The Indonesian Journal of Computer Science
www.ijcs.net
Volume 15, Issue 5, October 2026
https://doi.org/10.33022/ijcs.v15i5.5240

A Comprehensive Review of IoT Vulnerability Assessment Frameworks and Security Approaches for Smart Building Environments

Ntshabele Koketso[1], Morongwe Molaba[2]
koketso.ntshabele@nwu.ac.za[1], morongwemolaba@gmail.com[2]
[1,2] Department of Computer Science, Faculty of Natural and Agricultural Sciences, North West University, Mafikeng Campus

Article Information

Received : 1 Sep 2026
Revised : 15 Sep 2026
Accepted : 25 Oct 2026

Keywords

IoT, Smart buildings, Security frameworks, Consumer devices, Machine learning

Abstract

The rapid growth of Internet of Things (IoT) devices has led to a huge increase in the usage of consumer and smart devices resulting in a significant expansion of the attack surface available to malicious actors, introducing a wide range of security vulnerabilities that existing assessment frameworks have struggled to adequately address. Despite growing research attention, majority of proposed vulnerability assessment approaches have been validated only in controlled or simulated environments, raising serious concerns about their real-world applicability, particularly in the heterogeneous conditions of consumer smart building and smart home environments. This paper presents a comprehensive review of 22 peer-reviewed studies on IoT vulnerability assessment, security frameworks, and countermeasure approaches, with a specific focus on their applicability to smart building environments. A thematic review of 22 peer-reviewed studies was conducted, analysing existing IoT security approaches, identifying vulnerabilities and attack types, the challenges facing current frameworks, and future research directions, with a specific focus on their applicability to smart building and consumer IoT environments. The analysis reveals that IoT vulnerability research remains fragmented, with no single framework comprehensively addressing the full security lifecycle from vulnerability discovery through to prevention. Scanning-based approaches are the most widely adopted for detection, while machine learning and federated learning methods show the most promise for scalable, accurate threat detection. However, most proposed solutions fail to account for the device heterogeneity, resource constraints, and shared infrastructure conditions of real-world smart building deployments. This paper identifies the key challenges in the field and recommends that future research prioritise validating frameworks in operational smart home, smart building and industrial IoT environments to assess whether laboratory results hold in practical applications.

Attribution-ShareAlike 4.0 International License

A. Introduction

Internet of Things (IoT) has become one of the defining technological develop-ments of the past decade, connecting billions of physical devices to the internet, and enabling them to sense, communicate, and act with minimal human intervention [3], [5]. From household appliances to industrial control systems, IoT adoption has ex-panded into nearly every sector of daily life, including the built environment. Smart buildings are one of the fastest-growing application domains for this technology, promising improved efficiency, convenience, and centralised control over building op-erations such as lighting, security, climate, and access management [7], [8], [18].

This growth, however, has not been matched by a corresponding maturity in se-curity practice. As IoT devices grow rapidly within smart building environments, they introduce a wide and often poorly understood attack surface. Unlike traditional IT in-frastructure, consumer-grade IoT devices are frequently designed with cost and con-venience prioritised over security, resulting in widespread weaknesses that can be ex-ploited by malicious actors [3], [20]. The literature consistently identifies a recurring cluster of vulnerabilities across device categories: weak or unchanged default creden-tials remain the most exploited weakness [4], [9]; frequent data transmission over un-encrypted channels, exposing communications to eavesdropping and man-in-the-middle attacks [7], [8]; outdated firmware and the absence of systematic patch management, which leave known vulnerabilities unaddressed long after patches become available [16]; and unnecessary open ports that enable remote discovery and exploitation at scale [10], [11]. These weaknesses are further worsened by the extreme heterogeneity of IoT hardware — the diversity of manufacturers, operating systems, and communication protocols which makes the application of uniform security con-trols impractical [3], [6]. Identifying and addressing these weaknesses requires struc-tured vulnerability assessment — the systematic process of identifying, quantifying, and prioritising security flaws within a system or network [1], [12].

Despite the severity of these challenges, the research community has not yet pro-duced a comprehensive, integrated vulnerability assessment framework validated un-der conditions that reflect the complexity of real-world consumer IoT deployments. Existing approaches remain largely fragmented, concentrating on individual detection techniques rather than addressing the full security lifecycle from vulnerability discov-ery through to prevention and remediation [1], [11]. Furthermore, majority of pro-posed frameworks have been evaluated only in idealised or partially simulated envi-ronments, with empirical validation in real-world smart building deployments re-maining the field's most critical and unresolved gap [1], [7], [12], [15], [17].

This paper presents a comprehensive review of 22 peer-reviewed studies on IoT vulnerability assessment frameworks, security approaches, and countermeasure strat-egies, with a specific focus on their relevance and applicability to smart building and consumer IoT environments. The review analyses existing security approaches, the vulnerabilities and attack types they target, the challenges facing current frameworks, and future research directions that remain unaddressed in the literature.

The remainder of the paper is structured as follows: Section B presents background and IoT architecture and smart building environments, Section C presents the related works. Section D discusses the research methods, and Section E presents the analysis of iot vulnerability assessment frameworks and security approaches while Section F presents the discussion. Section G presents possible research directions, lastly, Section H concludes the study.

B. Background

B.1 IoT Architecture and Smart Building Environments

Internet of Things refers to a network of physical devices embedded with sensors, software, and connectivity that enables them to collect and exchange data with minimal human intervention [3], [5]. IoT adoption has expanded across a wide range of application domains including healthcare, agriculture, industrial systems, and smart infrastructure, with smart buildings emerging as one of the fastest-growing deployment contexts [7], [18]. Smart buildings integrate consumer IoT devices into shared network infrastructure to automate lighting, security, climate control, and access management [8], [18].

Figure 1 illustrates the typical architecture of a consumer IoT smart building environment, showing four devices connected through a shared network gateway to the broader internet. As shown, the assessment host (Kali Linux) connects to the same shared gateway, enabling systematic vulnerability assessment of all devices from a single point, a configuration that reflects realistic network conditions in consumer smart building deployments.

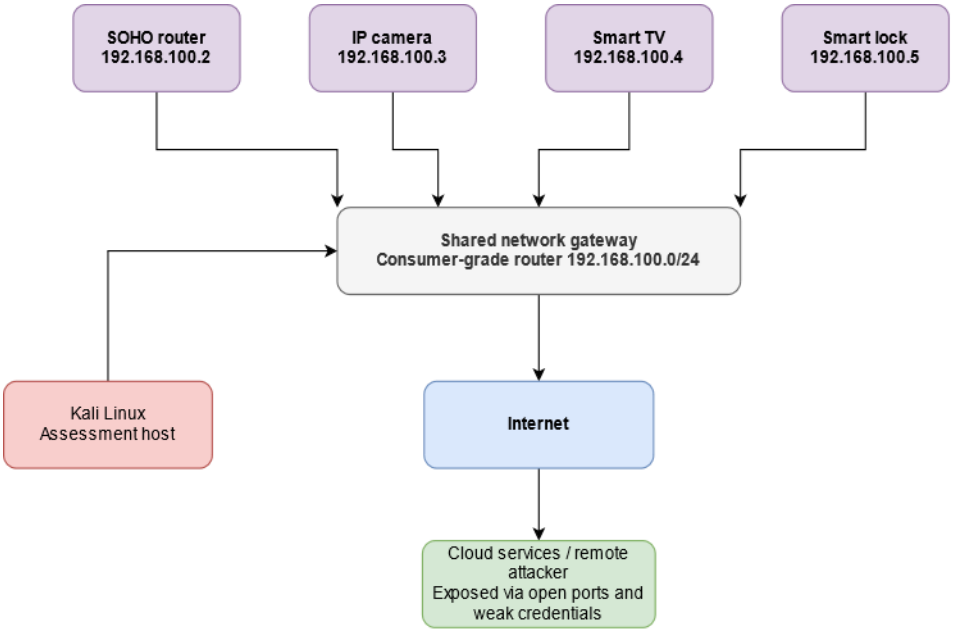

Figure 1. IoT smart building architecture

Unlike enterprise IoT environments, smart building deployments are characterized by consumer-grade infrastructure, heterogeneous device ecosystems spanning multiple manufacturers and communication protocols, and non-technical end users who rarely update firmware or change default credentials

[4], [6]. This combination of factors creates a particularly complex and often poorly understood attack surface. IoT devices are frequently designed with cost and convenience prioritized over security, resulting in widespread weaknesses across device categories [3], [20]. The literature reports that 70% of IoT devices contain exploitable security flaws, with each device carrying an average of 25 vulnerabilities [3].

