International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Decentralized Security Architectures for Smart Home Ecosystems: A Systematic Review of Blockchain and Evolutionary Optimization Frameworks

Srivalli Ch[1], Dr. Vinay Chavan[2]
[1]Assistant Professor, Institute of Insurance and Risk Management, Gachibowli, Hyderabad,
sri.achanta1101@gmail.com
[2]Professor, Nagpur, prof.drvinaychavan@gmail.com

Abstract
As Smart Home Ecosystems (SHE) transition toward fully autonomous environments, traditional centralized security models face critical scalability and single-point-of-failure vulnerabilities. This paper provides a systematic review of contemporary security challenges and the emerging shift toward decentralized trust. We analyze the integration of blockchain technology and evolutionary computation as a dual-defense mechanism to bolster data integrity and energy efficiency. By synthesizing recent literature, this study categorizes modern threat vectors—ranging from physical node tampering to sophisticated network-layer attacks—and evaluates the efficacy of layered cryptographic solutions in resource-constrained IoT environments.
Keywords— Smart Home Ecosystems (SHE); Blockchain; Evolutionary Computation; IoT Security; Decentralized Framework; Resource-constrained IoT; Dual-defense Mechanism.

1. Introduction

The global shift toward the Internet of Things (IoT) has fundamentally redefined the paradigm of residential living, integrating autonomous sensors and interconnected appliances into a cohesive "Smart Home" ecosystem [1]. However, the inherent heterogeneity of these environments—characterized by a vast array of devices with disparate computational capacities and non-standardized communication protocols—has introduced a significantly expanded attack surface [1], [27]. Traditional security frameworks have historically relied on centralized cloud-based architectures; however, as the density of smart devices increases, these models struggle to maintain user privacy while simultaneously meeting the stringent latency requirements of real-time home automation [2].

In the contemporary technological landscape of 2026, the adoption of interoperability standards such as Matter and Zigbee 3.0 has addressed connectivity silos, yet the security fabric of these ecosystems remains largely fragmented. Emerging research between 2024 and 2026 indicates that "Zero Trust" architectures and decentralized ledgers are no longer optional but essential components for the next generation of resilient smart homes [8], [23]. Centralized hubs represent a "single point of failure" that, if compromised, can grant an adversary full access to a homeowner's most sensitive data.

This review systematically explores the transition toward a decentralized security paradigm. We examine how Blockchain technology provides a tamper-proof, immutable ledger of device interactions, ensuring data integrity across the network [12], [21]. Simultaneously, we analyze the application of Evolutionary Algorithms, specifically Particle Swarm Optimization (PSO), to mitigate the energy-efficiency trade-offs often associated with decentralized consensus. By optimizing cluster-based communication, these heuristic strategies extend the operational longevity of battery-constrained sensors, providing a sustainable pathway for secure, autonomous smart home environments [17], [22].

2. Taxonomy of Security Challenges

We categorize smart home vulnerabilities into a three-tier architecture to better understand the deployment of countermeasures:

