

Systematic Review

A Systematic Review of Smart Home IoT Security: Applications, Threat Taxonomy, Privacy Risks, and Emerging Defensive Solutions

Dalibor Radovanovic , Nikola Savanovic , Jelena Janackovic and Petar Kresoja 

Faculty of Informatics and Computing, Singidunum University, Danijelova 32, 11000 Belgrade, Serbia; nsavanovic@singidunum.ac.rs (N.S.); jjanackovic@singidunum.ac.rs (J.J.); pkresoja@singidunum.ac.rs (P.K.)

* Correspondence: dradovanovic@singidunum.ac.rs

Abstract

The rapid proliferation of Internet of Things (IoT) technologies has transformed the modern home into a complex cyber-physical ecosystem encompassing hundreds of millions of connected devices globally. Smart homes support automation, energy management, and healthcare monitoring, but they also introduce a broad and evolving range of security and privacy challenges. This review examines 233 sources published between 2018 and May 2025, selected through a PRISMA-informed process covering five major academic databases and relevant standards and technical reports. It discusses communication protocols, including Matter, develops a Threat-Layer-Defense synthesis matrix covering ten attack categories; examines the practical limitations of AI-based anomaly detection and blockchain-based trust management; and derives recommendations for manufacturers, platform providers, users, and regulators. Privacy challenges, regulatory frameworks, and user behavior are considered alongside technical threats. The findings suggest that scalable smart home security requires coordinated progress in protocol standardization, enforceable device update lifecycles, gateway-level anomaly detection, and privacy-preserving local analytics rather than reliance on a single technical solution.

Keywords: IoT; smart home; security; privacy; threat taxonomy; AI anomaly detection; blockchain; Matter protocol; cyber threats; PRISMA survey

1. Introduction

The Internet of Things (IoT) has emerged as one of the most consequential technological paradigms of the early twenty-first century. Building on the general IoT survey by Salih et al. [1], the present paper narrows its focus to the smart home, one of the most dynamic and security-critical deployment domains. The scale of adoption is significant: approximately 478–482 million homes worldwide were equipped with at least one smart device by 2025 [2], with annual shipments reaching 1.77 billion units [3] and a global market valuation of approximately \$147.5 billion [4]. Total global IoT endpoints across all sectors independently exceeded 15 billion in 2025 [5], a distinct and larger population that encompasses industrial, automotive, and infrastructure deployments.

The security implications are severe and documented. Data throughout 2023 identified smart televisions (34%), smart plugs (18%), DVRs (13%), and home routers (12%) as the most exploited device categories [6], with buffer overflow vulnerabilities comprising 28.25% and DoS-class weaknesses 27.20% of identified vulnerabilities [6]. A persistent behavioral



Academic Editor: Cristian González García

Received: 1 June 2026

Revised: 27 July 2026

Accepted: 28 July 2026

Published: 1 August 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 Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

gap compounds the risk: 76% of users are aware of security risks, but only 24% perform regular firmware updates [7].

Existing surveys on smart home IoT security vary in scope and methodology. Table 1 compares this review with six representative prior works across eight dimensions. The review combines a PRISMA-informed methodology (Section 2) with an analysis of smart home applications and communication architectures (Sections 1.2 and 3), a Threat-Layer-Defense synthesis matrix (Section 4.5), an examination of AI datasets and evaluation challenges (Section 7.1), an assessment of blockchain applicability (Section 7.2), and stakeholder-oriented recommendations (Section 8.2). The research questions are introduced in Section 2.1 and revisited in the conclusion.

Table 1. Comparison of This Survey with Representative Prior Works Across Eight Dimensions.

Prior Survey	Scope	Smart Home Focus	Threat Taxonomy	Matter	AI/ML	Blockchain	Privacy/Reg.	Advantages of This Work
Aldahmani et al., 2023 [8]	Smart home	Yes	Partial	No	No	No	Partial	Matrix; PRISMA; AI/BC critique; recommendations
Yuan et al., 2023 [9]	Smart home	Yes	Partial	No	Partial	No	No	Matter; PRISMA; recommendations; datasets
Hammi et al., 2022 [10]	Smart home vuln.	Yes	Yes	No	No	No	No	Matter; AI; blockchain; datasets; recommendations
Bhuyan et al., 2022 [11]	BC/SDN/NFV	Partial	No	No	No	Yes	No	Full scope; synthesis matrix; PRISMA
Salih et al., 2022 [1]	General IoT	No	No	No	No	No	No	Smart home; security taxonomy; all above
Zia et al., 2025 [12]	Smart home/cities	Yes	Partial	Partial	No	No	No	Matrix; datasets; BC critical eval
This review	Smart home security	Yes	Full matrix	Yes	Critical	Critical	Full	—

1.1. Motivation and Problem Statement

Smart home deployments differ from industrial or enterprise IoT in four respects that affect security design. First, the extreme device heterogeneity spanning constrained Class 1 devices (sensors, actuators) to full-featured hubs and voice assistants creates an attack surface that no single protocol or defense mechanism can uniformly protect. Second, the residential deployment context means that end users, not trained administrators, are responsible for device configuration, firmware updates, and network segmentation. Third, the intimate nature of smart home data (occupancy patterns, health metrics, behavioral routines) elevates privacy risks to a level commensurate with technical security threats. Fourth, the market fragmentation across ecosystems (Apple HomeKit, Google Home, Amazon Alexa, Matter) produces interoperability gaps that attackers exploit through cross-app interference and insecure bridge implementations. These four factors guided our decision to conduct a structured, PRISMA-informed review that maps the threat landscape, evaluates existing and emerging defenses, and identifies actionable gaps for each stakeholder group.