B.2. Common IoT Security Vulnerabilities

The reviewed literature consistently identifies a recurring cluster of vulnerabilities across consumer IoT device categories. Understanding these vulnerabilities is foundational to evaluating the assessment frameworks designed to detect them.

Weak or default credentials are the most exploited vulnerability across all IoT device categories [2], [4], [9]. Many devices come with factory-set usernames and passwords that users rarely change, enabling unauthorized access without requiring sophisticated attack techniques. Poornachandran et al. [9] demonstrated this at scale by scanning the Indian Autonomous System Number space and finding that out of 14 209 routers identified, only 17% could be considered safe, with the majority either using default credentials or exposing sensitive configuration data without authentication.

Unencrypted communications represent the second most persistent vulnerability. Thomas [4] and Siboni et al. [7] document IoT devices transmitting sensitive data without encryption across protocols including HTTP, Telnet, and FTP, leaving communications exposed to eavesdropping and man-in-the-middle attacks. Mulero-Palencia and Monzon Baeza [8] found that in smart buildings, weaknesses in common protocols particularly HTTP/Apache HTTPD, SSH/OpenSSH, and FTP were more prevalent and exploitable than device-specific software flaws.

Outdated firmware and poor patch management leave known vulnerabilities unaddressed long after patches become available [16]. Bakhshi et al. [16] identify closed-source firmware as a structural barrier to vulnerability analysis, preventing security tools from inspecting device internals without physical access. Yu et al. [3] further note that where firmware update channels exist, they are often unencrypted and unauthenticated, creating an additional attack surface rather than reducing one.

Unnecessary open ports and poor network configuration enable remote discovery and exploitation at scale [2], [11]. Markowsky [2] demonstrated using Shodan, Masscan, and Nmap that many IoT devices are publicly discoverable and openly broadcast their device type, firmware version, and open ports, providing attackers with sufficient reconnaissance information to mount targeted attacks.

Device heterogeneity and resource constraints compound all of the above vulnerabilities. Yu et al. [3] and Almazrouei et al. [12] identify the diversity of IoT hardware — different CPU architectures, operating systems, communication protocols — as a fundamental obstacle to building unified security solutions. Chen et al. [6] note that resource constraints on IoT devices frequently prevent the full implementation of robust security algorithms, including complete TLS

implementations, blockchain nodes, or machine learning-based intrusion detection systems.

B.3. Common Security Attacks on IoT Devices

The vulnerabilities described above enable a wide range of attacks documented across the reviewed literature. Figure 2 maps each vulnerability category to the attack types it enables, showing how weaknesses at the device and network level translate into exploitable security incidents.

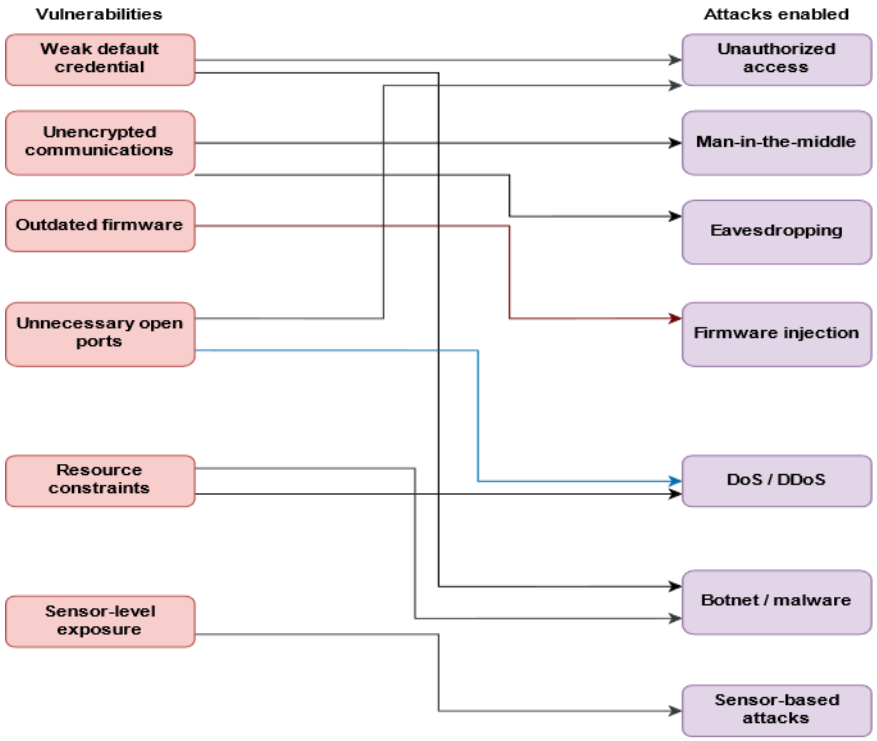

Figure 2. IoT vulnerability categories and the attack types enabled.

1. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks exploit the limited computational resources of IoT devices to overwhelm them with traffic, disrupting availability. Srivastava et al. [5] and Siwakoti et al. [10] both identify DDoS as among the most damaging attack types enabled by IoT vulnerabilities, noting the rise of organized criminal infrastructure including Impersonation-as-a-Service and Hack-for-hire services that weaponize compromised IoT devices into botnets for DDoS campaigns.
2. Man-in-the-middle (MITM) attacks intercept communications between IoT devices and servers, enabling credential theft and data manipulation. Poornachandran et al. [9] demonstrated that compromised SOHO routers can redirect DNS traffic to malicious servers, effectively enabling MITM attacks at the network infrastructure level without requiring device-level access.
3. Eavesdropping attacks exploit unencrypted communications to capture sensitive data in transit. Thomas [4] and Siboni et al. [7] both identify

eavesdropping as a direct consequence of plaintext data transmission over protocols such as Telnet, FTP, and unencrypted HTTP.

4. Firmware and physical attacks target the device itself rather than its network communications. Bakhshi et al. [16] classify firmware attacks into categories including malicious injection through unauthenticated update channels and exploitation of vulnerabilities in embedded software components. Aziz Al Kabir et al. [20] note that many IoT devices are physically accessible in consumer environments, making physical extraction of credentials and firmware a realistic attack vector.
5. Sensor-based attacks represent an often-overlooked attack surface specific to IoT devices. Sikder et al. [14] demonstrate that 60% of documented sensor-based attacks target sensors that operate without requiring explicit user permissions, making them accessible to malicious applications without triggering any security alerts.
6. Botnet recruitment and malware injection exploit weak credentials and unpatched firmware to compromise devices and enlist them into criminal infrastructure. Siwakoti et al. [10] document how IP cameras, security cameras, and routers are the most widely compromised device types for botnet recruitment, with Mirai being the most prominent example of large-scale IoT compromise enabled by default credentials left unchanged.

C. Related Works

Several existing review and survey studies have examined aspects of IoT security relevant to this paper, providing a foundation upon which this review builds while al-so highlighting the gaps it seeks to address.

Baho and Abawajy [1] conducted the most directly relevant systematic review, screening 1 479 papers and analysing 27 studies focused specifically on IoT vulnerabil-ity quantification frameworks. Their findings established that IoT vulnerability as-sessment research remains in its early stages, that existing frameworks are predomi-nantly adapted from conventional IT systems rather than purpose-built for IoT, and that the widely adopted Common Vulnerability Scoring System (CVSS) reflects famili-arity rather than suitability for the IoT context. Critically, they found that most frameworks had only been validated through simulation in controlled environments and called for validation on actual IoT networks. While this study provides the most comprehensive quantitative overview of existing frameworks, it does not examine specific assessment methodologies in depth, nor does it analyse smart building envi-ronments as a deployment context.

