ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

Cyber Physical Security and Interoperability Challenges in IoT Based Smart Building Systems A Narrative Critical Review

[1]Imran Muhammed Awwal; [2]Jamiu Lateef

[1]Department of Building, Obafemi Awolowo University, Ile-Ife, Nigeria

[2]Department of Civil and Environmental Engineering, Case Western Reserve University, Cleveland, United States.

Publication Date: 2025/12/29

Abstract: The proliferation of Internet of Things (IoT) devices within smart buildings has enabled significant advancements in operational efficiency, energy management, and occupant experience. This integration, however, converts modern buildings into complex cyber-physical systems (CPS), introducing a new class of vulnerabilities at the intersection of the digital and physical realms. This paper presents a narrative-critical review of the dual challenges confronting these environments: cyber-physical security and system interoperability. A taxonomy of threats is presented, highlighting attack vectors that range from data exfiltration to the physical disruption of building operations. Concurrently, the review investigates the pervasive issue of interoperability, where a fragmented ecosystem of proprietary protocols and data models creates systemic inefficiencies and profound security gaps. This paper critically analyzes current technical and architectural solutions, including AI-based intrusion detection, blockchain, middleware, and digital twins, evaluating their efficacy in addressing these intertwined challenges. This review's core contribution is the synthesis of these domains, arguing that the lack of semantic interoperability is an architectural flaw that precludes the effective deployment of modern security paradigms and that the systemic skills gap presents a non-technical barrier as significant as any technical challenge. The analysis culminates in a strategic research roadmap to address these coupled challenges holistically.

Keywords: *Smart Buildings, Internet of Things (IoT), Cyber-Physical Systems (CPS), Cybersecurity, Interoperability, Digital Twin, Intrusion Detection, Building Management Systems (BMS), Operational Technology (OT)*

How to Cite: Imran Muhammed Awwal; Jamiu Lateef (2025) Cyber Physical Security and Interoperability Challenges in IoT Based Smart Building Systems A Narrative Critical Review. *International Journal of Innovative Science and Research Technology*, 10(12), 1826-1835. https://doi.org/10.38124/ijisrt/25dec1366

I. INTRODUCTION

The smart building market is undergoing an accelerated transformation, with projections estimating its global value will exceed $570 billion by 2030 [1]. This growth is driven by the large-scale integration of Internet of Things (IoT) devices, which convert static structures into dynamic, data-rich, and interconnected cyber-physical systems [2]. The convergence of traditional Operational Technology (OT), such as HVAC and access control, with modern Information Technology (IT) and cloud platforms, promises unprecedented gains in efficiency. However, this hybrid ecosystem also creates a vastly expanded and heterogeneous attack surface. Recent cybersecurity reports indicate a significant surge in cyber-attacks targeting building automation systems, with threats evolving from theoretical risks to practical exploits [3, 4]

The challenges confronting the deployment of secure and efficient smart buildings are twofold and deeply interconnected. First, the cyber-physical security of these systems is a primary concern. Malicious actors can exploit vulnerabilities to manipulate essential building functions, including HVAC, lighting, and access control, due to increased connectivity and complexity [5]. The consequences extend far beyond data loss; they include the potential for physical disruption, large-scale energy fraud, operational shutdowns, and direct threats to occupant safety [6].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

Second, the smart building ecosystem suffers from profound interoperability issues. The market is characterized by a heterogeneity of communication protocols and proprietary, vendor-specific data models, which complicate integration and system coordination [7]. This fragmentation creates a disjointed operational environment. The lack of interoperability not only hinders unified management and data analytics but also directly complicates the uniform deployment of security policies. Security gaps often emerge at seams where disparate, poorly integrated systems meet, especially when open standards and shared data frameworks are absent [8].

While substantial research addresses these domains, it does so in a dangerously siloed manner, representing a field-wide blind spot. The existing literature is bifurcated. One stream focuses on high-level security mechanisms, such as developing trustworthy federated learning models for intrusion detection in 6G-connected buildings [9]. Another stream focuses on interoperability solutions, such as the semantic mapping of proprietary building data to standardized ontologies for compliance and integration [10]. The critical analysis of their intersection is not merely less common; its absence is a systemic failure. Even the most advanced AI-based security models are functionally useless if they cannot semantically understand the data they are monitoring, and a perfectly mapped ontology is insecure if the underlying devices are vulnerable.

This paper's core thesis is that cyber-physical security and interoperability are not parallel challenges but a single, deeply coupled problem. The lack of semantic interoperability is a fundamental architectural flaw that actively precludes the effective implementation of modern, holistic security paradigms like Zero Trust Architecture (ZTA), which depend on a unified understanding of identity, context, and data. This paper provides a narrative-critical review to prove this thesis, synthesizing these disparate domains. The objectives are: (1) to develop a taxonomy of cyber-physical threats grounded in empirical data; (2) to critically analyze the root causes of interoperability friction and its security implications; (3) to evaluate contemporary solutions, highlighting the systemic tension between top-down architectures and bottom-up device insecurity; and (4) to propose a formal strategic research roadmap.