1.2. Smart Home Ecosystem and Architecture Overview

A smart home integrates IoT-enabled devices and sensors to enable remote monitoring, control, and automation of domestic functions, relying on end devices, communication networks, and cloud or edge computing platforms [13–15]. The ecosystem is dominated by four major platforms (Apple HomeKit, Google Home, Amazon Alexa, and the emerging Matter standard [16]) alongside a fragmented base of proprietary manufacturers. This fragmentation is a primary source of interoperability and security challenges [9]. Devices range from environmental sensors and smart locks to voice assistants and healthcare wearables; each category carries specific attack vectors discussed in Section 4.

Smart home architecture follows a five-layer model [1,17]: Perception Layer (sensors, actuators), Network Layer (wireless/wired protocols), Middleware Layer (cloud/edge analytics, AI inference), Application Layer (mobile apps, voice control, automation logic), and Business Layer (policy management, third-party integration, access control). An Adaptation Layer between the Perception and Network layers bridges heterogeneous device protocols [17]. No single communication protocol is optimal across all security dimensions; relevant trade-offs in latency, range, encryption support, and known vulnerabilities are considered throughout the review.

1.3. Contributions and Advantages over Prior Surveys

Table 1 compares this review with six representative prior works across eight dimensions. Several earlier surveys address smart home IoT security with a narrower scope or without a systematic review method. Aldahmani et al. [8] focus on smart home security but do not use PRISMA or provide a combined assessment of AI, blockchain, and stakeholder recommendations. Yuan et al. [9] examine threats but do not cover Matter or dataset evaluation challenges. Hammi et al. [10] focus on vulnerabilities without addressing AI-based detection or blockchain applicability. The present review applies reproducible inclusion and exclusion criteria to 233 sources, examines the conditions under which AI-based detection and blockchain may provide practical value, as well as their remaining limitations, introduces a Threat-Layer-Defense matrix covering ten attack categories, and summarizes recommendations for manufacturers, platform providers, end users, and regulators.

The paper is structured as follows: Section 1 provides the motivation, defines the smart home ecosystem and architecture, and positions this survey relative to prior works. Section 2 presents the PRISMA-informed methodology and research questions. Section 3 maps smart home applications to their security linkages. Sections 4 and 5 classify threats and privacy risks. Sections 6 and 7 assess existing defenses and emerging solutions. Section 8 proposes research directions and stakeholder recommendations. Section 9 discusses limitations. Section 10 concludes.

2. Survey Methodology

2.1. Research Questions

This systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [18] adapted for scoping reviews in computer science. The review is organized around five research questions (RQs) that are explicitly addressed in the corresponding sections and revisited in the conclusion:

- RQ1: Which communication protocols dominate smart home IoT deployments and what are their specific security limitations? (Sections 1.2, 3 and 6.2)
- RQ2: What are the most persistent and impactful threat categories across the device, network, cloud, and application layers of smart home systems? (Section 4)
- RQ3: Which existing defenses address these threats, where do known gaps remain, and what is the research priority for each? (Sections 4.5 and 6)

- RQ4: Under what specific conditions do AI-based anomaly detection and blockchain-based trust management provide practical, demonstrable security value, and where do they fall short? (Section 7)
- RQ5: What research gaps and actionable recommendations remain for achieving secure, privacy-preserving smart home ecosystems? (Sections 5 and 8)

2.2. Search Strategy

Literature searches were conducted in January–May 2025 across five major academic databases: IEEE Xplore, ACM Digital Library, Elsevier ScienceDirect, Springer Link, and MDPI Open Access Repository. Authoritative grey literature from ENISA, NIST, the Connectivity Standards Alliance (CSA/Matter), and Gartner were incorporated for standards and market context.

The primary search string was: (“Internet of Things” OR “IoT”) AND (“smart home” OR “home automation” OR “connected home”) AND (“security” OR “privacy” OR “cyber” OR “attack” OR “vulnerability”). Complementary strings targeted AI anomaly detection, blockchain security and Matter protocol specifically. The systematic search was completed in May 2025. Works published after this date fall outside the review scope; readers are encouraged to consult recent literature for developments in the smart home security domain, where threat profiles shifted substantially between 2020 and 2025.

2.3. Inclusion and Exclusion Criteria

Included: peer-reviewed journal/conference papers published in January 2018–May 2025; English language; addresses IoT security, privacy, architecture, or applications in a domestic context; available as full text. Excluded: non-domestic IoT focus without smart home relevance; papers superseded by more recent work from the same group; inadequate quality (no peer review, no references, or clear methodological deficiency). Market data from authoritative industry sources (Statista, Ericsson, Juniper Research) was accepted for quantitative market context.

2.4. Search Results and PRISMA Flow

Table 2 summarizes the literature search results by database. The analytical corpus comprises 233 sources: 189 peer-reviewed journal or conference papers, 22 standards documents or authoritative technical reports, and 22 market context sources as illustrated in Figure 1. References cited in this paper represent a curated selection of the most impactful works from this corpus, prioritizing IEEE, ACM, Elsevier, Springer, and MDPI publications. Temporal distribution shows a pronounced increase in smart home security publications from 2020 onward, consistent with accelerated adoption and associated growth in research attention. An AI-based language tool was used for grammar checking and language refinement of selected passages during manuscript preparation; all content was reviewed and verified by the authors. The PRISMA 2020 checklist is provided as Supplementary Table S1. Full characteristics of all 233 included sources are provided in Table S2 of the Supplementary Materials.

Table 2. Literature Search Results by Database (PRISMA-Informed).

Database	Initial Results	After Title/Abstract Screen	After Full-Text Review	Included in Corpus
IEEE Xplore	1847	312	94	61
ACM Digital Library	923	187	58	37
Elsevier ScienceDirect	1204	241	71	44

Table 2. Cont.

