Pegem Journal of Education and Instruction, Vol. 16, No. 1, 2026 (pp. 1860-1869)

RESEARCH ARTICLE WWW.PEGEGOG.NET

Towards an Autonomic Sentinel: A Systems Engineering Perspective on Residential Electronic Security in the IoT Era

Dahmane Mahdi Imad El dine
Faculty of Sciences and Technology, Ziane Achour University of Djelfa, Algeria
Email: mah7dah7@gmail.com

Received : 21/07/2025 ; Accepted : 21/12/2025 ; Published : 07/02/2026

Abstract

Residential security is transitioning from stand-alone burglar alarms to complex Cyber-Physical Systems (CPS) tightly coupled with the Internet of Things (IoT). This evolution enables context-aware sensing, edge intelligence, and remote management but simultaneously increases system complexity, widens the attack surface, and raises challenging questions about interoperability, latency, and privacy. Existing research on smart home security is often fragmented, focusing on isolated protocols or specific computer vision algorithms without an integrated systems engineering perspective. This paper bridges this gap by offering a system-level analysis and a conceptual framework for residential electronic security. First, we develop a functional taxonomy of intrusion detection and analyze key sensing modalities (volumetric, perimetric, and video-based) based on signal processing physics and performance metrics. Second, we critically evaluate communication architectures (Zigbee, Z-Wave, Thread/Matter), highlighting trade-offs in latency and resilience. Third, we examine the role of Edge Computing and Deep Learning in video analytics, presenting a latency model that contrasts cloud-centric and edge-centric processing. Finally, we propose an Autonomic Residential Security Architecture (ARSA) that integrates heterogeneous sensing, edge AI, and Federated Learning into a continuous "sense–analyze–plan–act–learn" loop. This architecture serves as a reference for designing resilient, privacy-aware, and self-managing security systems.

Keywords: Cyber-Physical Systems (CPS), Smart Home Security, Internet of Things (IoT), Intrusion Detection, Edge Computing, Matter Protocol, Federated Learning, Cybersecurity.

1. Introduction

The protection of residential spaces has traditionally relied on mechanical barriers and simple electromechanical circuits. The emergence of the Internet of Things (IoT) [1]–[3] has fundamentally reshaped this landscape, transforming the modern home into a distributed Cyber-Physical System (CPS). Contemporary security systems now integrate volumetric motion detection, intelligent video surveillance, and automated actuators, all interconnected via diverse wireless protocols [4].

While these advancements offer improved situational awareness, they introduce significant engineering challenges. The reliance on cloud computing for critical tasks introduces latency and privacy risks, while the proliferation of wireless sensors expands the attack surface [5]. Furthermore, the market suffers from fragmentation, where proprietary ecosystems hinder the development of coherent, interoperable security solutions.

This paper addresses these challenges by providing a comprehensive systems engineering analysis. Unlike traditional surveys that list consumer devices, this study dissects the architectural integration of sensing physics, communication topology, and algorithmic decision-making. The primary contribution is the proposal of an Autonomic Residential Security Architecture (ARSA), which leverages Edge AI and Federated Learning to create a self-managing and privacy-preserving security shield.

2. Related Work

The literature on IoT security is extensive but often segmented. Foundational surveys by Atzori et al. [1] and Al-Fuqaha et al. [6] established the architectural layers of IoT but did not focus specifically on residential security constraints.

2.1. Smart Home Security Protocols

Security analysis of home automation protocols has been a major research focus. Geneiatakis et al. [7] and Knight et al. [8] analyzed vulnerabilities in Zigbee and Wi-Fi, highlighting susceptibility to jamming and replay attacks. More recently, the release of the Matter standard [9] has prompted new studies on interoperability and IP-based security in smart homes [10], [11].

2.2. Edge Intelligence in Surveillance

The shift from cloud to edge computing is well-documented. Shi et al. [12] articulated the vision of edge computing for latency-sensitive applications. In the context of security, Zhang and Wang [13] compared edge vs. cloud architectures, demonstrating the efficiency of local processing for anomaly detection. Recent advances in lightweight Convolutional Neural Networks (CNNs), such as YOLO Nano and MobileNet, have enabled real-time object detection on resource-constrained devices [14], [15].