II. OVERVIEW OF IOT-BASED SMART BUILDING SYSTEMS

To analyze these interconnected systems, a layered architectural model is essential. This paper adopts a generalized four-layer framework, as delineated in Figure 1 of the Brains4Buildings reference architecture, which illustrates the flow of data from physical sensing to user-facing applications [11]. This abstraction clarifies the distinct roles and security boundaries at each stage of operation. The Perception Layer represents the CPS interface, where digital commands become physically active. The Network Layer handles data transit, often bridging disparate media. The Middleware Layer acts as the "central nervous system" for data processing and abstraction [12]. Finally, the Application Layer provides human operators and tenants with control and insight.

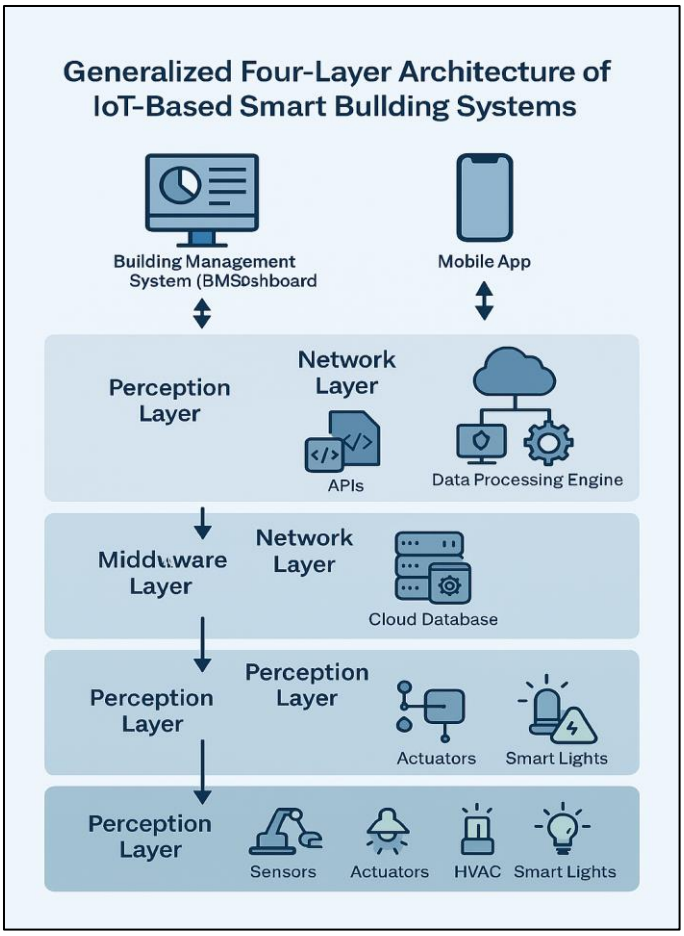

Fig 1: Generalized Four-Layer Architecture of IoT-Based Smart Building Systems

The functionality of this architecture is contingent upon a diverse and often incompatible set of communication protocols. This protocol fragmentation is a primary source of systemic friction. Table 1 presents a comparative analysis of the dominant protocols, categorizing them by their operational domain and key characteristics to highlight the sources of this heterogeneity.

This heterogeneity necessitates the use of gateways as critical network components. These gateways are the nexus of the entire problem this paper addresses. They are the choke points where protocol translation occurs (e.g., from Zigbee to IP), where data from disparate systems converges, and, consequently, where interoperability failures and security vulnerabilities are most acutely concentrated. These devices become high-value attack targets, and single points of failure are often managed as black boxes with minimal security oversight [13, 14].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

The coexistence of modern IT protocols like MQTT with legacy OT protocols such as BACnet is a defining feature of intelligent building systems. This mix, as illustrated by EMQ's Neuron framework, demands complex protocol translation at the gateway of an architectural weak point that can be exploited by attackers [15]. Trend Micro's research highlights how these gateways often lack proper security controls, making them critical points of failure [16]. Moreover, the complexity and frequent unencrypted deployment of BACnet/IP directly enable "BACnet-to-ransomware" attack vectors, as seen in recent threat analyses [17].

Table 1: Comparison of Common Smart Building Communication Protocols

Protocol	OSI Layer	Typical Use Case	Key Security/Interoperability Characteristic
BACnet	Application	Building Automation and Control (HVAC, Lighting)	Dominant standard in commercial OT; complex object model. Often deployed unencrypted (BACnet/IP), making it a prime attack target [18].
KNX	Application	Home and Building Control (Lighting, Blinds, Security)	Robust, decentralized, and standardized (ISO/IEC 14543). Security [19] is available but not universally adopted.
Zigbee	Network/MAC	Low-power wireless sensor networks (Sensors, Lighting)	Mesh networking; low data rate; security is reliant on correct key management, which is often implemented poorly [20]
MQTT	Application	IoT device-to-cloud communication	Lightweights publish/subscribe model; ideal for cloud integration. Security relies on TLS and robust broker access control. [21]
CoAP	Application	Constrained device communication	Lightweight request/response model; UDP-based. Security is achieved via DTLS, which adds overhead. [22]
Wi-Fi	Network/Data Link	High-bandwidth data (Cameras, User Devices)	Ubiquitous in IT environments; requires careful network segmentation (e.g., VLANs) to isolate OT traffic [23]

III. CYBER-PHYSICAL SECURITY THREATS AND VULNERABILITIES

The convergence of IT and OT in smart buildings introduces cyber-physical threats, where digital attacks produce tangible physical consequences. To systematically analyze these vectors, this paper proposes a cyber-physical attack taxonomy, presented in Figure 2, which classifies threats based on their primary impact domain: confidentiality, integrity, availability, and composite cyber-physical manipulation [24].