Database	Initial Results	After Title/Abstract Screen	After Full-Text Review	Included in Corpus
Springer Link	876	158	49	31
MDPI Repositories	634	143	52	38
Grey Literature (ENISA, NIST, CSA, Gartner)	—	—	27	22
Total	5484	1041	351	233

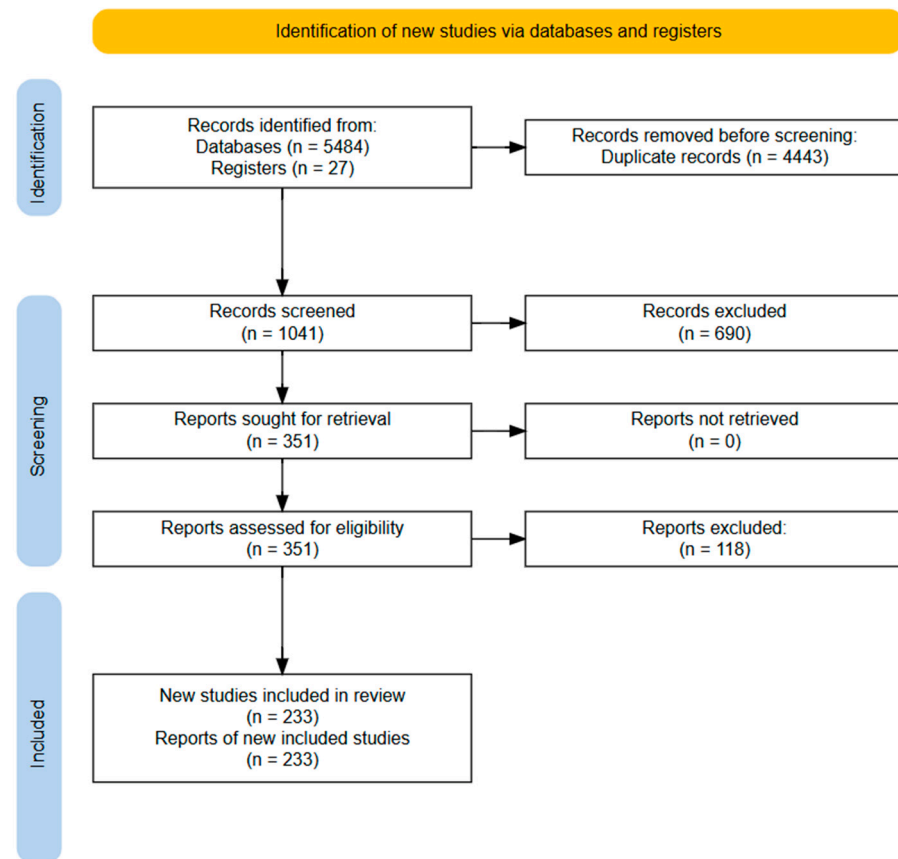


Figure 1. PRISMA2020 Literature Selection Flow Diagram.

3. Applications of IoT in Smart Homes and Security Linkage

Smart home applications are presented here not as independent capabilities but in direct connection to the security and privacy risks they introduce, providing the motivating context for the threat analysis in Section 4.

3.1. Energy Management and Environmental Control

Smart thermostats apply machine learning to occupancy patterns to optimize HVAC, with independently verified energy savings of 10–23% [19,20]. Smart metering and demand response programs enable grid participation. Security linkage: sub-second smart meter readings enable occupancy inference without any device compromise, a passive privacy threat addressed in Section 5 [21].

3.2. Security and Surveillance

AI-powered cameras with motion detection and facial recognition, video doorbells, smart locks with access logging, and professional monitoring integration define the smart security segment [22]. Security linkage: facial recognition data, continuous video streams, and cloud-hosted recordings represent high-sensitivity data assets whose unauthorized

access constitutes both a security breach and a privacy violation; cloud storage exposure is the dominant attack vector for this category [6].

3.3. Healthcare and Assisted Living

Ambient assisted living (AAL) systems deploy distributed sensors to monitor elderly or disabled residents, detecting falls and tracking medication adherence [23]. Wearable IoT devices continuously measure biometric parameters for remote clinical monitoring, extending the telemedicine paradigm documented in Salih et al. [1]. Security linkage: biometric and health data represent the highest-sensitivity category under GDPR and equivalent frameworks; unauthorized access carries direct physical and legal consequences.

3.4. Comfort, Entertainment, and Automation

Voice-controlled assistants serve as automation hubs; scene-based rules encode conditional behaviors. Matter-compatible cross-ecosystem automation is progressively reducing fragmentation barriers [16]. Security linkage: automation logic creates unsafe actuation risks, unauthorized commands triggering lock release, thermostat manipulation, or appliance activation, which cross-app interference attacks (Section 4.4) exploit [24].

3.5. Smart City Integration

Smart homes contribute to city-level environmental monitoring, grid demand response, and EV charging infrastructure [25]. Security linkage: cross-domain data integration creates attack propagation pathways; a compromised smart home device may serve as an entry point into broader city infrastructure, multiplying the impact of a single-device compromise.

4. Security Threats and Vulnerabilities

4.1. Attack Surface Overview

The smart home attack surface spans device, network, cloud/edge, and application layers. Heterogeneous devices, default credentials, irregular firmware cycles, and absent security baselines create a high-value target environment [8]. Buffer overflow remains the leading vulnerability class (28.25%), followed by DoS-class weaknesses (27.20%), both persistent despite being well-understood, due to constrained hardware and weak manufacturer incentives [6].

4.2. Device-Level Vulnerabilities

- **Default Credentials:** Devices shipped with unchanged defaults enable trivial unauthorized access—operationally the most exploited weakness and the root cause of the Mirai botnet that disrupted critical Internet infrastructure in 2016.
- **Insecure Firmware:** Known CVEs, hardcoded credentials, and exposed debug interfaces (UART, JTAG) allow local exploitation. Long device lifecycles mean significant portions of installed bases run end-of-support firmware.
- **Lack of Secure Boot:** Without cryptographic firmware verification at startup, devices are vulnerable to persistent compromise via firmware replacement attacks.
- **Physical Tampering:** Devices in accessible locations are subject to hardware-level attacks including side-channel analysis and fault injection, particularly relevant for smart locks and outdoor cameras.