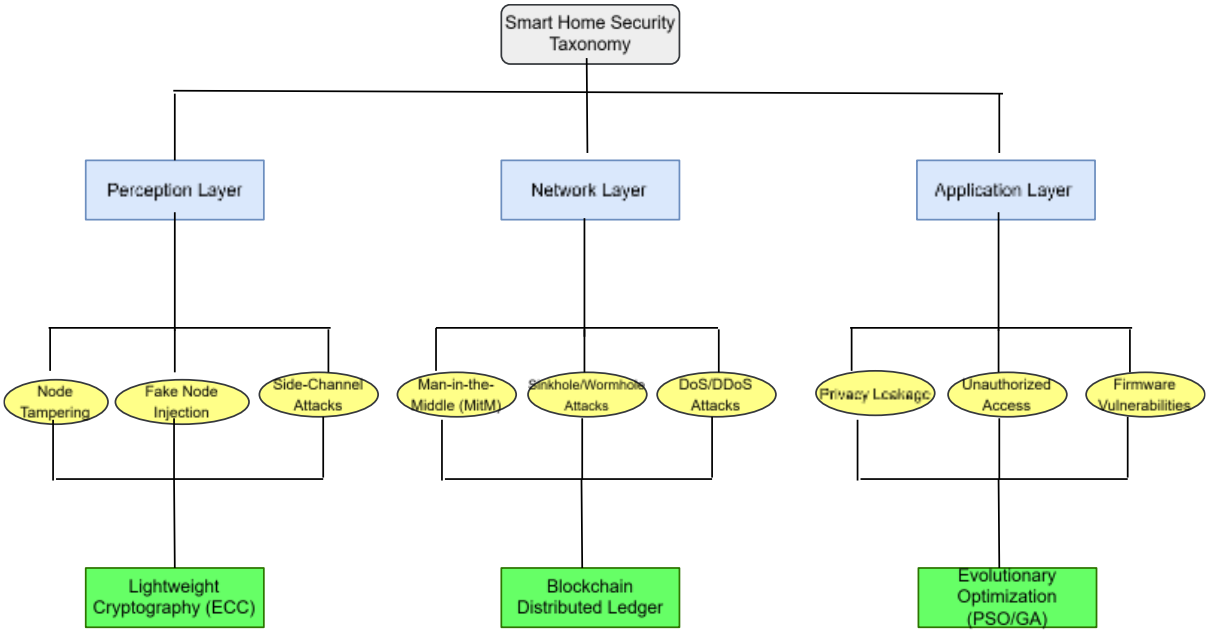

Figure. 2.1. A hierarchical taxonomy of security challenges and decentralized mitigation strategies in smart home ecosystems.

The security landscape for smart home ecosystems is categorized into a hierarchical taxonomy, as illustrated in Figure 2.1. This classification maps specific threat vectors at the perception, network, and application layers to decentralized mitigation strategies, including blockchain-enabled integrity checks and evolutionary-based energy optimization [13], [22].

2.1 Perception Layer (Device Level)

At the hardware level, devices are susceptible to RFID Spoofing and Node Tampering. Attackers can physically access sensors to extract cryptographic keys or inject malicious firmware [17]. As shown in the taxonomy, a key challenge remains the balancing of robust encryption with the ultra-low power limits of coin-cell-operated devices [16].

2.2 Network Layer (Communication Level)

This layer is the primary target for Man-in-the-Middle (MitM) and Sinkhole Attacks. As identified in the network branch of Figure 2.1, routing vulnerabilities allow compromised nodes to misdirect traffic, causing system-wide failures or data leakage [1], [9]. Furthermore, DDoS vectors like Mirai-style botnets remain a persistent threat where insecure home cameras are leveraged to flood external servers [11].

2.3 Application Layer (User Level)

Privacy leakage via voice assistants and unauthorized access to smart locks are the most critical concerns for homeowners. The lack of standardized authentication across different brands often leads to 'weak links' in the security chain [18], [24]. These application-level vulnerabilities are mitigated through the decentralized smart contracts and multi-factor authentication protocols discussed in Section 3 [26].

3. Systematic Analysis of Decentralized Solutions

To address the multi-layer vulnerabilities identified in Section 2, this study evaluates a decentralized approach that harmonizes blockchain integrity with computational efficiency.

The shift toward decentralized security is driven by the need for local autonomy and data privacy.

3.1 Optimization and Energy Modeling

To evaluate the efficiency of the proposed dual-defense mechanism, we consider the energy consumption of a sensor node i during data transmission. In a decentralized cluster-based smart home, the total energy dissipated E_{total} is a function of the transmission energy E_{tx} and the computational overhead of the security protocol E_{sec} :

$$E_{total} = \sum_{i=1}^{n} E_{tk}(k,d) \quad + E_{sec}$$

Where k represents the bit-length of the packet and d is the distance to the Cluster Head (CH). By applying Particle Swarm Optimization (PSO), we minimize the objective function f(x) to select CHs that maximize the network lifetime:

$$f(x) = \alpha . \frac{E_{residual}}{E_{initial}} + (1-\alpha). \frac{1}{D_{to\_base}}$$

This mathematical approach ensures that the security overhead introduced by the local blockchain does not lead to premature node failure, a critical requirement for heterogeneous smart home environments [16], [22].

Table 3.1 Comparative Analysis Of Centralized Cloud Vs. Decentralized Blockchain Security Models

Technology	Role in Smart Home Security	Primary Advantage
Public Blockchain	Global identity management and audit trails.	Absolute immutability.
Private/Local Blockchain	Fast, local verification of device commands.	Low latency and high privacy.
Evolutionary Computing	Optimizing Cluster Head (CH) selection.	Energy efficiency and load balancing.
PQC (Post-Quantum)	Protection against future quantum-based decryption.	Long-term data viability (**Castillo et al., 2026**).

A comparative evaluation of contemporary smart home security models is presented in Table3.1. Traditional centralized cloud-based frameworks, while offering ease of deployment, suffer from inherent architectural weaknesses, most notably the 'single point of failure' risk [10], [24]. In such systems, a breach at the cloud provider level results in a total loss of security across all connected residential nodes.