Similarly, Almazrouei et al. [12] conducted a systematic review of 34 journal arti-cles and 28 conference papers examining the use of attack graphs for IoT vulnerability assessment, finding that Bayesian network-based models performed best for handling uncertainty and association over time, while Markov Decision Process approaches struggled with NP-hard complexity at enterprise scale. Similarly, to Baho and Abawajy [1], they concluded that most proposed solutions remain limited to simulated or testbed environments, identifying empirical validation as the field's most pressing gap. While attack graph analysis offers a structured approach to modelling multi-step at-tack paths across heterogeneous

IoT ecosystems, it has not been applied within smart building environments specifically.

In Srivastava et al. [5], the authors examined IoT security threats across all layers of the IoT architecture through a survey of over 100 studies, finding that no single se-curity approach is sufficient to address the full spectrum of IoT vulnerabilities. Hybrid intrusion detection systems combining signature-based, anomaly-based, and specifica-tion-based detection performed best for threat coverage, while blockchain-based au-thentication showed the most promise for device identity and data integrity in future large-scale deployments. However, significant open challenges remained in scalability, standardisation, and real-time threat detection — challenges that are directly relevant to the smart building environment examined in this review.

In a similar study, Siwakoti et al. [10] reviewed 64 research papers, 19 surveys, and 12 white papers alongside CVE database and Shodan exposure data, finding that IP cameras, security cameras, and routers are the most widely vulnerable device types, and that AI and machine learning-based countermeasures offer the most promising defence against sophisticated IoT attacks. Alfahaid et al. [21] extended this finding through a comprehensive survey of machine learning-based IoT security solutions published between 2020 and 2024, concluding that federated learning and deep learn-ing performed best for privacy-preserving and high-accuracy threat detection respec-tively, though high computational costs and adversarial vulnerabilities remain open challenges for deployment on resource-constrained IoT devices.

Yu et al. [3] conducted a structured survey of vulnerability analysis, discovery, detection, and mitigation techniques across IoT devices, evaluating them against five criteria including attack surface coverage, technical requirements, architecture sup-port, operating system support, and AI integration. They found that network scanning methods such as Shodan and Censys performed best for large-scale detection of known vulnerabilities, while deep learning-based binary similarity detection methods showed the most promise for cross-architecture vulnerability detection. Bakhshi et al. [16] ex-tended this line of inquiry specifically to firmware, reviewing static, dynamic, and hy-brid auditing approaches and finding that hybrid techniques offered the most com-plete coverage, with machine learning and blockchain-based approaches identified as the most promising future directions for automating firmware security auditing across the heterogeneous IoT landscape.

Bustos et al. [11] addressed the fragmented state of domestic IoT security research through a PRISMA 2020 systematic review of 40 studies combined with Design Science Research Methodology, proposing a four-module theoretical framework covering vul-nerability knowledge, automated scanning, context-aware prioritisation, and stand-ardisation. Their context-aware prioritisation module was identified as the most sig-nificant contribution, ranking vulnerabilities by household-specific factors rather than generic CVSS severity metrics. However, the framework was evaluated through inter-nal consistency checks rather than real-world deployment, and its applicability to smart building environments beyond domestic settings was not examined.

As discussed above, while these existing review studies [1, 3, 5, 10, 11, 12, 16, 21] collectively document the vulnerability landscape, evaluate specific assessment tech-niques, and identify the absence of real-world validation as a persistent gap, none spe-cifically examines how vulnerability assessment frameworks perform within smart building environments under conditions that reflect the complexity of real consumer IoT deployments. Furthermore, no existing review integrates scanning-based, penetra-tion testing, traffic analysis, and firmware mapping approaches within a single empir-ical evaluation. This paper addresses both gaps by reviewing 22 studies across six thematic assessment categories and situating the analysis specifically within the smart building and consumer IoT context.

D. Research Method

The adopted research method for this review was designed to systematically analyze existing IoT vulnerability assessment frameworks, security approaches, and countermeasure strategies, with particular emphasis on their applicability to smart building and consumer IoT environments. To achieve this, the reviewed studies were classified into six major thematic categories: vulnerability detection and scanning, authentication and access control, encryption and secure communication, firmware vulnerability auditing, artificial intelligence and machine learning-based detection, and blockchain-based approaches. This classification reflects the diverse techniques currently employed to identify, assess, detect, mitigate, and manage security vulnerabilities across heterogeneous IoT environments.

Each thematic category was examined according to the assessment technique or framework employed, the IoT vulnerabilities and attack types addressed, the tools or technologies used, the evaluation environment, the reported findings or performance outcomes, and the limitations affecting practical deployment. Particular attention was given to whether the proposed approaches had been evaluated using simulations, controlled testbeds, organizational networks, or real-world consumer IoT and smart building environments. This evaluation criterion was considered important because the applicability of many existing IoT security approaches is influenced by device heterogeneity, limited computational resources, shared network infrastructure, diverse communication protocols, and the security practices of non-technical users.

Relevant peer-reviewed journal articles, conference papers, review studies, and other scholarly sources addressing IoT vulnerability assessment and security were selected from the available literature. The review focused primarily on studies that demonstrated direct relevance to IoT vulnerability discovery, detection, analysis, prioritization, or mitigation, while also considering their relevance to smart building and consumer IoT environments. The primary selection criteria included the relevance of the study to the research topic, the originality or technical contribution of the proposed approach, the range of vulnerabilities or attacks addressed, the presence of experimental, simulated, or empirical validation, and the identification of limitations or challenges affecting real-world implementation.

Studies were identified through IEEE Xplore and Google Scholar using combinations of the keywords “IoT vulnerability assessment”, “IoT security framework”, “smart building security”, and “consumer IoT vulnerabilities”. They were primarily selected from publications within the last five years to ensure the review reflects the current state of IoT vulnerability assessment research. A small number of older studies were also included where the issues, vulnerabilities, or techniques they discuss remain directly relevant to current IoT security challenges. For example, Mulliner's [22] 2009 NFC vulnerability analysis, and Markowsky's [2] and Poornachandran et al.'s [9] 2015 scanning methodologies, remain widely cited baseline techniques in current IoT security literature despite their age. Device-specific attack surfaces such as Bluetooth and NFC were considered relevant where the assessment techniques used are transferable to the broader IoT vulnerability assessment context [13], [22]. Studies were excluded if they did not address IoT vulnerability assessment, detection, or mitigation directly, or if they focused exclusively on enterprise, IT security with no IoT-specific component.

Information extracted from these studies was systematically compared across the six thematic categories to identify common approaches, strengths, limitations, and gaps in the current state of IoT vulnerability assessment research. The analysis also examined the relationship between vulnerability categories and the security attacks they enable, including unauthorized access, eavesdropping, man-in-the-middle attacks, denial-of-service attacks, malware and botnet recruitment, and firmware-level attacks.