This attack surface is not theoretical; it is empirically demonstrable. A recent firmware security analysis using the EMBA framework revealed that Building Automation System (BAS) devices often contain thousands of Common Vulnerabilities and Exposures (CVEs) per image, with some scans reporting over 1,500 CVEs per firmware highlighting the systemic insecurity of smart building foundations [25].

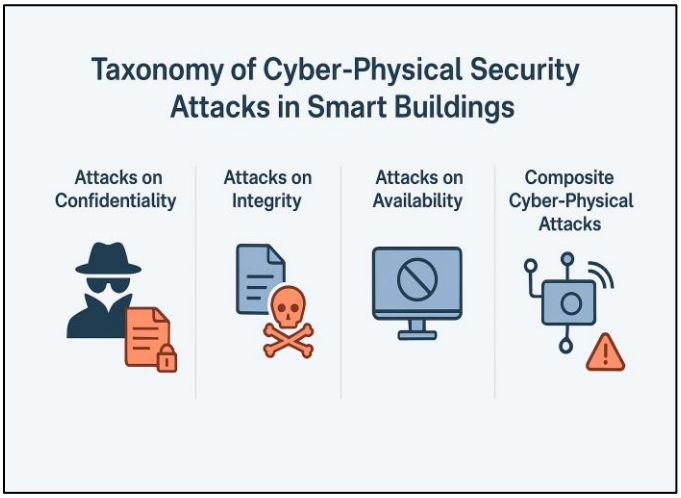

Fig 2: Taxonomy of Cyber-Physical Security Attacks in Smart Buildings

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

Recent case studies validate these threats. Vulnerability cascades like Ripple20 and Urgent/11 affected low-level TCP/IP stacks embedded in millions of smart devices, including building controllers exposing them to remote code execution and denial-of-service attacks [26, 27].

Security researchers at the 2024 Black Hat conference highlighted a BACnet-to-ransomware attack path, where adversaries exploited an unauthenticated BACnet/IP port on an HVAC controller to pivot into the central Building Management System (BMS), ultimately encrypting its database and disabling ventilation [28].

The empirical data on firmware vulnerabilities exposes a critical tension at the heart of the smart building paradigm: the dichotomy between top-down architectural ideals and the bottom-up reality of device-level insecurity. While the literature proposes sophisticated, high-level solutions such as secure fog computing [29] and Digital Twins [30], these frameworks attempt to impose systemic order from a holistic vantage point. However, firmware-level analyses reveal that the foundational components of these architectures of smart sensors, controllers, and embedded systems are riddled with known CVEs, often stemming from outdated or vulnerable TCP/IP stacks and embedded web servers. A conceptually flawless Zero Trust Architecture (ZTA) becomes futile if it rests on devices that can be compromised at the firmware level. This contradiction underscores a vital truth: security must be embedded from the supply chain upward, not retrofitted as an architectural afterthought.

IV. INTEROPERABILITY ISSUES IN SMART BUILDING SYSTEMS

Interoperability, the ability of systems from different vendors to exchange and make use of information, remains a primary obstacle to creating truly smart and secure buildings. This lack of Interoperability manifests across multiple technical and semantic layers, generating distinct friction points that hinder seamless integration. Table 2 deconstructs this issue by identifying the primary challenges at each layer and mapping the direct security implications that arise from them. As Froehlich explains [31], misalignment between building technology integration, interoperability, and security often stems from inconsistent design and deployment practices, leading to fragmented systems that fail to meet performance and compliance expectations.

Table 2: Interoperability Friction Points and Their Security Implications

Layer of Interoperability	Description of Challenge	Direct Security Implication
Technical (Network)	Incompatible communication protocols (e.g., Zigbee vs. BACnet/IP). Requires complex gateways.	Gateways become single points of failure and high-value attack targets; security policies are difficult to enforce uniformly across protocol boundaries.
Syntactic (Data Format)	Systems use different data formats and encoding (e.g., JSON, XML, proprietary binary).	Data translation at gateways can be computationally expensive, creating latency that hinders real-time intrusion detection. Malformed data packets can be used to exploit parsers.
Semantic (Meaning)	Lack of a common data model. One vendor's "Zone Temperature" (tagged zone-temp) is another "RoomTemp" (tagged rm_t).	Prevents unified data analytics and control logic. Hinders the development of system-wide security rules based on data context.
Organizational (Vendor)	Proprietary "walled gardens" and vendor lock-in. APIs may be non-existent, poorly documented, or expensive.	Security patches from one vendor may break integrations with another. Creates a dependency on vendors for security, limiting autonomous defense.