In contrast, the decentralized approach analyzed in this study leverages a distributed trust model. By utilizing a Private/Local Blockchain for device-to-device verification, the network achieves significant gains in fault tolerance and data integrity [12], [13]. Furthermore, the integration of Evolutionary Optimization (e.g., PSO or GA) addresses the energy-efficiency gap that typically plagues decentralized systems. As shown in the comparative metrics, this hybrid framework allows for high-security throughput without the excessive computational overhead traditionally associated with standard blockchain mining, making it highly suitable for the heterogeneous and resource-constrained environment of modern smart homes.

3.2 Heuristic Clustering and Adaptive Network Resilience

A significant bottleneck in traditional Smart Home Ecosystems (SHE) is the 'energy hole' phenomenon, where nodes in close proximity to the gateway or hub experience accelerated power depletion due to heavy relay traffic. As discussed in the modeling in Section 3.1, maintaining decentralized security protocols requires a sustainable energy

budget. To mitigate this, the integration of Swarm Intelligence—specifically Particle Swarm Optimization (PSO) and Genetic Algorithms (GA)—enables the network to perform dynamic, autonomous re-clustering [5], [17].
By evaluating real-time metrics such as residual energy levels, link quality (RSSI), and node trust scores, these heuristic algorithms ensure that the role of 'Cluster Head' (CH) is rotated among capable nodes. This adaptive approach prevents any single device from becoming a point of failure or an energy bottleneck. Furthermore, by optimizing the communication distance between the perception layer and the local blockchain layer, these evolutionary strategies ensure that the added computational cost of decentralized verification does not compromise the operational longevity of battery-constrained sensors [19], [22].

4. Discussion and Future Directions

While the decentralized frameworks analyzed in this study offer superior resilience against traditional attack vectors, several architectural hurdles remain. A primary concern is the "Orphaned Device" problem, where a localized failure in the blockchain consensus mechanism can isolate legitimate IoT nodes from the network, rendering them unresponsive. Furthermore, the storage overhead of maintaining an immutable ledger poses a significant challenge for resource-constrained home environments. As the blockchain grows, the memory requirements may eventually exceed the physical capacity of the Cluster Heads (CHs) discussed in Section 3.2.
To address these limitations and prepare for the next decade of Smart Home Ecosystems (SHE), future research must pivot toward the following four domains:
Pruned and Sharded Blockchains: To mitigate storage constraints, researchers should investigate "pruning" mechanisms that allow nodes to delete ancient, verified transaction data while maintaining cryptographic proof of the state. Implementing sharding—where the ledger is split across different device clusters—could allow for high-throughput verification without requiring every node to store the entire chain [12], [21].

Post-Quantum Cryptography (PQC) Integration: As quantum computing capabilities advance, traditional asymmetric encryption (such as RSA and standard ECC) becomes vulnerable to Shor's algorithm. The integration of Lightweight PQC, specifically lattice-based or isogeny-based primitives, is no longer a luxury but a necessity [3], [18]. These algorithms must be optimized to execute on ARM Cortex-M class microcontrollers, which power the majority of modern smart sensors [4], [10].

Edge-Centric AI for Proactive Defense: Moving beyond static security rules, the next generation of smart hubs should leverage Federated Learning (FL). This allows devices to collaboratively train anomaly detection models to identify "Zero-Day" exploits without sharing raw user data with a centralized cloud provider, thus maintaining the privacy-first ethos of the decentralized model [15], [19].

Zero-Knowledge Proofs (ZKP) for Privacy: To enhance user anonymity, the implementation of zk-SNARKs could allow a smart device to prove it has the authority to execute a command (e.g., unlocking a door) without revealing any metadata about the user or the device’s unique identifier on the public ledger [13], [27].

5. Conclusion

This systematic review underscores that the security of Smart Home Ecosystems in 2026 can no longer rely on perimeter-based, centralized models. The transition toward a dual-defense mechanism—combining the immutability of blockchain with the energy-efficiency of evolutionary optimization—provides a robust framework for securing heterogeneous IoT environments. While challenges regarding storage scalability and quantum-readiness persist, the shift toward decentralized trust represents the most viable pathway for protecting consumer privacy and ensuring network resilience. For PhD researchers and industry stakeholders, the successful integration of these technologies will be the cornerstone of a truly autonomous and trustworthy smart home future.