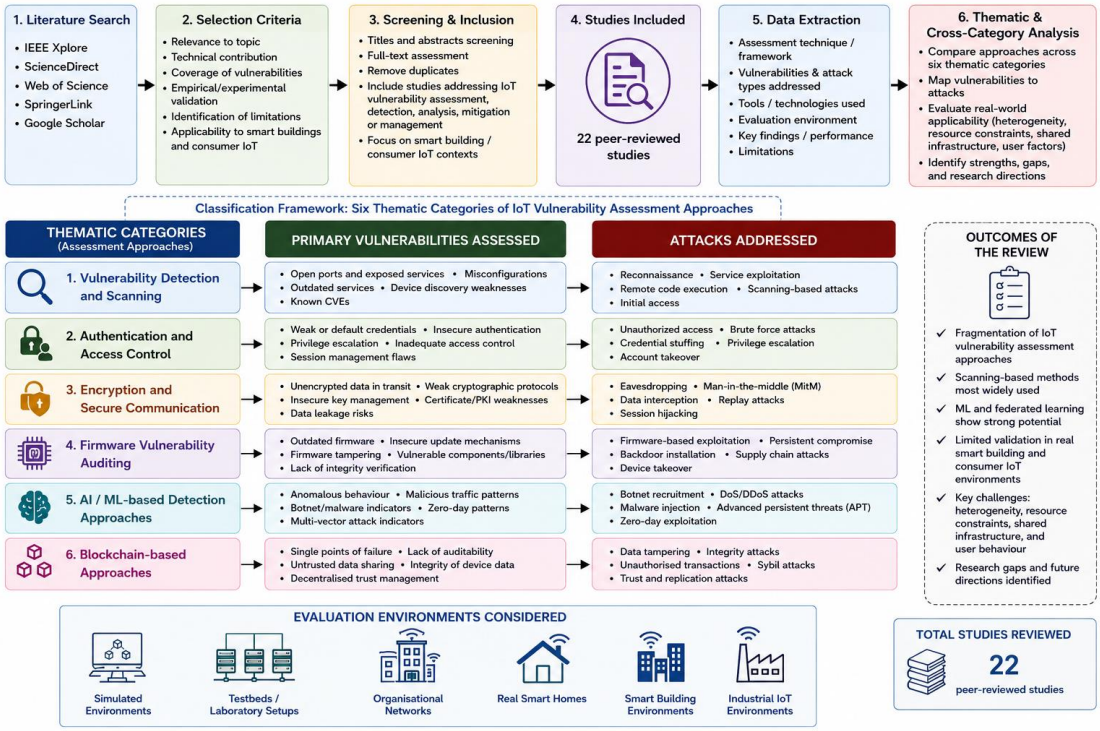

Figure 3. Methodology framework for IoT vulnerability assessment

Furthermore, a cross-category analysis was conducted to determine whether any individual assessment approach provides comprehensive coverage of the IoT security lifecycle, from vulnerability discovery and detection to exploitation

confirmation, prioritization, prevention, and remediation. The comparative analysis also considered the suitability of the reviewed approaches for heterogeneous and resource-constrained smart building environments. This enabled the study to identify three central issues across the reviewed literature: the fragmentation of existing IoT vulnerability assessment approaches, the limited representation of smart building environments as an evaluation context, and the continued lack of validation under realistic operational conditions.

The resulting thematic and cross-category analysis provides a structured basis for comparing existing IoT vulnerability assessment frameworks and identifying the research gaps that must be addressed to improve their practical applicability. Figure 3 presents the methodological relationship between the six thematic assessment categories, the major vulnerability areas they target, and the corresponding attack types addressed in the reviewed literature.

E. Analysis of IoT Vulnerability Assessment Frameworks and Security Approaches

This section presents a comprehensive analysis of the 22 peer-reviewed studies reviewed in this paper, organized across six thematic categories: vulnerability detection and scanning, authentication and access control, encryption and secure communication, AI and ML-based detection approaches, blockchain-based approaches, and firmware vulnerability auditing. The analysis examines the techniques and tools used, their strengths and limitations, and their applicability to smart building and consumer IoT environments. Tables 1 through 6 summarize the key findings per category, and Figure 3 provides a thematic overview of how the six categories relate to the vulnerability and attack landscape established in Section 2.

Figure 3 and Table 1 below maps each assessment category to the vulnerabilities it targets, and the attack types it addresses, providing a visual framework for the analysis that follows.

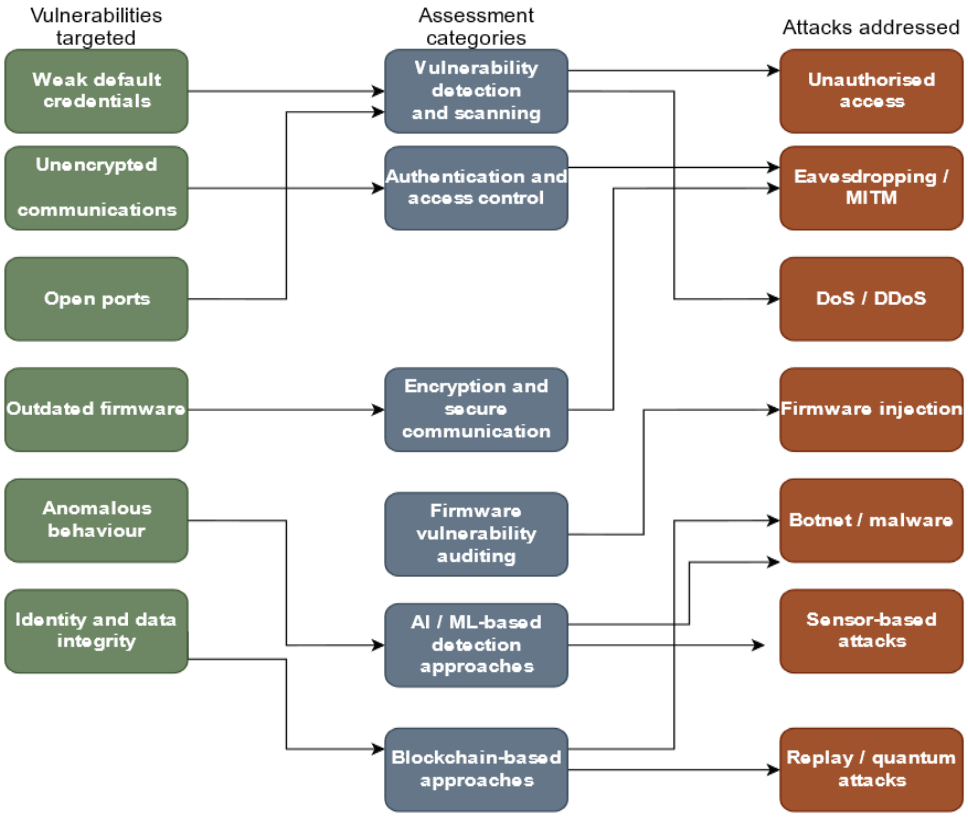

Figure 3. Thematic IoT vulnerability assessment

Table 1. Summary of Reviewed Studies Across Six IoT Security Assessment Categories

Studies	Vulnerability Detection and Scanning	Authentication and Access Control	Encryption and Secure Communication	Firmware Vulnerability Auditing	AI and Machine Learning-Based Detection Approaches	Blockchain-Based Approaches
[1]	☑					
[2]	☑					
[3]	☑		☑	☑	☑	
[4]	☑	☑				
[5]			☑			☑
[6]		☑	☑			
[7]	☑				☑	
[8]	☑	☑	☑			
[9]	☑	☑				
[10]	☑					☑
[11]	☑				☑	
[12]					☑	
[13]	☑					
[14]					☑	
[15]				☑		
[16]				☑		
[17]					☑	
[18]					☑	
[19]						☑
[20]				☑		
[21]					☑	
[22]	☑					

E.1. Vulnerability Detection and Scanning

Scanning and detection techniques are the most widely represented assessment category across the reviewed literature, forming the foundation of the majority of IoT vulnerability assessment approaches. These techniques range from passive internet-wide reconnaissance to active network scanning and custom-built tools tailored to specific device categories.

Markowsky [2] demonstrated three active scanning approaches using Shodan to identify vulnerable SOHO routers, Masscan to scan large address spaces for devices susceptible to the Heartbleed vulnerability, and Nmap combined with the Printer Exploitation Toolkit to locate exposed networked printers. The results showed that many IoT devices are publicly discoverable and openly broadcast their device type, firmware version, and open ports, providing attackers with

sufficient reconnaissance information for targeted exploitation. Shodan performed best as a broad reconnaissance tool due to its banner-indexing capability and integration with known vulnerability databases, though it is limited to publicly exposed devices and may produce false positives by matching exploits to service banners regardless of actual exploitability [2], [15].

Mulero-Palencia and Monzon Baeza [8] applied Shodan specifically to smart building environments, cross-referencing results against the CVE and NVD databases and scoring findings using the CVSS v3.1 framework. Their results showed that device-specific CVEs were less prevalent than weaknesses in common building protocols, particularly HTTP/Apache HTTPD, SSH/OpenSSH, and FTP with several devices found to be accessible without any authentication whatsoever. This finding is directly relevant to the smart building context and underscores the importance of protocol-level scanning alongside device-specific CVE mapping [8].

Siboni et al. [7] developed the most technically comprehensive scanning-based assessment in the reviewed literature — a modular, layer-based security testbed combining Nmap, Wireshark, Metasploit, and Nikto with custom analysis plugins. Applied across a range of real IoT devices including smart home appliances, cameras, and wearables, the testbed covered port scanning, fingerprinting, process enumeration, vulnerability scanning, fuzzing, DoS resilience measurement, and password complexity checking. The framework achieved strong results across all device categories, though the authors acknowledged that the controlled environment may not fully replicate the complexity of real-world consumer deployments [7].