4.3. Network-Level Attacks

- **Man-in-the-Middle (MitM):** Misconfigured or absent TLS enables interception and command modification. Independent security analysis of Amazon Alexa confirmed exploitable third-party skill attack surfaces [26].

- Botnet Recruitment and DDoS: Resource-constrained devices with predictable behavior are routinely recruited into botnets (Mirai, Mozi, BrickerBot) for large-scale DDoS attacks. DoS vulnerability prevalence of 27.20% indicates systemic susceptibility [6,27].
- Replay Attacks: Systems without nonce-based challenge-response authentication are vulnerable to credential replay, enabling authentication bypass without decryption.
- Protocol Downgrade: In heterogeneous networks, adversaries may force negotiation of weaker legacy protocol versions, undermining encryption.

4.4. Cloud and Application-Level Threats

- Insecure APIs: REST and MQTT cloud management APIs with inadequate authentication enable mass-device takeover. A single vulnerable API endpoint can expose the entire device population of a manufacturer.
- Cross-App Interference: Malicious or compromised automation applications can issue unauthorized device commands through shared platform state, as formally analyzed in *IoTCom* [24].
- Supply Chain Attacks: Compromised firmware or software distributed through legitimate update channels represents a high-impact, difficult-to-detect threat vector [28].

4.5. Threat-Layer-Defense Synthesis Matrix

Table 3 consolidates ten attack categories with their targeted layers, affected protocols, representative attacks, primary defenses, remaining gaps, research priority (High/Medium), and priority research needs.

Table 3. Original Synthesis Matrix: Threat-Layer-Defense Analysis with Defense Gaps, Priority, and Research Needs.

Threat Category	Target Layer	Affected Protocols	Representative Attack	Primary Defense	Defense Gap	Priority	Research Need
Default credentials	Device	All	Mirai botnet	Mandatory credential change at setup	User noncompliance; no enforcement mechanism	High	UX-enforced secure onboarding; policy mandates
Buffer overflow/RCE	Device firmware	All	CVE-based remote code execution	Secure coding; memory-safe languages	Constrained HW; decade-long update cycles	High	Automated firmware analysis; post-EOL patching
Firmware tampering	Device	All	Persistent backdoor implant	Secure boot + cryptographically signed OTA	Complex key mgmt; legacy devices excluded	High	Lightweight secure boot for Class 1 devices (≤ 128 KB)
MitM/eavesdropping	Network	Wi-Fi, Zigbee, BLE	Credential theft; command injection	TLS 1.3/DTLS; WPA3-SAE	TLS misconfiguration; legacy downgrade attacks	High	Automated TLS config auditing; protocol enforcement
DDoS/botnet	Network	IP-based: Wi-Fi, Thread	Volumetric service disruption	Rate-limiting; ISP-level filtering; segmentation	Static rules fail novel botnet variants	High	AI behavioral anomaly detection at gateway
Replay attack	Network/Auth	All auth protocols	Authentication bypass	Nonce-based challenge-response	Implementation variability across vendors	Medium	Standardized lightweight auth protocol (ED-HOC/OSCORE)

Table 3. Cont.

Threat Category	Target Layer	Affected Protocols	Representative Attack	Primary Defense	Defense Gap	Priority	Research Need
Cross-app interference	Application	Automation platforms	Unauthorized device command via app logic	App permission model; event sandboxing	Incomplete isolation in current Matter/Alexa/GH platforms	High	Formal verification of automation trigger logic
Insecure cloud API	Cloud	REST/MQTT	Mass-device takeover via single endpoint	OAuth 2.0; API gateway; rate-limiting	Third-party integrations bypass API controls	Medium	Automated API security testing; penetration requirements
Supply chain attack	Device/Cloud	All	Malicious firmware via OTA update	Code signing; vendor attestation	Trust anchored at manufacturer; no independent audit	High	Third-party firmware binary auditing frameworks
Behavioral profiling	Application/Cloud	All data streams	Passive occupancy/lifestyle inference	Data minimization; differential privacy	Incomplete regulatory enforcement; no technical standard	High	Privacy—preserving local analytics at edge gateway

5. Privacy Challenges in Smart Home IoT

Privacy and security constitute distinct but intersecting risk dimensions. Security threats target device integrity and service availability; privacy risks arise from the systematic collection, retention, and sharing of behavioral data, independently of any external attack. Smart home devices generate rich profiles: occupancy patterns, sleep schedules, dietary habits, and health trajectories. Data minimization deficiencies are widespread: empirical analysis shows that devices collect substantially more data than their stated function requires, with data transmitted to manufacturer cloud servers without meaningful user visibility or control [29].

Inference attacks present a significant privacy risk. Sub-second smart meter readings can identify individual appliances and accurately infer occupancy without any device compromise [30]. Encrypted traffic metadata alone, packet timing, size, and frequency, can identify device types and infer domestic activities without decryption [21]. Robotic vacuum cleaners that generate floor-plan maps represent a recently identified category of high-sensitivity data with unclear data governance [29].

The regulatory landscape is evolving, but enforcement remains incomplete. GDPR imposes data minimization, purpose limitation, and right-to-erasure requirements. The EU Cyber Resilience Act (CRA, entering force October 2024) mandates security-by-design and vulnerability disclosure for all connected products marketed in the EU [31]. The UK Product Security and Telecommunications Infrastructure (PSTI) Act (2024) bans default passwords and requires published vulnerability disclosure policies. The US IoT Cybersecurity Improvement Act requires NIST-aligned security standards for government-procured IoT [32]. Empirical research demonstrates that even technically sophisticated users remain uncertain about what their devices collect and what mitigations are available [33].