The lack of semantic interoperability is particularly problematic. It prevents the creation of a unified single pane of glass for security monitoring. To illustrate, consider a plausible attack scenario: an attacker spoofs sensor data to an integrated system. The HVAC subsystem, communicating via BACnet, reports a data point tagged as Room Temp with a value of 40°C. Simultaneously, the fire alarm subsystem, using a proprietary protocol, reports its status as Normal. A unified, semantically aware security system would immediately flag this as a critical contradiction, a potential sensor spoofing attack or an incipient fire. However, in a non-interoperable system, these data points exist in separate, meaningless silos. The BMS sees only a high temperature and commands more cooling. The fire system sees nothing amiss. An attacker can exploit this semantic seam to physically damage equipment or create hazardous conditions, confident that the siloed systems are incapable of correlating the data.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

Organizational friction in smart buildings isn't just a technical inconvenience; it's a structural and economic reality. Many vendors have a clear business incentive to build proprietary ecosystems that make it difficult for customers to switch providers or integrate third-party tools. While this strategy may support brand loyalty, it often comes at the expense of security. When building operators are locked into closed systems, they're frequently unable to deploy independent, best-in-class cybersecurity tools. Instead, they're left relying on whatever limited protections each vendor offers, protections that may not be sufficient in today's threat landscape.

The 2023 report from the Association for Smarter Homes & Buildings (ASHB) underscores this issue [32]. It points out that vendor lock-in can severely restrict visibility across systems, delay the rollout of critical security patches, and make it harder to detect threats that span multiple platforms. In effect, the lack of interoperability doesn't just slow innovation; it actively weakens a building's ability to defend itself against cyber threats.

V. SECURITY AND INTEROPERABILITY SOLUTIONS

The body of research offers no shortage of proposed solutions for securing smart buildings, ranging from low-level cryptographic fixes to sweeping architectural frameworks. But not all solutions are created equally, and their effectiveness often depends on context. Table 3 lays out a comparative analysis of these approaches, weighing each against its intended purpose and, just as importantly, its limitations.

As Aliero and colleagues point out in their systematic review [33], cryptographic protocols and secure communication layers form a solid foundation, but they tend to fall short when deployed across diverse, real-world building systems. They're often difficult to scale and adapt in environments where devices vary widely in capability and design. On the other hand, high-level strategies like fog computing and digital twins offer a more holistic defense, helping to coordinate security across systems. Yet these approaches come with their own hurdles; interoperability issues, high implementation costs, and latency concerns that can undermine their responsiveness in critical situations.

Table 3: Comparative Analysis of Solution Modalities

Solution Modality	Primary Goal	Examples	Key Limitation
Technical (Security)	Secure data and devices	Lightweight Encryption (e.g.,PRESENT), Device Authentication (e.g., PUFs)	Often protocol-specific; does not address interoperability. May be too complex for legacy devices.
Technical (Data Integrity)	Establish trust and auditability	Blockchain for Access Control / Data Logs	Scalability concerns; high computational overhead. Best for specific use cases, not blanket logging.
Intelligent (Threat Detection)	Detect anomalous activity	AI/ML-based Intrusion Detection (IDS)	Requires large, high-quality, and semantically labeled datasets for training; high false-positive rates.
Architectural (Integration)	Normalize data and protocols	Middleware, IoT Platforms (e.g., FIWARE)	Can become a centralized bottleneck and a high-value attack target; may not solve the semantic problem.
Architectural (Semantics)	Provide common meaning	Ontologies (e.g., SAREF, Brick, Haystack)	Adoption is not universal; it requires significant upfront engineering effort to map existing, non-compliant systems.
Holistic (Convergence)	Unify security and interoperability	Digital Twins	High complexity and cost to develop and maintain an accurate, real-time model. Requires skills that are not common in facility management.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

A. Technical and Intelligent Solutions

At the device and network level, many of the security conversation centers on strengthening communication channels. This typically involves deploying lightweight cryptographic protocols that are optimized for resource-constrained IoT devices. For instance, recent studies have explored how post-quantum cryptographic frameworks can secure real-time communications in edge networks without overwhelming device capabilities [34].

Another promising approach is the use of Physical Unclonable Functions (PUFs), hardware-based identifiers that leverage microscopic variations in manufacturing to create unique, tamper-resistant device fingerprints. These have shown strong potential for lightweight, anonymous authentication in smart infrastructure contexts [35].

Blockchain technology is also frequently proposed, largely due to its immutable ledger and decentralized trust model. While it holds promise, especially for applications like secure identity management and audit trails, experts caution against treating it as a universal fix. As Shojaei and Naderi argue, blockchain is best suited for specific, high-value scenarios where traceability and stakeholder trust are paramount, rather than as a blanket solution for all smart building security needs [36].

Artificial intelligence is increasingly being used to build smarter, more adaptive Intrusion Detection Systems (IDS) for smart buildings. One of the most promising developments in this space is the use of federated learning, which allows multiple devices to collaboratively train models without sharing raw data. This approach is particularly appealing for environments where privacy and bandwidth are limited. Recent work by Garroppo et al. (2025) shows how federated learning can support trustworthy, lightweight IDS frameworks in 6G-connected smart buildings [9], balancing detection accuracy with privacy preservation.

But there's a catch. These AI-driven systems rely heavily on access to consistent, semantically rich data to learn and improve. Ironically, the same interoperability issues that make advanced analytics necessary, such as fragmented data formats and inconsistent device semantics, also limit the quality of data available to train these models. As Al-Rakhami and Al-Masri point out, without unified data models and integration standards, AI and machine learning systems struggle to deliver meaningful insights, creating a feedback loop that undermines their effectiveness [37].