Poornachandran et al. [9] developed a custom two-phase scanner combining TCP SYN probing and HTTP fingerprinting to target SOHO router vulnerabilities specifically. Scanning the Indian Autonomous System Number space over three months, they found that out of 14 209 routers identified, only 17% could be considered safe, the majority redirected DNS traffic to suspicious or malicious servers. The ROM-0 vulnerability proved the most severe, enabling complete unauthenticated extraction of router configuration files including admin passwords without any brute forcing [9].

Bustos et al. [11] proposed an Automated Scanning Engine as one module within their four-component theoretical framework for domestic IoT security, while also noting that traditional scanners such as Nmap and Masscan remain foundational for device discovery and port scanning but cannot detect deeper firmware-level vulnerabilities [11].

Table 2. Summary of Scanning and Detection Tools in IoT

Studies	Tool	Key Finding	Limitation
[2], [3], [8], [10]	Shodan / Censys	Best for large-scale passive reconnaissance; integrates with CVE/NVD	Limited to publicly exposed devices; false positives possible
[7], [4]	Nmap	Versatile; covers port scanning, fingerprinting, service enumeration	Cannot detect deep firmware vulnerabilities
[2]	Masscan	Extremely fast scanning of large address spaces	Limited depth of analysis
[7]	Nikto	Detects web server misconfigurations	Limited to web-facing services

		and known issues	
[7]	Metasploit	Validates real exploitability through active exploitation	Requires expertise; active use carries risks
[7], [4]	Wireshark	Detects unencrypted traffic and anomalous network behaviour	Passive; requires manual interpretation
[9], [11]	Custom scanners	Highly targeted detection for specific device categories	Not generalizable across device types

E.2. Authentication and Access Control

Authentication weaknesses are the primary attack vector across the reviewed literature, consistently identified as the most exploited vulnerability in consumer IoT devices. The studies reviewed examine both the nature of these weaknesses and the countermeasures proposed to address them.

Thomas [4] and Poornachandran et al. [9] both identify weak or unchanged default credentials as the root cause of the majority of IoT compromises studied, finding that even when technical vulnerabilities such as ROM-0 exist, default credentials provide the path of least resistance for attackers. Markowsky [2], Mulero-Palencia and Monzon Baeza [8], and Siwakoti et al. [10] reach the same conclusion across different device categories and scanning approaches — default credentials require no sophisticated attack technique, making them the single most accessible and most exploited vulnerability across consumer IoT deployments.

In response, Thomas [4] and Mulero-Palencia and Monzon Baeza [8] recommend two-factor authentication (2FA) as a primary countermeasure, showing measurable security improvement when implemented. Chen et al. [6] evaluate Role-Based Access Control (RBAC) within their IoT security taxonomy, finding that while it offers structured access management, resource constraints on IoT devices frequently limit its full implementation. Chen et al. [6] also assess ContexIoT, a context-sensitive permission system designed specifically for smart home IoT as a countermeasure against unauthorised access. Poornachandran et al. [9] recommend that ISPs enforce mandatory password change policies and implement random password generation as baseline access control measures for SOHO routers.

A persistent challenge identified across these studies is that proposed authentication countermeasures are frequently evaluated in isolation or in controlled settings, without addressing the practical realities of non-technical end users who rarely change default credentials or enable 2FA [4], [8], [9].

Table 3. Summary of Authentication and Access Control Mechanisms

Studies	Mechanism	Key Finding	Limitation
[4], [8]	Two-factor authentication (2FA)	Measurable security improvement against credential attacks	Affects usability; adoption low among non-technical users
[6]	Role-based access control (RBAC)	Structured access management	Resource constraints limit full implementation
[6]	ContexIoT	Context-sensitive permissions for smart home IoT	Limited to specific application scenarios
[9]	Mandatory password change / random generation	Reduces default credential exploitation	Requires ISP or manufacturer enforcement

E.3. Encryption and Secure Communication

Unencrypted communications represent the second most persistent vulnerability category across the reviewed literature, with multiple studies documenting IoT devices transmitting sensitive data in plaintext over protocols including HTTP, Telnet, and FTP.

Mulero-Palencia and Monzon Baeza [8] found HTTP and SSH-related weaknesses to be the most frequent vulnerability category across smart building devices, recommending strong TLS encryption as the primary countermeasure. Thomas [4] and Siboni et al. [7] both document unencrypted data transmission as a direct enabler of eavesdropping and man-in-the-middle attacks across the device categories they examined. Chen et al. [6] evaluate four encryption-related countermeasures within their IoT security taxonomy: TLS/HTTPS for communication encryption, encrypted firmware update channels, Message Authentication Codes (MACs) for data integrity in resource-constrained environments, and multi-path data transmission as a resilience mechanism against MITM attacks and DoS.

Yu et al. [3] and Srivastava et al. [5] both identify encrypted and authenticated firmware update channels as a critical countermeasure, noting that where update mechanisms do exist, they are frequently unencrypted and unauthenticated, creating an additional attack surface rather than reducing one. Bustos et al. [11] highlight the broader standardization challenge, noting that poor standardization across IoT communication protocols including MQTT, Zigbee, Z-Wave, BLE, and CoAP compounds the difficulty of applying uniform encryption standards across heterogeneous device ecosystems [11].

Table 4. Summary of Encryption and Secure Communication Techniques.

Studies	Technique	Key Finding	Limitation
[6], [8]	TLS / HTTPS	Primary countermeasure for communication encryption	Requires correct configuration to be effective
[3], [5]	Encrypted firmware updates	Prevents malicious firmware injection	Implementation overhead on resource-constrained devices
[6]	Message Authentication Codes	Lightweight integrity verification	Key management challenges
[6]	Multi-path transmission	Improves resilience against MITM and DoS	Increased network complexity

E.4. Firmware Vulnerability Auditing

Firmware-level vulnerabilities represent one of the most structurally challenging categories in IoT security, primarily because closed-source firmware prevents external inspection without physical device access, and because resource-constrained IoT devices are often unable to run traditional security analysis tools.

Bakhshi et al. [16] conducted the most comprehensive review of firmware vulnerability auditing techniques in the reviewed literature, systematically examining static, dynamic, and hybrid auditing approaches alongside their ability to scale and detect unknown attacks. Static analysis examines firmware images without execution, enabling broad vulnerability mapping but unable to detect runtime behaviours. Dynamic analysis monitors device behaviour during execution, capturing runtime vulnerabilities that static methods miss, but requires

a running device and cannot inspect code that never executes during the test session. Hybrid approaches combining both methods offer the most complete coverage, though they are significantly more resource-intensive [16]. Bakhshi et al. [16] identify machine learning and blockchain-based approaches as the most promising future directions for automating and scaling firmware security auditing across the heterogeneous IoT landscape.

Oser et al. [15] implemented SAFER — a semi-automated framework combining network-based device identification with automated firmware retrieval and NVD vulnerability mapping — and evaluated it on the large-scale heterogeneous network at CERN. SAFER successfully identified 531 of 572 devices (92.83% identification rate), analyzed 825 firmware images, and predicted current and future security risk for 240 devices, correctly predicting future risk for 91% of devices. This represents the strongest empirical firmware assessment result in the reviewed literature, though its evaluation remained within a controlled organizational network rather than a consumer smart building deployment [15].

Yu et al. [3] identify closed-source firmware as a structural barrier to analysis, with VulSeeker a deep learning-based binary similarity detection tool identified as the most promising approach for cross-architecture vulnerability detection, particularly relevant given the heterogeneous hardware landscape of consumer IoT [3].

Table 5. Summary of Firmware Vulnerability Auditing Approaches.

Studies	Technique	Key Finding	Limitation
[16], [3]	Static firmware analysis	Broad vulnerability mapping without execution	Cannot detect runtime behaviours
[16]	Dynamic firmware analysis	Captures runtime vulnerabilities	Requires running device; misses unexecuted code paths
[16]	Hybrid (static + dynamic)	Most complete coverage	Resource-intensive; complex to implement
[15]	NVD cross-referencing (SAFER)	92.83% device identification; 91% future risk prediction	Evaluated in organizational network, not consumer IoT
[3]	VulSeeker (deep learning)	Most promising for cross-architecture detection	Computationally intensive

E.5. AI and Machine Learning-Based Detection Approaches

Artificial intelligence and machine learning approaches are the fastest-growing assessment category in the reviewed literature, appearing across multiple studies as the most promising path toward scalable, automated IoT vulnerability detection and mitigation.