6. Existing Security Mechanisms

6.1. Authentication and Access Control

MFA combining knowledge, possession, and biometric factors is the current best practice for smart home access management. Matter mandates certificate-based device attestation via PKI, ensuring cryptographic device identity verification at commissioning [16]. ABAC and RBAC provide fine-grained authorization differentiation [34]. Practical

certificate management for non-technical households remains unresolved, and certificate revocation infrastructure for consumer IoT devices is largely absent, unlike in enterprise PKI deployments.

6.2. Encryption and Secure Communication

TLS 1.3 and DTLS provide channel encryption for device-to-cloud and device-to-device communication. CoAP with DTLS and MQTT with TLS are the dominant application-layer implementations [35]. WPA3 with Simultaneous Authentication of Equals (SAE) addresses the KRACK and dictionary attack vulnerabilities of WPA2-PSK [36]. A persistent operational problem is TLS misconfiguration, expired certificates, weak cipher suites, and disabled validation, which undermines encryption even where nominally deployed [11].

6.3. Intrusion Detection Systems

Network-based IDS monitor smart home traffic for signatures or behavioral anomalies. Rule-based systems fail against novel vectors; anomaly-based systems are more robust but require per-device baselines and are sensitive to legitimate behavioral changes that generate false positives [27]. Practical edge deployment on constrained home routers, rather than the cloud, remains architecturally and computationally challenging for current gateway hardware generations.

6.4. Firmware Update Security

Cryptographically signed OTA updates with preinstallation verification are the mandatory baseline. Because appliances often remain in service for a decade beyond firmware support, a substantial and growing fraction of deployed devices carry unpatched CVEs [6]. Potential systemic mitigations include mandatory minimum update support periods (proposed in CRA and PSTI), community-maintained open-source firmware, and ISP-level network-layer protection for end-of-life devices.

7. Emerging Solutions: Capabilities and Limitations

7.1. AI-Based Threat Detection: Capabilities, Datasets, and Limitations

AI and machine learning can complement rule-based systems by identifying previously unseen traffic patterns. LSTM networks for temporal traffic analysis and CNNs for static feature extraction have shown strong performance in detecting IoT botnet traffic and intrusion patterns in controlled settings [37]. Federated learning can reduce the privacy risks associated with centralizing residential traffic for model training: local models are trained on each home gateway, while only parameter updates are shared with a central aggregator [38].

Several limitations affect the practical use of these methods:

- **False Positive Rate:** Models trained on one household's behavioral baseline perform poorly in others due to occupant and appliance diversity. False alarm rates of even 1% translate to multiple false alerts per day in a home with tens of devices, a level that rapidly erodes user trust and leads to system disablement [39].
- **Dataset Limitations:** Most published results use laboratory or synthetic datasets (e.g., N-BaIoT, MedBIoT, IoT-23, Edge-IIoTset [40]) that do not reflect real residential behavioral variability, device heterogeneity, or legitimate traffic evolution over months. The absence of longitudinal, demographically diverse real-home datasets is a fundamental constraint on progress [37,38].
- **Adversarial Robustness:** Adversarial traffic crafting, generating device communications that evade an anomaly model while conducting an attack, is underexplored in smart home literature. Evasion attacks against smart home physical event verification

have been demonstrated [39], but systematic adversarial robustness evaluation is absent from most published IDS proposals.

- **Edge Deployment Constraints:** Capable AI inference on Class 1 IoT devices (≤ 128 KB RAM) remains infeasible with current model architectures. Gateway-class deployment (e.g., home router with 256 MB+ RAM) is achievable but requires model compression and quantization techniques [41,42].
- **Explainability:** IDS systems for domestic users must explain decisions in non-technical language to be actionable. The explainability gap between high-performance deep learning models and user-comprehensible outputs is an unresolved design challenge.

AI-based detection can still be useful at the gateway level, but its practical use depends on these constraints.

7.2. Blockchain for Smart Home Security: Potential and Limitations

Blockchain's properties, decentralization, immutability, cryptographic verification, and smart contract-based access control, map onto several smart home security requirements. Decentralized identity systems enable device attestation without dependence on manufacturer certificate authorities [10,43]. Immutable audit logs provide forensic evidence. Smart contract policies can be enforced cryptographically [44].

Consortium blockchain architectures, in which a defined set of trusted nodes collectively validate transactions, are proposed for smart home environments as a balance between decentralization and real-time IoT performance [11]. This choice is technically necessary: public blockchain Proof-of-Work consensus is computationally and energetically infeasible on smart home microcontrollers. Even Proof-of-Stake variants impose latency incompatible with time-sensitive actuation such as lock release or alarm triggering.

In most smart home scenarios, however, blockchain remained largely theoretical in 2025. The main issue is architectural fit: trustless decentralization and censorship resistance are rarely necessary in a domestic threat model dominated by external attackers. A properly configured local controller using PKI, hardware security modules (HSMs), or secure enclaves can provide comparable authentication and integrity with lower latency, energy use, and implementation complexity. Before adopting blockchain, practitioners should identify which required property cannot be provided by standard PKI or a trusted local controller [45]. Blockchain may offer distinct value in narrower settings that require verifiable multi-party audit trails, such as rental properties, elder-care environments with multiple caregivers, or insurance-verified security claims. These use cases require further empirical evaluation.