B. Architectural Frameworks

Zero Trust Architecture (ZTA) is widely recognized as the future of cybersecurity, especially in complex environments like smart buildings. Its core principles, such as continuous verification and strict access controls, are well-suited for modern IT systems. But applying these same principles to legacy operational technology (OT) is far from straightforward. Many OT devices were never designed with security in mind; they run on outdated protocols, have limited processing power, and often require persistent connections to function properly. As highlighted by Veridify Security [38], integrating ZTA into these environments demands creative workarounds like security overlays or software-defined networking, which can be effective but are rarely seamless.

On the other end of the spectrum, Digital Twin (DT) technology offers a more holistic path forward. By creating virtual replicas of physical systems, DTs allow operators to simulate attacks, test defenses, and optimize responses, all without touching the live infrastructure. This sandbox approach is especially valuable for critical systems where downtime isn't an option. The BIM-SEC framework, introduced by Abdullahi and Lazarova-Molnar [39], demonstrates how DTs can be used to model cyber threats and evaluate countermeasures in smart building environments. However, the promise of DTs comes with a steep price: building and maintaining high-fidelity twins requires significant investment in data integration, modeling expertise, and computational resources. As Wang et al. [40] note, the complexity of aligning real-time data with virtual models remains a major barrier to widespread adoption.

VI. STANDARDS, REGULATIONS, AND THE HUMAN FACTOR

The challenges of securing smart buildings and ensuring interoperability go far beyond technical specifications; they're deeply rooted in policy, regulation, and human factors. While frameworks like the NIST Cybersecurity Framework [41] and the IEC 62443 series [42] offer structured, risk-based guidance, their adoption in the building sector remains limited. Many facility managers and integrators view these standards as overly complex or misaligned with the operational realities of legacy systems and fragmented vendor ecosystems.

This implementation gap is becoming harder to ignore as regulatory pressure mounts [43]. The European Union's Cyber Resilience Act (CRA), adopted in 2024, marks a significant shift from voluntary compliance to mandatory secure-by-design requirements for all digital products, including IoT devices [44, 45, 46]. This regulation compels manufacturers to embed cybersecurity throughout the product lifecycle, from development to decommissioning, fundamentally changing how smart building technologies are designed and deployed.

At the same time, data privacy laws like the General Data Protection Regulation (GDPR) continue to impose strict controls on how occupancy and movement of data are collected and processed [47, 48]. In smart buildings, where sensors constantly monitor presence and behavior, ensuring compliance with GDPR is not just a legal obligation, it's a design imperative. As highlighted in recent research, even seemingly anonymous data, like foot traffic patterns, can raise privacy concerns if not handled with care.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

Perhaps the most significant non-technical barrier to securing smart buildings is the systemic skills gap. The complexity of modern solutions like Zero Trust Architecture, federated learning, and digital twins, demands a rare blend of expertise across cybersecurity, IT networking, data science, and operational technology. Yet, professionals with this kind of cross-disciplinary knowledge are in short supply. According to the 2024 ISC2 Cybersecurity Workforce Study, this shortage is especially acute in sectors integrating AI and IoT, where the demand for hybrid skills far outpaces availability [49]. Without a parallel investment in workforce development, even the most advanced technical frameworks and regulatory mandates will struggle to gain meaningful traction.

VII. DISCUSSION AND FUTURE RESEARCH DIRECTIONS

The preceding analysis confirms a central insight: cyber-physical security and interoperability are not separate challenges; they are deeply intertwined. Gaps in interoperability create exploitable seams in security, while fragmented security solutions are often too costly or impractical to implement across diverse systems. This synthesis brings several urgent issues into focus.

First, the sector must reconcile forward-looking regulations with backward-facing infrastructure. The EU's Cyber Resilience Act (CRA) mandates secure-by-design principles for new digital products, but most Building Management Systems (BMS) have lifecycles of 15-20 years [50]. This means that for the foreseeable future, smart buildings will operate as hybrids, mixing secure new devices with legacy systems that were never designed for modern threats. This temporal security seam poses a long-term risk. Research into non-intrusive security wrappers such as bump-in-the-wire defenses and protocol-compliant authentication layers is not just theoretical; it's a practical necessity for bridging this gap [51]

Second, there's a growing disconnect between the realities of device-level vulnerabilities and the ambitions of system-wide modeling. With some IoT devices exposing over 1,500 known CVEs (Common Vulnerabilities and Exposures), the bottom-up threat landscape is vast and granular [52]. Meanwhile, frameworks like high-fidelity Digital Twins promise holistic oversight but often demand resources and precision that are unrealistic for most deployments. As Yitmen et al. argue, the future lies in good enough modeling tools that balance fidelity with feasibility, offering actionable insights without overwhelming complexity [53].

To guide future work, Table 4 consolidates these insights into a strategic research agenda, highlighting the key gaps and proposing actionable directions for the field.