Siboni et al. [7] integrated ML-based anomaly detection and device-type identification into their modular IoT security testbed, achieving classification accuracy of 0.99 (±0.01) for known device types, 0.96 (±0.07) for unknown device types, and 100% true positive malware detection for the IP camera category. This represents the strongest ML performance result in the reviewed literature, though obtained under controlled testbed conditions [7]. Mothukuri et al. [17] addressed the privacy limitation of centralised ML approaches by implementing federated learning using Gated Recurrent Unit (GRU) models trained locally on IoT devices,

sharing only model weights rather than raw data. The federated GRU approach outperformed centralised ML baselines in both privacy preservation and attack detection accuracy, and outperformed LSTM-based models in computational efficiency during training [17].

Sikder et al. [14] evaluated context-aware intrusion detection systems (6thSense and Aegis) specifically designed for sensor-rich smart devices, finding detection accuracy exceeding 97% against sensor-based attacks — the highest IDS accuracy result across the reviewed literature. Almazrouei et al. [12] found that Bayesian network-based attack graph models are most effective for handling uncertainty and temporal relationships in IoT vulnerability assessments, while Markov Decision Process approaches struggle with NP-hard complexity at enterprise scale [12]. Bustos et al. [11] propose a Context-Aware Prioritisation Module that ranks vulnerabilities using contextual factors — device criticality, privacy impact, and external exposure — going beyond standard CVSS scores to reflect the practical risk profile of household IoT devices [11]. Siwakoti et al. [10] and Alfahaid et al. [21] both conclude that AI and machine learning represent the most flexible and scalable defence against evolving IoT attacks, though deployment on resource-constrained devices remains a significant practical challenge [10], [21].

Table 6. Summary of AI and ML-based Approaches

Studies	Technique	Key Finding	Limitation
[7]	ML anomaly detection	99% known device classification; 100% malware detection	Controlled testbed only; not validated in real deployments
[17]	Federated learning (GRU)	Outperforms centralized ML; privacy-preserving	Requires coordination infrastructure across devices
[14]	Context-aware IDS (6thSense, Aegis)	>97% detection accuracy for sensor-based attacks	Limited by device computational capability
[12]	Bayesian attack graphs	Best for uncertainty and temporal relationships	Scalability challenges at enterprise scale
[3]	VulSeeker (deep learning)	Most promising for cross-architecture detection	Computationally intensive for constrained devices
[11]	Context-aware prioritization	More practical than CVSS for household IoT	Requires rich contextual data to be effective

E.6. Blockchain-Based Approaches

Blockchain-based security solutions represent the least mature but most theoretically ambitious assessment category in the reviewed literature, with current studies identifying significant promise alongside unresolved practical challenges.

Srivastava et al. [5] identify blockchain-backed authentication as one of the most promising approaches for protecting device identities and ensuring data integrity in large-scale IoT environments, while simultaneously acknowledging that scalability and real-time performance requirements remain major unresolved challenges. Siwakoti et al. [10] classify blockchain as a countermeasure in their attack taxonomy, noting that while conceptually strong, its high resource requirements currently hinder practical deployment on resource constrained IoT devices [10].

Aleisa [19] presents the most fully developed blockchain-based framework in the reviewed literature — the Unified Quantum-Resilient Blockchain-Zero-Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF), which integrates blockchain with Zero Trust Architecture, post-quantum cryptography, and Zero-Knowledge Proofs for privacy-preserving authentication. Evaluated using Kaggle datasets, QBC-ZKPAF demonstrated protection against replay, side-channel, collusion, MITM, and quantum computing attacks including collusion attacks that none of the comparison models addressed. The Zero-Knowledge Proof component performed best for enabling authentication without revealing sensitive device information [19]. However, this framework was evaluated in a simulated environment and has not been deployed on actual resource constrained IoT devices, leaving its real-world applicability uncertain.

Table 7. Summary of Blockchain-based Approaches

Studies	Technique	Key Finding	Limitation
[5], [10]	Blockchain authentication	Strong device identity and data integrity protection	Scalability and energy consumption challenges
[19]	QBC-ZKPAF	Protection across all major attack categories including quantum	Simulated evaluation only; not deployed on IoT hardware

E.7. Summary and Cross-Category Analysis

The analysis across the six categories reveals several overarching patterns that are critical for contextualizing the findings within the smart building environment examined in this review.

First, no single assessment category addresses the full vulnerability lifecycle. Scanning tools detect vulnerabilities but cannot prevent exploitation; authentication mechanisms reduce the attack surface but do not detect intrusions; ML-based approaches detect anomalous behaviour but depend on training data and computational resources that resource-constrained IoT devices often cannot provide [3], [7], [10]. This fragmentation across categories directly confirms Baho and Abawajy's [1] finding that existing frameworks fail to address the full security lifecycle from discovery through to prevention.

Second, the smart building environment is underrepresented across all six categories. Only Muler/o-Palencia and Monzon Baeza [8] focus specifically on smart building deployments, all other studies examine generic IoT networks, consumer devices in isolation, or enterprise environments. This gap is particularly significant given the distinctive characteristics of smart building deployments, shared infrastructure, heterogeneous device ecosystems, consumer-grade routers, and non-technical users, which are not reflected in most of the testbed environments used to evaluate the frameworks reviewed.

Third, real-world validation remains absent across all six categories. As noted in Section 3, every category contains at least one study explicitly identifying simulation-only validation as a critical limitation [1], [7], [8], [11], [12], [15]. Even the strongest empirical results — Siboni et al.'s 99% classification accuracy [7] and Oser et al.'s 92.83% device identification rate [15] — were obtained in controlled

testbeds that the authors themselves acknowledge do not fully replicate real-world consumer IoT complexity.

F. Discussion

This section synthesises the findings of the comprehensive review presented in Section 4, drawing together the key themes that emerge across the six assessment categories and discussing their implications for IoT vulnerability assessment in smart building and consumer IoT environments.

F.1. Dominance of Scanning-Based Detection and Limits

The most consistent finding across the reviewed literature is the central role of network scanning tools particularly Shodan, Nmap, and Masscan — in IoT vulnerability detection. These tools are foundational across nearly all the assessment approaches reviewed and have demonstrated strong performance in their respective evaluation contexts [2], [3], [7], [8], [9]. However, a fundamental limitation emerges from the analysis: scanning-based approaches are effective at detecting the presence of vulnerabilities open ports, exposed services, default credentials, weak protocol configurations but they cannot confirm exploitability, detect runtime behaviours, analyse closed-source firmware internals, or prevent attacks once vulnerabilities are identified [11], [16]. As Bustos et al. [11] explicitly note, traditional scanners such as Nmap and Masscan remain unable to detect deeper firmware-level vulnerabilities, which represent one of the most persistent and structurally challenging categories in IoT security.

This limitation points to the need for multi-method assessment approaches that combine scanning with active penetration testing, traffic analysis, and firmware mapping.

F.2. Weak Default Credentials Remain the Most Persistent Vulnerability

Across all six assessment categories and across studies spanning 2015 to 2026, weak or unchanged default credentials are consistently identified as the single most exploited vulnerability in consumer IoT devices [2], [4], [8], [9], [10]. This finding has been documented for over a decade, but it remains unresolved despite the availability of straightforward countermeasures including mandatory password change policies, and random password generation [4], [8], [9]. The persistence of this vulnerability across the full-time span of the reviewed literature reflects a structural problem: proposed countermeasures are evaluated in controlled settings but are not enforced at the manufacturer or ISP level, and non-technical end users in smart building and consumer IoT environments rarely implement them voluntarily [9], [20]. This gap between known solutions and real-world adoption is itself a finding with direct implications for the practical recommendations this study will derive.