8. Future Research Directions and Practical Recommendations

8.1. Research Priorities Derived from Identified Gaps

- **AI False Positive Reduction and Cross-Household Generalization:** Transfer learning, domain adaptation, and online learning for smart home profiles; longitudinal real-home benchmark datasets; adversarial robustness evaluation protocols.
- **Lightweight Cryptography and Secure Boot for Class 1 Devices:** Integration of NIST ASCON (standardized 2023) [46] into secure boot and attestation for devices ≤ 128 KB RAM at commercially viable cost.
- **Matter Third-Party Integration Security Audit:** Formal verification of cross-app interaction policies; independent auditing of Matter cloud-bridge implementations and SDK security.
- **Privacy-Preserving Local Analytics:** Edge-deployable differential privacy and homomorphic encryption at the gateway level, enabling household analytics without cloud exposure.

- 6G Smart Home Security Architecture: Security modeling for 6G-connected smart homes addressing network slicing, reconfigurable intelligent surfaces, and AI-native 6G trust models.
- Blockchain Use Case Delimitation: Empirical definition of conditions where decentralized trust architectures outperform PKI; experimental comparison in rental and elder care deployments.
- User-Centered Security Design: HCI-grounded tools for non-expert users with automatic security baseline enforcement; co-design with elderly and accessibility-focused populations.

8.2. Stakeholder-Oriented Practical Recommendations

Table 4 presents structured recommendations for the four primary stakeholder groups whose actions collectively determine real-world smart home security outcomes.

Table 4. Stakeholder-Oriented Practical Recommendations.

Stakeholder	Recommended Action	Rationale/Evidence Link
Device Manufacturers	1. Prohibit default credentials; enforce unique per-device credentials at production. 2. Implement secure boot with cryptographically signed firmware on all new devices. 3. Commit to minimum 5-year post-sale OTA security update support. 4. Adopt NIST ASCON or equivalent lightweight cryptography for Class 1 devices.	Root cause of Mirai [Section 4.2]; Secure boot gap [Table 3]; Firmware lifecycle [Section 6.4]; NIST ASCON [Section 8.1]
Platform Providers (Ecosystem Operators)	1. Enforce permission isolation between third-party automation applications. 2. Independently audit Matter bridge implementations and cloud API endpoints. 3. Deploy certificate revocation infrastructure for all Matter-attested devices. 4. Implement AI-based anomaly detection at gateway/hub level with user-explainable alerts.	Cross-app interference [Table 3, Section 4.4]; Matter-related gaps [Sections 1.2 and 6.1]; Auth gap [Section 6.1]; AI IDS [Section 7.1]
End Users	1. Enable automatic firmware updates on all smart home devices. 2. Segment IoT devices onto a dedicated VLAN or guest network. 3. Replace default credentials immediately on device setup. 4. Review and revoke unnecessary third-party application permissions periodically.	Update gap: 76% aware, 24% act [Section 1]; Network segmentation [Table 3]; Default credential risk [Section 4.2]
Regulators and Standards Bodies	1. Mandate minimum 5-year security update obligations for all IoT devices (aligned with EU CRA) 2. Require security labeling/certification visible to consumers at point of sale. 3. Establish manufacturer liability for post-market security failures in consumer IoT. 4. Harmonize GDPR, CRA, PSTI, and NIST IoT guidelines into a unified international framework.	CRA/PSTI/NIST IR 8228 [Section 5]; Regulatory fragmentation [Section 5]; Privacy enforcement gap [Section 5]

9. Limitations

This survey has several limitations. First, although the PRISMA-informed methodology provides systematic coverage across five databases, restricting the search to English-language publications may exclude relevant work from other regions, particularly East

Asia. Second, the rapid evolution of IoT technologies means that findings related to specific protocol vulnerabilities and Matter limitations may need to be updated as new versions are released. Third, this review focuses primarily on consumer-grade smart home devices; industrial and enterprise IoT deployments with different threat models and regulatory requirements are outside its scope. Fourth, the High/Medium priorities in the Threat-Layer-Defense matrix (Table 3) reflect the authors' assessment of the available evidence rather than a formal meta-analytic ranking. Fifth, the conclusions regarding AI-based detection and blockchain reflect the current state of these technologies; advances in federated learning, edge computing, and zero-knowledge proofs may change the applicability boundaries described in Section 7. Finally, the stakeholder recommendations in Section 8 are derived from the reviewed literature and expert judgment rather than empirical validation with manufacturers or end users.

10. Conclusions

This review analyzed 233 sources using a PRISMA-informed process and combined the findings in a discussion of communication protocols, the Threat-Layer-Defense matrix in Table 3, an evaluation of AI-based detection and blockchain, and stakeholder recommendations.

The findings address the five research questions. Communication protocols differ in their security trade-offs, and Matter improves device attestation and interoperability but does not eliminate risks associated with legacy devices. Default credentials, buffer overflows, and DDoS-related weaknesses remain persistent threats, while Table 3 links these threats to defenses, unresolved gaps, and research priorities. AI-based detection is most promising at the gateway level but remains constrained by false positives, dataset limitations, and adversarial robustness; blockchain is useful mainly in multi-party audit settings where PKI alone is insufficient. Privacy risks arising from behavioral profiling require both technical safeguards and stakeholder action.

Overall, wider deployment of secure smart home systems will require stronger standards and regulatory support for credential management, firmware updates, and minimum encryption requirements. Matter addresses important architectural weaknesses, although its benefits apply mainly to newer devices. Gateway-level AI can support anomaly detection when false positives are managed, but it should not be presented as comprehensive protection. Privacy also requires data minimization, local processing where feasible, and enforceable privacy-by-design requirements at the device and platform levels.

Future empirical work will target validation of the threat taxonomy through real-world smart home network datasets and experimental evaluation of federated AI security models under longitudinal residential deployment conditions.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/bdcc10080252/s1>. Table S1: PRISMA 2020 Checklist; Table S2: Study Characteristics of Included Sources.