Table 4: A Strategic Research Roadmap for Secure and Interoperable Smart Buildings

Identified Systemic Gap	Proposed Research Thrust	Key Research Questions
The Legacy Burden: A massive installed base of insecure OT systems with long lifecycles cannot be replaced overnight.	Scalable Legacy System Retrofitting: Develop non-intrusive security "wrappers" and intelligent gateways to protect vulnerable assets.	-How can modern cryptographic and authentication policies be applied to legacy protocols like BACnet/IP without requiring device replacement? - Can AI-powered gateways be developed to learn and enforce baselines for the legacy devices they protect, detect and block anomalous commands in real-time?
The Semantic-Security Chasm: The lack of common data models prevents context-aware security monitoring and holistic threat detection.	Context-Aware Cyber-Physical IDS: Create trivially aware Intrusion Detection Systems that fuse network, physical, and semantic data streams.	- What data fusion models can effectively correlate low-level network anomalies with high-level semantic context (e.g., from a Brick schema) to reduce false positives? - How can an IDS be designed to distinguish between a malicious command and an unusual but legitimate operational command?
The Architectural Dilemma: Holistic solutions (e.g., full-fidelity Digital Twins) are too complex and costly for widespread adoption.	"Good Enough" Modeling ("DT-Lite"): Develop lightweight, security-focused digital models tailored for threat simulation and response planning.	- What is the minimum viable data set required to accurately model a building *only* for the purpose of cyber-physical attack simulation? - Can these DT-Lite models be automatically generated from network traffic and configuration files to drastically reduce manual engineering costs?

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

The IT/OT Paradigm Clash: IT-centric security models (e.g., ZTA) are not directly applicable to the real-time, resource-constrained nature of OT.	Cyber-Physical Zero Trust Architecture (CP-ZTA): Adapt and re-engineer ZTA principles for the unique constraints of building automation.	- How can lightweight, continuous authentication and micro-segmentation be designed for low-power IoT/OT devices? - What are the most viable policy enforcement points in a hybrid network of modern and legacy components?
The Systemic Skills Gap: The required convergent skill set (firmware security, networking, AI/ML, OT) is largely absent in the current workforce.	AI for Autonomous Operations: Leverage AI and Machine Learning for autonomous security management, semantic discovery, and decision support.	- Can ML models be trained to autonomously discover legacy devices and map their proprietary data points to a standard ontology (e.g., Brick), automating interoperability? - Can explainable AI (XAI) be developed to provide autonomous remediation suggestions in clear language that a facilities manager can trust and act upon?

VIII. CONCLUSION

This paper offers a narrative-critical review of the intertwined challenges of cyber-physical security and interoperability in modern IoT-based smart buildings. Rather than treating these as separate issues, the analysis shows they are deeply connected, each one shaping and complicating the other. The review identifies three major systemic failures that continue to hold the field back: the fragmented nature of research, the tension between idealized architectural models and the messy reality of vulnerable devices, and the growing skills gap that limits the workforce's ability to implement and manage advanced solutions.

Looking at current approaches, the field is clearly shifting away from isolated technical fixes and moving toward more intelligent, integrated frameworks. Yet, this transition is far from smooth. The complexity of these solutions, combined with the widespread presence of outdated systems, makes practical adoption difficult. New regulations are pushing for stronger security, but they are colliding with legacy infrastructure that was never built to meet these standards. This creates what the paper refers to as a temporal security seam, a long-term vulnerability that demands immediate attention.

To help guide future progress, the paper presents a strategic research roadmap. This roadmap lays out a clear agenda focused on developing retrofittable security tools, context-aware artificial intelligence, and autonomous systems that can adapt to real-world constraints. By taking a holistic view, the paper argues that the next generation of smart buildings can achieve both efficiency and resilience, protecting not just digital assets, but the people and environments they serve.

REFERENCES

[1]. Grand View Research. (2024). Smart building market size & share Industry report, 2030. https://www.grandviewresearch.com/industry-analysis/global-smart-buildings-market
[2]. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), 164-173. http://dx.doi.org/10.4236/jcc.2015.35021
[3]. Forescout. (2024). Rising threats to industrial and building automation systems: A 2024 cybersecurity report. UNDERCODE News. https://undercodenews.com/rising-threats-to-industrial-and-building-automation-systems-a-2024-cybersecurity-report/
[4]. Siemens. (2024, February 20). Cybersecurity in building automation: The time to act is now! https://blog.siemens.com/2024/02/cybersecurity-in-building-automation-the-time-to-act-is-now/
[5]. Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candanf, K. S., & O'Neill, Z. (2023). A critical review of cyber-physical security for building automation systems. ArXiv. https://arxiv.org/abs/2210.11726
[6]. Runge, I. M., Akinci, B., & Bergés, M. (2023). Challenges in cyber-physical attack detection for building automation systems. In BuildSys '23: Proceedings of the 10th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation. https://doi.org/10.1145/3600100.3623738
[7]. Affonso, E. O. T., Branco, R. R., Menezes, O. V. C., Guedes, A. L. A., Chinelli, C. K., Haddad, A. N., & Soares, C. A. P. (2024). The main barriers limiting the development of smart buildings. Buildings, 14(6), 1726. https://doi.org/10.3390/buildings14061726
[8]. ESI Technologies. (2025, September 10). Smart building security: Key interoperability trends 2025. https://esicorp.com/smart-building-security-key-interoperability-trends-2025/