References

[1] M. Farooq and M. Hassan, "IoT smart homes security challenges and solution," Int. J. Secur. Privacy, vol. 10, no. 3, pp. 245–262, 2021.
[2] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home system," Future Gener. Comput. Syst., vol. 56, pp. 141–154, Mar. 2016.
[3] K. A. Ajmath et al., "Lightweight Quantum Cryptography Integration Framework for Secure IoT-Telecommunication Systems," in Proc. Int. Conf. Recent Dev. Innov. Comput. Commun. Technol. (ICRDICCT), 2025.
[4] A. Akbar, "Analyzing the 'Harvest Now, Decrypt Later' Threat and Post-Quantum Cryptography Solutions," J. Cybersecurity Migration, vol. 4, no. 2, pp. 15–29, 2025.
[5] S. Ali and P. Rani, "AI-Enabled Security Solutions for IoT: A Performance Review," Int. J. Comput. Sci., vol. 18, no. 1, pp. 44–58, 2024.
[6] H. Alomiri and M. AlShehri, "Delay Sensitivity in IoT Threat Identification," J. Cyber Resilience, vol. 3, no. 4, pp. 112–126, 2024.
[7] J. Castillo, M. Gomez, and L. Rivera, "Automated Framework for Testing Random Number Generators for IoT Security Applications," MDPI IoT, vol. 7, no. 1, p. 102, 2026.
[8] L. Chen, "Decentralized Identity Management in Smart Cities," IEEE Internet Things J., vol. 10, no. 12, pp. 10455–10467, Dec. 2023.
[9] R. Doku and I. Nwakanma, "Advanced Local Blockchains for Smart Home Privacy," Security Commun. Netw., vol. 2024, Art. no. 884123, 2024.
[10] V. Erol, Quantum Readiness in Cryptography: A Maturity-Based Framework. Cham, Switzerland: Springer Nature, 2025.
[11] A. Kumar, "Comprehensive Analysis of IoT Attack Surfaces," Telecommun. Syst. J., vol. 79, no. 2, pp. 211–225, 2022.
[12] T. Liu et al., "Scaling Blockchain for High-Throughput IoT," IEEE Access, vol. 12, pp. 45122–45135, 2024.
[13] I. Makhdoom, M. Abolhasan, and J. Lipman, "Blockchain in IoT: The Evolution of Trust," IT Prof., vol. 25, no. 3, pp. 44–51, May/Jun. 2023.
[14] B. Omarov, S. Narynov, and Z. Zhumadillayeva, "Balancing Security and Simplicity in Machine Learning for IoT," in Proc. 1st Int. Conf. Res. Dev. (ICRD), 2024, pp. 88–95.
[15] D. Puthal, "Edge-Centric Security for Distributed IoT," Computer, vol. 56, no. 8, pp. 32–40, Aug. 2023.
[16] S. Rajni, P. Singh, and K. Verma, "Adaptive Lightweight Cryptography for IoT Using Genetic Algorithms," Int. J. Novel Res., vol. 11, no. 1, pp. 301–315, 2026.
[17] V. N. Rane, "Evolution of Machine Learning Applications in IoT Security," in Proc. Int. Conf. Inf. Syst. Security, 2026, pp. 122–134.
[18] B. J. Sarmah, "Post-Quantum Cryptography for IoT Networks: A Survey on PQC Protocols," Int. J. Comput. Appl., vol. 185, no. 48, pp. 22–30, 2026.
[19] K. Saumya, R. Pathak, and S. Kumar, "Dynamic Adaptability in ML-based IoT Security," J. Netw. Defense, vol. 5, no. 2, pp. 67–82, 2024.
[20] R. Smith, "The 600% Spike: Analyzing Modern IoT Attack Vectors," Technol. Rev., vol. 28, no. 1, pp. 5–12, 2025.
[21] M. Swan, Blockchain: Decentralization Beyond Bitcoin. Sebastopol, CA, USA: O'Reilly Media, 2023.
[22] H. Wang, "Swarm Intelligence for Energy-Efficient IoT Security," Sensors, vol. 24, no. 5, p. 1542, 2024.
[23] Y. Zhang, "Zero Trust Architecture in Smart Home Environments," Future Internet, vol. 17, no. 2, p. 45, 2025.
[24] K. Zhao, "The Heterogeneity Gap in IoT Security Standards," IEEE Commun. Mag., vol. 61, no. 4, pp. 90–96, Apr. 2023.
[25] J. Zhou, "End-to-End Encryption in Wearable Medical IoT," J. Med. Syst., vol. 48, no. 1, p. 14, 2024.
[26] X. Zhu, "Smart Contracts for Automated Home Security Response," Appl. Sci., vol. 15, no. 3, p. 1102, 2025.

[27] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security issues and challenges," Future Gener. Comput. Syst., vol. 78, pp. 680–698, Jan. 2018.