Author Contributions: Conceptualization, D.R.; methodology, D.R.; software, D.R., J.J., P.K. and N.S.; validation, D.R., J.J., P.K. and N.S.; formal analysis, D.R.; investigation, D.R., J.J., P.K. and N.S.; data curation, J.J., P.K. and N.S.; writing—original draft preparation, D.R.; writing—review and editing, D.R., J.J., P.K. and N.S.; visualization, J.J., P.K. and N.S.; supervision, D.R.; project administration, D.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT (GPT-5.5) for grammar checking and language refinement of selected passages. The authors have 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.

Abbreviations

The following abbreviations are used in this manuscript:

ABAC	Attribute-Based Access Control
AAL	Ambient Assisted Living
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASCON	Authenticated Encryption (NIST Lightweight Cryptography Standard, 2023)
CoAP	Constrained Application Protocol
CRA	Cyber Resilience Act (EU)
CSA	Connectivity Standards Alliance
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
DoS	Denial of Service
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HCI	Human–Computer Interaction
HSM	Hardware Security Module
HVAC	Heating, Ventilation, and Air Conditioning
IDS	Intrusion Detection System
IoT	Internet of Things
ISP	Internet Service Provider
JTAG	Joint Test Action Group (hardware debug interface)
KRACK	Key Reinstallation Attack
LSTM	Long Short-Term Memory
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
MQTT	Message Queuing Telemetry Transport
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
OTA	Over-the-Air (update)
PKI	Public Key Infrastructure
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PSK	Pre-Shared Key
PSTI	Product Security and Telecommunications Infrastructure (Act, UK)
RBAC	Role-Based Access Control
REST	Representational State Transfer
RQ	Research Question
SAE	Simultaneous Authentication of Equals
SDK	Software Development Kit
SDN	Software-Defined Networking
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver–Transmitter

WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3

References

- Salih, K.O.M.; Rashid, T.A.; Radovanovic, D.; Bacanin, N. A Comprehensive Survey on the Internet of Things with the Industrial Marketplace. *Sensors* **2022**, *22*, 730. [CrossRef] [PubMed]
- Statista Research Department. Number of Smart Homes Worldwide 2020–2025. Statista. 2024. Available online: <https://www.statista.com/outlook/dmo/smart-home/worldwide> (accessed on 22 May 2026).
- Statista Research Department. Smart Home Device Shipments Worldwide 2020–2025. Statista. 2021. Available online: <https://www.statista.com/statistics/1223274/> (accessed on 22 May 2026).
- Statista Research Department. Smart Home. Statistics & Facts; Statista. 2025. Available online: <https://www.statista.com/topics/2430/smart-homes/> (accessed on 22 May 2026).
- Ericsson AB. *Ericsson Mobility Report November 2024*; Ericsson: Stockholm, Sweden, 2024. Available online: <https://www.ericsson.com/en/reports-and-papers/mobility-report> (accessed on 22 May 2026).
- Bitdefender; NETGEAR. *The 2024 IoT Security Landscape Report*; NETGEAR: San Jose, CA, USA, 2024. Available online: <https://www.netgear.com/hub/network/2024-iot-threat-report/> (accessed on 19 May 2026).
- Opara, V.; Chao, P.; Odera, D. Addressing IoT Vulnerabilities in Smart Homes. In *Proceedings of the 2025 8th International Conference on Software Engineering and Information Management (ICSEIM 2025)*; ACM: New York, NY, USA, 2025. [CrossRef]
- 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. [CrossRef]
- Yuan, B.; Wan, J.; Wu, Y.H.; Zou, D.; Chen, Z. On the Security of Smart Home Systems: A Survey. *J. Comput. Sci. Technol.* **2023**, *38*, 228–247. [CrossRef]
- Hammi, B.; Zeadally, S.; Khatoun, R.; Nebhen, J. Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. *Comput. Secur.* **2022**, *117*, 102677. [CrossRef]
- Bhuyan, M.; Kashiara, S.; Fall, D.; Taenaka, Y.; Kadobayashi, Y. A Survey on Blockchain, SDN and NFV for the Smart-Home Security. *Internet Things* **2022**, *20*, 100588. [CrossRef]
- Zia, M.F.; Siddiqua, M.; Ouameur, M.A.; Bagaa, M.; Al Turjman, F. Securing the Future: A Survey on Smart Home Security in IoT-Integrated Smart Cities. *Adv. Netw.* **2025**, *12*, 1–18. [CrossRef]
- Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87. [CrossRef]
- Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
- Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
- Connectivity Standards Alliance. *Matter Specification Version 1.3*; CSA: San Ramon, CA, USA, 2024. Available online: <https://csa-iot.org/developer-resource/specifications-download-request/> (accessed on 22 May 2026).
- Muccini, H.; Moghaddam, M.T. IoT Architectural Styles. In *Software Architecture*; Springer: Berlin, Germany, 2018; pp. 68–85. [CrossRef]
- Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]
- Chen, Z.; O'Neill, Z.; Wen, J.; Pradhan, O.; Yang, T.; Lu, X.; Lin, G.; Miyata, S.; Lee, S.; Shen, C.; et al. A Review of Data-Driven Fault Detection and Diagnostics for Building HVAC Systems. *Appl. Energy* **2023**, *339*, 121030. [CrossRef]
- Drgoña, J.; Arroyo, J.; Cupeiro Figueroa, I.; Blum, D.; Arendt, K.; Kim, D.; Ollé, E.P.; Oravec, J.; Wetter, M.; Vrabie, D.L.; et al. All You Need to Know About Model Predictive Control for Buildings. *Annu. Rev. Control* **2020**, *50*, 190–232. [CrossRef]
- Apthorpe, N.; Reisman, D.; Feamster, N. A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *arXiv* **2017**, arXiv:1705.06805. [CrossRef]
- Chowdhury, S.S.; Sarkar, S.; Syamal, S.; Sengupta, S.; Ghosh, S. IoT Based Smart Security and Home Automation System. In *Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 10–12 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 577–582. [CrossRef]
- Mamdiwar, S.D.; Shakruwala, Z.; Chadha, U.; Srinivasan, K.; Chang, C.Y. Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring. *Biosensors* **2021**, *11*, 372. [CrossRef] [PubMed]