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

[9]. Garroppo, R. G., Giardina, P. G., Landi, G., & Ruta, M. (2025). Trustworthy AI and federated learning for intrusion detection in 6G-connected smart buildings. Future Internet, 17(5), 191. https://doi.org/10.3390/fi17050191
[10]. ACCORD Consortium. (2023). Existing ontologies, standards, and data models in the building data domain relevant to compliance checking (Technical Report D2.1). European Union Horizon Europe Programme. https://accordproject.eu/wp-content/uploads/2023/09/ACCORD_D2.1_Technical_Report_Existing_Models.pdf
[11]. Chamari, L., Pauwels, P., Petrova, E., Dubbeldam, J. W., de Jong, N., & Gunderi, K. M. (2023). Reference architecture for smart buildings. Brains4Buildings Project. https://pure.tue.nl/ws/portalfiles/portal/306532899/B4B-WP4-D4.06_Reference_Architecture-FINAL.pdf
[12]. Apanavičienė, R., & Shahrabani, M. M. N. (2023). Key factors affecting smart building integration into smart city: Technological aspects. Smart Cities, 6(4), 1832-1857. https://doi.org/10.3390/smartcities6040085
[13]. Simeoni, E., Gaeta, E., García-Betances, R. I., Raggett, D., Medrano-Gil, A. M., Carvajal-Flores, D. F., Fico, G., Cabrera-Umpiérrez, M. F., & Arredondo Waldmeyer, M. T. (2021). A secure and scalable smart home gateway to bridge technology fragmentation. Sensors, 21(11), 3587. https://doi.org/10.3390/s21113587
[14]. IEEE IGSC. (2022). 2022 IEEE 13th International Green and Sustainable Computing Conference (IGSC). IEEE. https://doi.ieeecomputersociety.org/10.1109/IGSC55832.2022.9969359
[15]. Neuron Team. (2023). EMQ Neuron framework documentation. EMQ Documentation. Retrieved from https://docs.emqx.com/en/neuron/latest/
[16]. Balduzzi, M., Lin, P., Perine, C., Flores, R., Vosseler, R., & Bongiorni, L. (2020). Industrial Protocol Gateways Under Analysis. Black Hat USA Briefings. Trend Micro Research. Retrieved from https://i.blackhat.com/USA-20/Wednesday/us-20-Balduzzi-Industrial-Protocol-Gateways-Under-Analysis.pdf
[17]. Titterington, J. (2024). 2024 Ransomware Radar Report. Rapid7 Labs. Retrieved from https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf
[18]. Veridify Security. (2024, March 13). BACnet security issues and how to mitigate cyber risks. Retrieved from https://www.veridify.com/bacnet-security-issues-and-how-to-mitigate-cyber-risks/
[19]. KNX Association. (2025). KNX Secure - Security for smart buildings. Retrieved from https://www.knx.org/knx-en/for-professionals/index.php
[20]. Ghobakhlou, A., Al-Hamid, D. Z., Zandi, S., & Cato, J. (2025). A comprehensive analysis of security challenges in ZigBee 3.0 networks. Sensors, 25(15), 4606. https://doi.org/10.3390/s25154606
[21]. OASIS. (n.d.). MQTT Version 5.0. Retrieved from https://mqtt.org/
[22]. Shelby, Z., Hartke, K., & Bormann, C. (2014). The Constrained Application Protocol (CoAP) (RFC 7252). Internet Engineering Task Force. Retrieved from https://datatracker.ietf.org/doc/html/rfc7252
[23]. Trout Software. (2025). How to design VLANs for ICS security. Retrieved from https://www.trout.software/resources/tech-blog/how-to-design-vlans-for-ics-security
[24]. Martín Toral, I., Calvo, I., Villar, E., & Gil-García, J. M. (2024). Introducing security mechanisms in OpenFog-compliant smart buildings. Electronics, 13(15), 2900. https://doi.org/10.3390/electronics13152900
[25]. EMBA Project. (2023). EMBA - The firmware security analyzer [Software]. GitHub. Retrieved from https://github.com/e-m-b-a/emba
[26]. Cisco Blogs. (2020, June 26). Ripple20: Critical vulnerabilities might be putting your IoT/OT devices at risk. Retrieved from https://blogs.cisco.com/security/ripple20-critical-vulnerabilities-might-be-putting-your-iot-ot-devices-at-risk
[27]. Armis. (2020). URGENT/11: 11 zero-day vulnerabilities impacting billions of mission-critical devices. Retrieved from https://www.armis.com/research/urgent-11/
[28]. Rapid 7 Labs. (2024). 2024 Ransomware Radar Report. Retrieved from https://www.rapid7.com/globalassets/_pdfs/2024-rapid7-ransomware-radar-report-final.pdf
[29]. Abd El-Latif, A. A., Tawalbeh, L., Maleh, Y., & Gupta, B. B. (Eds.). (2024). Secure edge and fog computing enabled AI for IoT and smart cities. Springer. https://link.springer.com/book/10.1007/978-3-031-51097-7
[30]. Alnaser, A. A., Maxi, M., & Elmousalami, H. (2024). AI-powered digital twins and Internet of Things for smart cities and sustainable building environments. Applied Sciences, 14(24), 12056. https://doi.org/10.3390/app142412056
[31]. Froehlich, A. (2023, September 12). How building technology integration, interoperability, and security can align. Buildings. Retrieved from https://www.buildings.com/smart-buildings/iot/article/33018626/how-building-technology-integration-interoperability-and-security-can-align
[32]. ASHB. (2023). IoT Cybersecurity for Facilities Professionals in the Smart Built Environment (IS-2023-187). Association for Smarter Homes & Buildings. Retrieved from https://www.ashb.com/public_research/is-2023-187-iot-cybersecurity-for-facilities-professionals-in-the-smart-built-environment/
[33]. Aliero, M. S., Asif, M., Ghani, I., Pasha, M. F., & Jeong, S. R. (2022). Systematic review analysis on smart building: Challenges and opportunities. Sustainability, 14(5), 3009. https://doi.org/10.3390/su14053009