F.3. Smart Building Environments Are Underrepresented

A striking finding from the cross-category analysis is that only one study in the reviewed literature — Mulero-Palencia and Monzon Baeza [8] — focuses specifically on smart building deployments as an evaluation context. All other studies examine generic IoT networks, isolated consumer devices, or enterprise

environments. This is particularly significant given the distinctive characteristics of smart building deployments: shared network infrastructure, heterogeneous device ecosystems spanning multiple manufacturers and protocols, consumer-grade routers, and non-technical users who rarely update firmware or change default credentials [4], [6], [8]. Mulero-Palencia and Monzon Baeza's [8] finding that protocol-level weaknesses in HTTP, SSH, and FTP were more prevalent and exploitable than device-specific CVEs, suggests that the smart building context produces vulnerability patterns distinct from those found in generic IoT scanning studies, further emphasising the need for assessment approaches designed specifically for this environment.

F.4. AI and Machine Learning — Promising but Not Yet Deployable

The analysis of AI and ML-based approaches reveals a consistent pattern: these methods achieve the highest detection accuracy of any category reviewed, but their practical deployment on resource-constrained IoT devices remains a fundamental challenge. Siboni et al.'s [7] 99% classification accuracy and Sikder et al.'s [14] 97% IDS detection rate are the strongest performance figures in the reviewed literature, yet both were obtained under controlled conditions that do not reflect the computational constraints of real consumer IoT hardware. Mothukuri et al.'s [17] federated learning approach partially addresses this challenge by distributing training across devices rather than centralising it, but still requires coordination infrastructure that may not be available in consumer smart building deployments. Alfahaid et al. [21] identify this tension between the performance potential of advanced ML approaches and the resource constraints of the devices on which they must ultimately run as the defining open challenge in AI-driven IoT security research. As Siwakoti et al. [10] note, the development of lightweight ML models capable of running on constrained hardware is the most critical path toward making these approaches practically deployable.

F.5. The Absence of Real-World Validation — A Field-Wide Failure

The most significant finding of this review and the one most directly relevant to the gap this study addresses is the systematic absence of real-world empirical validation across all six assessment categories. This is not an isolated finding in one or two studies: it is noted explicitly as a critical limitation by Baho and Abawajy [1], Almazrouei et al. [12], Siboni et al. [7], Oser et al. [15], Mothukuri et al. [17], and Bustos et al. [11], spanning all six assessment categories. Even the frameworks that use real devices rather than purely simulated environments, most notably Siboni et al. [7] do so in controlled testbeds that the authors themselves acknowledge do not fully replicate the complexity of real consumer IoT deployments. The gap between what frameworks can achieve under idealised conditions and what they can demonstrate under the heterogeneous, resource-constrained, and user-behaviour-dependent conditions of actual smart building environments remains not just unaddressed but largely unacknowledged in the assessment methodology of most reviewed studies.

F.6. CVSS Inadequacy and the Need for IoT-Specific Frameworks

A final cross-cutting theme is the inadequacy of the Common Vulnerability Scoring System (CVSS) as a vulnerability prioritisation mechanism for IoT environments. Baho and Abawajy [1] find that CVSS dominates current IoT vulnerability quantification not because of its suitability but because of its familiarity, it was developed for traditional IT systems and does not account for IoT-specific properties such as physical access risks, resource constraints, device heterogeneity, or the household context of many deployments. Oser et al. [15] make the same observation, and Bustos et al. [11] propose the most concrete alternative: a Context-Aware Prioritisation Module that ranks vulnerabilities by device criticality, privacy impact, and external exposure rather than generic technical severity. This finding has direct implications for the framework evaluation component of this research, suggesting that any assessment framework applied to consumer smart building environments must be evaluated not only on its detection performance but on whether its prioritisation logic is meaningful in that specific deployment context.

G. Possible Reseach Directions

The findings of this review reveal several interconnected research directions that the field must urgently address. These directions emerge from the open challenges and limitations identified across all six assessment categories and are directly grounded in the recommendations made by the reviewed studies.

G.1. Real-World Empirical Validation

The most urgent and universally recommended direction is the validation of existing vulnerability assessment frameworks and tools in operational real-world IoT environments rather than simulated or controlled testbeds [1], [5], [7], [11], [12], [17]. While controlled evaluations have produced strong performance results such as Siboni et al.'s [7] 99% classification accuracy and Oser et al.'s [15] 92.83% device identification rate, the authors of both studies explicitly acknowledge that their environments do not fully replicate the complexity of real-world consumer IoT deployments. Future research should prioritise studies conducted in operational smart home, smart building, and industrial IoT environments to assess whether laboratory-derived results hold under practical conditions.

G.2. Development of IoT-Specific Vulnerability Frameworks

Baho and Abawajy [1], Oser et al. [15], and Bustos et al. [11] all call for vulnerability assessment frameworks specifically designed for IoT environments, rather than adaptations of IT-focused tools such as CVSS. The reviewed literature consistently shows that CVSS while the most widely adopted scoring system, was developed for traditional IT infrastructure, and does not account for IoT-specific properties including device heterogeneity, resource constraints, physical access risks, and the household or building context of many deployments [1], [15]. Next-generation frameworks should incorporate IoT-specific parameters and contextual severity assessment. The Context-Aware Prioritisation Module proposed by Bustos et al. [11] which ranks vulnerabilities by device criticality, privacy impact, and

external exposure rather than generic technical severity represents the most concrete template for this direction currently available in the literature.

G.3. Lightweight AI and Machine Learning Integration

Siwakoti et al. [10], Siboni et al. [7], Yu et al. [3], Mothukuri et al. [17], and Alfahaid et al. [21] all recommend AI and machine learning as the most promising path toward scalable, automated IoT vulnerability detection. However, a consistent finding across these studies is that the performance gains of advanced ML approaches come at a computational cost that resource constrained IoT devices cannot currently accommodate [10], [17], [21]. Specific future directions include: the development of lightweight ML models capable of running directly on constrained IoT hardware; federated learning approaches such as Mothukuri et al.'s [17] GRU-based framework that maintain privacy while enabling cross-device threat intelligence sharing; and deep learning-based binary similarity detection such as VulSeeker [3] for cross-architecture vulnerability identification across heterogeneous device ecosystems. Alfahaid et al. [21] additionally identify explainable AI and edge-based security frameworks as critical emerging directions for making ML-driven IoT security both interpretable and deployable.

G.4. Standardization of IoT Security Protocols

Bustos et al. [11], Srivastava et al. [5], Bakhshi et al. [16], and Chen et al. [6] all identify the absence of standardised security protocols across IoT communication stacks as a structural challenge that compounds every other vulnerability category reviewed. Poor standardisation across protocols including MQTT, Zigbee, Z-Wave, BLE, and CoAP prevents the application of uniform security controls across heterogeneous device ecosystems and makes holistic vulnerability assessment impractical at scale [11]. Future research and regulatory efforts should prioritise the development and enforcement of unified security standards across both protocols and device categories. Without standardisation, fragmented security solutions will continue to address individual protocols or device classes in isolation, leaving the system-level attack surface unaddressed.

G.5. Integrated Multi-Layered Security Architectures

Multiple studies conclude that isolated, single-layer defences are insufficient for securing IoT devices no single technique addresses the full vulnerability lifecycle from discovery through to prevention and remediation [6], [5], [7]. Future research should develop and evaluate architectures that integrate scanning tools, intrusion detection systems, authentication mechanisms, encryption, and AI-based anomaly detection into unified, deployable security frameworks applicable to consumer IoT environments. Srivastava et al. [5] identify hybrid IDS systems combining signature-based, anomaly-based, and specification-based detection as the best-performing multi-layer approach currently in the literature, a finding that points toward integration as the most productive direction for future framework development.

G.6. Addressing the Sensor-Level Attack Surface

Sikder et al. [14] identify sensor-based attacks particularly those exploiting sensors such as accelerometers, gyroscopes, microphones, and light sensors that operate without requiring explicit user permissions, as a critically under-addressed threat vector, accounting for 60% of documented sensor-driven attacks [14]. Yet many vulnerability assessment frameworks reviewed in this paper do not address sensor-level security at all. Future research should develop IoT-specific permission systems and context-aware monitoring mechanisms to protect the sensor layer, which currently sits outside the scope of most scanning, firmware, and network-level assessment approaches.