24. Alhanahnah, M.; Stevens, C.; Chen, B.; Yan, Q.; Bagheri, H. IotCom: Dissecting Interaction Threats in IoT Systems. *IEEE Trans. Softw. Eng.* **2023**, *49*, 1523–1539. [\[CrossRef\]](#)
25. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19. *Sustain. Cities Soc.* **2021**, *75*, 103311. [\[CrossRef\]](#) [\[PubMed\]](#)
26. 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. [\[CrossRef\]](#)
27. Gelgi, M.; Guan, Y.; Arunachala, S.; Samba Siva Rao, M.; Dragoni, N. Systematic Literature Review of IoT Botnet DDoS Attacks and Evaluation of Detection Techniques. *Sensors* **2024**, *24*, 3571. [\[CrossRef\]](#) [\[PubMed\]](#)
28. Liu, P.; Zheng, Y.; Sun, C.; Qin, C.; Fang, D.; Liu, M.; Sun, L. FITS: Inferring Intermediate Taint Sources for Effective Vulnerability Analysis of IoT Device Firmware. In *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 4 (ASPLOS '23), Vancouver, BC, Canada, 25–29 March 2023*; ACM: New York, NY, USA, 2023; pp. 138–152. [\[CrossRef\]](#)
29. Magara, T. Internet of Things (IoT) of Smart Homes: Privacy and Security. *J. Electr. Comput. Eng.* **2024**, *2024*, 7716956. [\[CrossRef\]](#)
30. Vojkovic, G.; Milenkovic, M.; Katulic, T. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. *Bus. Syst. Res. J.* **2020**, *11*, 167–185. [\[CrossRef\]](#)
31. European Union Agency for Cybersecurity (ENISA). *Cybersecurity of Smart Home Devices*; ENISA: Athens, Greece, 2023. Available online: <https://www.enisa.europa.eu/publications/cybersecurity-of-smart-home-devices> (accessed on 22 May 2026).
32. NISTIR 8228; Considerations for Managing IoT Cybersecurity and Privacy Risks. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [\[CrossRef\]](#)
33. Löbner, S.; Tronnier, F.; Miller, L.; Lindemann, J. An In-Depth Analysis of Security and Privacy Concerns in Smart Home IoT Devices Through Expert User Interviews. In *Information Security Education—Challenges in the Digital Age*; IFIP Advances in Information and Communication Technology; Drevin, L., Leung, W.S., von Solms, S., Eds.; Springer: Cham, Switzerland, 2024; Volume 707, pp. 97–110. [\[CrossRef\]](#)
34. Al-Fuqaha, A.I.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [\[CrossRef\]](#)
35. Colakovic, A.; Hadzialic, M. Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues. *Comput. Netw.* **2018**, *144*, 17–39. [\[CrossRef\]](#)
36. Wi-Fi Alliance. *Wi-Fi CERTIFIED WPA3 Specification Version 3.0*; Wi-Fi Alliance: Austin, TX, USA, 2022. Available online: <https://www.wi-fi.org/file/wpa3-specification> (accessed on 22 May 2026).
37. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [\[CrossRef\]](#)
38. Nguyen, T.D.; Marchal, S.; Miettinen, M.; Fereidooni, H.; Asokan, N.; Sadeghi, A.R. DIOT: A Federated Self-Learning Anomaly Detection System for IoT. In *Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS 2019)*; IEEE: Piscataway, NJ, USA, 2019; pp. 756–767. [\[CrossRef\]](#)
39. Ozmen, M.O.; Song, R.; Farrukh, H.; Celik, Z.B. Evasion Attacks and Defenses on Smart Home Physical Event Verification. In *Proceedings of the 30th Annual Network and Distributed System Security Symposium (NDSS 2023)*; Internet Society: Reston, VA, USA, 2023. [\[CrossRef\]](#)
40. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access* **2022**, *10*, 40281–40306. [\[CrossRef\]](#)
41. Aazam, M.; Zeadally, S.; Harras, K.A. Deploying Fog Computing in Industrial IoT and Industry 4.0. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4674–4682. [\[CrossRef\]](#)
42. Lin, J.; Chen, W.-M.; Lin, Y.; Cohn, J.; Gan, C.; Han, S. MCUNet: Tiny Deep Learning on IoT Devices. In *Advances in Neural Information Processing Systems 33 (NeurIPS 2020)*; Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M.-F., Lin, H.-T., Eds.; Curran Associates, Inc.: Red Hook, NY, USA, 2020; Volume 33, pp. 11711–11722. Available online: <https://papers.nips.cc/paper/2020/hash/86c51678350f656dcc7f490a43946ee5-Abstract.html> (accessed on 22 May 2026).
43. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [\[CrossRef\]](#)
44. Elloh Adja, Y.C.; Hammi, B.; Serhrouchni, A.; Zeadally, S. A Blockchain-Based Certificate Revocation Management and Status Verification System. *Comput. Secur.* **2021**, *104*, 102209. [\[CrossRef\]](#)

45. Obaidat, M.A.; Rawashdeh, M.; Alja'afreh, M.; Abouali, M.; Thakur, K.; Karime, A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data Cogn. Comput.* **2024**, *8*, 174. [CrossRef]
46. National Institute of Standards and Technology. *Lightweight Cryptography Standardization: ASCON Selected*; NIST: Gaithersburg, MD, USA, 2023. Available online: <https://csrc.nist.gov/projects/lightweight-cryptography> (accessed on 22 May 2026).

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.