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25dec1366

[34]. Rahmati, M., & Rahmati, N. (2025). Lightweight post-quantum cryptographic frameworks for real-time secure communications in IoT edge networks. Telecommunication Systems, 88, Article 136. https://doi.org/10.1007/s11235-025-01372-1
[35]. Guo, Y., Li, L., Jin, X., An, C., Wang, C., & Huang, H. (2025). Physical-unclonable-function-based lightweight anonymous authentication protocol for smart grids. Electronics, 14(3), 623. https://doi.org/10.3390/electronics14030623
[36]. Shojaei, A., & Naderi, H. (2024). Blockchain technology for a circular built environment. In A Circular Built Environment in the Digital Age (pp. 213-228). Springer. https://doi.org/10.1007/978-3-031-39675-5_12
[37]. Al-Rakhami, M., & Al-Masri, E. (2023). Artificial intelligence and machine learning in smart building environments: Challenges and opportunities. Sensors, 23(4), 1987. https://doi.org/10.3390/s23041987
[38]. Veridify Security. (2025, May 9). Zero Trust security for legacy OT devices. https://www.veridify.com/zero-trust-security-for-legacy-ot-devices/
[39]. Abdullahi, S. M., & Lazarova-Molnar, S. (2024). Toward a unified security framework for digital twin architectures. 2024 IEEE International Conference on Cyber Security and Resilience (CSR). https://zenodo.org/records/14070853
[40]. Wang, Y., Alnaser, A. A., Maxi, M., & Elmousalami, H. (2024). AI-powered digital twins and Internet of Things for smart cities and sustainable building environments. Applied Sciences, 14(24), 12056. https://doi.org/10.3390/app142412056
[41]. NIST. (2023). Cybersecurity Framework 2.0. National Institute of Standards and Technology. https://www.nist.gov/cyberframework
[42]. Tremlet, C. (2023, October 22). Adopting IEC 62443 standards for infrastructure cybersecurity. Embedded. https://www.embedded.com/adopting-iec-62443-standards-for-infrastructure-cybersecurity/
[43]. Audit Peak. (2023). Benefits & Challenges in Implementing NIST CSF. https://www.auditpeak.com/challenges-in-implementing-nist-csf/
[44]. Kitchen, M. (2024, October 11). The Cyber Resilience Act Explained: A Roadmap for IoT Manufacturers. EPS Global. https://www.epsprogramming.com/blog/the-cyber-resilience-act-explained/
[45]. Domas, S. (2024, October 21). What the Cyber Resilience Act Means for IoT Manufacturers. Forbes Technology Council. https://www.forbes.com/sites/forbestechcouncil/2024/10/21/what-the-cyber-resilience-act-means-for-iot-manufacturers/
[46]. Stenberg, E. (2025, January 22). The Cyber Resilience Act: How Manufacturers Can Meet New EU Standards. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/the-cyber-resilience-act-how-manufacturers-can-meet-new-eu-standards-and-strengthen-product-security/
[47]. Harper, S., Mehrnezhad, M., & Mace, J. C. (2022). User privacy concerns and preferences in smart buildings. In Proceedings of the International Conference on Human-Computer Interaction. https://link.springer.com/content/pdf/10.1007/978-3-030-79318-0_5.pdf
[48]. Terabee. (2022). GDPR and People Counters: Smart and Safe Decisions. https://www.terabee.com/people-counters-powering-data-driven-decisions-in-gdpr-compliant-smart-buildings/
[49]. ISC2. (2024, October 31). 2024 ISC2 Cybersecurity Workforce Study. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
[50]. IFMA. (2024, January 22). Optimizing building management with a lifecycle approach. IFMA Knowledge Library. https://knowledgelibrary.ifma.org/optimizing-building-management-with-a-lifecycle-approach/
[51]. Aldar, A., Chan, C.-F., & Zhou, J. (2023). Non-intrusive protection for legacy SCADA systems. IEEE Communications Magazine. https://www.bohrium.com/paper-details/non-intrusive-protection-for-legacy-scada-systems/864974017780515085-2442
[52]. Lavrinovica, I., Judvaitis, J., Laksis, D., Skromule, M., & Ozols, K. (2024). A comprehensive review of sensor-based smart building monitoring and data gathering techniques. Applied Sciences, 14(21), 10057. https://doi.org/10.3390/app142110057
[53]. Yitmen, I., Almusaed, A., Hussein, M., & Almssad, A. (2025). AI-driven digital twins for enhancing indoor environmental quality and energy efficiency in smart building systems. Buildings, 15(7), 1030. https://doi.org/10.3390/buildings15071030