G.7. Scalable Blockchain Solutions for IoT Authentication

While Srivastava et al. [5] and Siwakoti et al. [10] identify blockchain-based authentication as theoretically promising for securing device identity and data integrity at scale, scalability, latency, and energy consumption remain unresolved challenges for deployment on resource-constrained IoT hardware. Aleisa's [19] QBC-ZKPAF framework demonstrates strong protection across all major attack categories in simulation but has not been evaluated on actual IoT devices. Future research should explore lightweight blockchain architectures or hybrid approaches that combine blockchain for identity management with lighter-weight protocols for data exchange, addressing the resource gap that currently prevents practical deployment.

G.8. User Education and Policy-Level Interventions

A recurring finding across the reviewed literature is that many of the most persistent IoT vulnerabilities particularly weak default credentials and absent firmware updates persist not because of a lack of technical solutions, but because of user behaviour and manufacturer incentives [4], [8], [9]. Poornachandran et al. [9] specifically recommend ISP-level enforcement of mandatory password change policies and random password generation as a baseline intervention. Thomas [4] and Mulero-Palencia and Monzon Baeza [8] both highlight that non-technical smart building users rarely implement available security measures voluntarily. Future research directions in this area include the development of usable security interfaces designed for non-technical users, ISP and manufacturer-level enforcement of secure default configurations, and regulatory frameworks that mandate minimum security standards for consumer IoT devices prior to market release addressing the structural gap between available solutions and real-world adoption.

H. Conclusion

This paper has presented a comprehensive review of 22 peer-reviewed studies on IoT vulnerability assessment frameworks, security approaches, and countermeasure strategies, with a specific focus on their relevance and applicability to smart building and consumer IoT environments. The review was organised across six thematic assessment categories — vulnerability detection and scanning, authentication and access control, encryption and secure communication, firmware vulnerability auditing, AI and ML-based detection

approaches, and blockchain-based approaches, and drew together the security challenges, open issues, and future research directions identified across all reviewed studies.

The analysis reveals that the IoT security research community has made meaningful progress in documenting the vulnerability landscape and developing individual assessment techniques. Scanning tools such as Shodan, Nmap, and Masscan have proven effective for large-scale device discovery and port enumeration [2], [3], [8]. Authentication countermeasures including two-factor authentication and role-based access control have demonstrated measurable security improvements [4], [6], [8]. Machine learning-based detection approaches particularly federated learning and context-aware intrusion detection systems have achieved the highest detection accuracy of any category reviewed, with Siboni et al. [7] reporting 99% classification accuracy and Sikder et al. [14] reporting over 97% detection accuracy against sensor-based attacks. Firmware auditing techniques, when combined into hybrid static and dynamic approaches, offer the most complete coverage of device-level vulnerabilities [16]. Blockchain-based frameworks such as QBC-ZKPAF [19] demonstrate comprehensive protection against emerging attack categories including quantum computing attacks that no comparison model addresses.

However, three overarching findings emerge from the analysis that collectively define the current state and future direction of the field. First, no single assessment category or technique addresses the full vulnerability lifecycle from discovery and detection through to exploitation confirmation, prioritisation, and remediation — confirming the fragmentation identified by Baho and Abawajy [1] as the field's defining structural weakness. Second, smart building environments remain significantly underrepresented as an evaluation context across all six assessment categories, with only Mulero-Palencia and Monzon Baeza [8] specifically targeting smart buildings, despite the distinctive vulnerability patterns these environments produce compared to generic IoT networks. Third, and most critically, real-world empirical validation is absent across all six assessment categories, even the strongest performance results in the reviewed literature were obtained under controlled conditions that the authors themselves acknowledge do not fully replicate real-world consumer IoT deployment complexity [1], [7], [11], [12], [15], [17].

These three findings converge on a single conclusion: the field has developed a range of technically capable vulnerability assessment approaches but has not yet demonstrated that they work under the conditions in which they must ultimately operate. The gap between laboratory performance and real-world applicability particularly in the heterogeneous, resource-constrained, and user-behaviour-dependent conditions of smart building environments remains the most critical and least addressed challenge in consumer IoT security research.

This paper contributes to addressing that gap by synthesising the existing evidence base across all major assessment categories, identifying the specific limitations that prevent existing frameworks from being deployed in smart building contexts, and establishing a foundation for empirical evaluation under realistic consumer IoT conditions. The eight research directions identified in Section 6 spanning real-world validation, IoT-specific framework development,

lightweight AI integration, protocol standardisation, multi-layered security architectures, sensor-level protection, scalable blockchain solutions, and user education collectively define the work that remains to be done to close the gap between what IoT vulnerability assessment frameworks can achieve in idealised environments and what they can demonstrate in the field.

I. Acknowledgment

This research This research was supported by the Unit for Data Science and Computing (UDSC) and the Department of Computer Science at the North-West University Mafikeng campus, South Africa

J. References

[1] S. A. Baho and J. Abawajy, "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks," *Electronics*, vol. 12, no. 5, p. 1176, 2023.

[2] L. M. G. Markowsky, "Scanning for Vulnerable Devices in the Internet of Things," in *Proc. 2015 IEEE 8th Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Warsaw, Poland, 2015, pp. 463–467.

[3] M. Yu et al., "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," *Future Internet*, vol. 12, no. 2, p. 27, 2020.

[4] J. Thomas, "Analysis of Vulnerabilities in IOT Devices and the Solutions," B.S. thesis, Dept. Computer Science, Texas Southern Univ., 2021.

[5] A. Srivastava et al., "Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," *Int. J. Communication Systems*, vol. 33, no. 12, p. e4443, 2020.

[6] K. Chen et al., "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," *J. Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, 2018.

[7] S. Siboni et al., "Security Testbed for Internet-of-Things Devices," *IEEE Trans. Reliability*, vol. 68, no. 1, pp. 23–44, 2019.

[8] S. Mulero-Palencia and V. Monzon Baeza, "Detection of vulnerabilities in smart buildings using the Shodan tool," *Electronics*, vol. 12, no. 23, p. 4815, 2023.

[9] P. Poornachandran et al., "Internet of Vulnerable Things (IoVT): Detecting Vulnerable SOHO Routers," in *Proc. 2015 Int. Conf. Information Technology (ICIT)*, Bhubaneswar, India, 2015, pp. 119–123.

[10] Y. R. Siwakoti et al., "Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures," *IEEE Internet of Things* J., vol. 10, no. 13, pp. 11224–11239, 2023.

[11] D. F. R. Bustos et al., "Automated Vulnerability Scanning and Prioritisation for Domestic IoT Devices/Smart Homes: A Theoretical Framework," *Electronics*, vol. 15, no. 2, p. 466, 2026.

[12] O. S. M. B. H. Almazrouei et al., "A review on attack graph analysis for IoT vulnerability assessment: challenges, open issues, and future directions," *IEEE Access*, vol. 11, pp. 44350–44376, 2023.

[13] L. Kavisankar et al., "A Comprehensive Bluetooth Security Audit Framework for IoT Devices," *Computers & Security*, p. 104840, 2026.

[14] A. K. Sikder et al., "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.
[15] P. Oser et al., "Risk prediction of IoT devices based on vulnerability analysis," *ACM Trans*. Privacy and Security, vol. 25, no. 2, pp. 1–36, 2022.
[16] T. Bakhshi et al., "A review of IoT firmware vulnerabilities and auditing techniques," *Sensors*, vol. 24, no. 2, p. 708, 2024.
[17] V. Mothukuri et al., "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things J*., vol. 9, no. 4, pp. 2545–2554, 2021.
[18] A. Bhardwaj et al., "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities," *Egyptian Informatics J*., vol. 25, p. 100443, 2024.
[19] M. A. Aleisa, "Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments," *IEEE Access*, 2025.
[20] M. Aziz Al Kabir et al., "Securing IoT devices against emerging security threats: Challenges and mitigation techniques," *J. Cyber Security Technology*, vol. 7, no. 4, pp. 199–223, 2023.
[21] A. Alfahaid et al., "Machine learning-based security solutions for IoT networks: A comprehensive survey," *Sensors*, vol. 25, no. 11, p. 3341, 2025.
[22] C. Mulliner, "Vulnerability analysis and attacks on NFC-enabled mobile phones," in *Proc. 2009 Int. Conf. Availability, Reliability and Security*, 2009.