture for next generation e-health services. *IEEE J. Biomed. Health Inform.* **2013**, *17*, 9–18.
168. Kumar, P.; Chauhan, S.; Awasthi, L.K. Human activity recognition using deep learning: Review, methodologies, progress and future research directions. *Arch. Comput. Methods Eng.* **2024**, *31*, 179–219.
169. Aldahmani, A.; Ouni, B.; Lestable, T.; Debbah, M. Cyber-security of embedded IoTs in smart homes: Challenges, requirements, countermeasures, and trends. *IEEE Open J. Veh. Technol.* **2023**, *4*, 281–292.
170. Kaiser, M.; Griessl, R.; Kucza, N.; Haumann, C.; Tigges, L.; Mika, K.; Hagemeyer, J.; Porrmann, F.; Rückert, U.; vor dem Berge, M.; et al. VEDLIoT: Very efficient deep learning in IoT. In *Proceedings of the 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 963–968.
171. Mika, K.; Griessl, R.; Kucza, N.; Porrmann, F.; Kaiser, M.; Tigges, L.; Hagemeyer, J.; Trancoso, P.; Azhar, M.W.; Qararyah, F.; et al. VEDLIoT: Next generation accelerated AIoT systems and applications. In *Proceedings of the 20th ACM International Conference on Computing Frontiers*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 291–296.

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