2.3. Federated Learning for Privacy

Federated Learning (FL), introduced by McMahan et al. [16], allows model training on decentralized data. Its application to Intrusion Detection Systems (IDS) in IoT has been explored by varying authors [17]–[19], focusing mostly on network traffic anomalies. However, the application of FL specifically for collaborative residential physical security remains an under-explored area which this paper aims to address.

3. The Physics of Sensing and Detection Logic

To engineer a robust system, one must understand the underlying physics of sensing modalities. We classify detection functions into Volumetric, Perimetric, and Visual categories.

[Figure 1 Placeholder]

(Instructions for drawing Figure 1: Draw a hierarchical tree diagram. Title: "Taxonomy of Residential Intrusion Detection". Root node branches into: 1. Volumetric (PIR, Microwave, Ultrasonic), 2. Perimetric (Magnetic Contacts, Glass Break, Vibration/Shock), 3. Visual (IP Cameras, Thermal Imaging), 4. Environmental (Contextual sensing).

Table 1. Taxonomy of Residential Intrusion Detection Technologies

Level	Parent Node	Node / Technique	Brief Description
0	—	Residential Intrusion Detection	Root category covering intrusion detection in residential environments.
1	Residential Intrusion Detection	Volumetric Sensing	Volumetric sensing of object motion within indoor spaces.
1	Residential Intrusion Detection	Perimetric Sensing	Sensing along protected perimeters such as doors and windows.
1	Residential Intrusion Detection	Visual Sensing	Visual-based sensing using image and video data.
1	Residential Intrusion Detection	Contextual Sensing	Context-aware sensing based on audio and environmental cues.
2	Volumetric Sensing	PIR Sensors	Passive infrared sensors for detecting human presence and motion.
2	Volumetric Sensing	Microwave Doppler	Microwave Doppler-based motion detection sensors.
2	Perimetric Sensing	Magnetic Contacts	Magnetic reed contacts for door and window status monitoring.
2	Perimetric Sensing	Glass Break (Acoustic)	Acoustic sensing for detecting glass breakage events.
2	Visual Sensing	IP Cameras (CNNs)	IP cameras integrated with CNN-based visual analytics.
2	Visual Sensing	Thermal Imaging	Thermal imaging sensors for detecting objects via heat signatures.
2	Contextual Sensing	Audio Analytics	Audio-based analytics for detecting anomalous acoustic events.

3.1. Sensor Fusion and Mathematical Modeling

Passive Infrared (PIR) sensors are ubiquitous but prone to false alarms caused by thermal noise. Modern engineering mitigates this via Sensor Fusion, typically pairing PIR with Microwave (MW) Doppler radar. The Doppler shift f_d for a target moving at velocity v is given by:

$$f_d = f_r - f_t = \frac{2v f_t \cos\theta}{c}$$

where f_t is the transmitted frequency, f_r is the received frequency, θ is the angle between the direction of motion and the radar beam, and c is the speed of light.

Alarm = PIR ∧ MW

ensuring that an alarm is triggered only when both thermal differential and Doppler shift are detected simultaneously [20]. This significantly reduces the Nuisance Alarm Rate (NAR).

3.2. Inertial and Spectral Analysis for Perimetric Protection

Perimetric sensors, such as glass break detectors, rely on spectral and temporal analysis of sound signatures. A typical glass break event produces a characteristic pattern:

an initial low-frequency “thud” (often below 200 Hz) as the object impacts the glass, followed by a high-frequency “crash” component (above 3 kHz) when the glass shatters.

Commercial detectors implement band-pass filtering and time-windowing to detect this sequence. A trigger is asserted only if:

- A low-frequency impulse is detected;
- A high-frequency burst follows within a small time window
  Δt, typically ms and <150
- The combined spectral energy matches a predefined glass break template [21].

4. Communication Architectures: The Nervous System

The communication subsystem serves as the nervous system of a residential security CPS. Its design dictates reliability, latency, energy efficiency, and resilience against both failures and attacks.

4.1. Wireless Mesh vs Star Topologies

Zigbee and Z-Wave adopt mesh topologies where nodes can relay messages for each other, extending range through multi-hop routing. Z-Wave operates in the sub-GHz band and generally offers superior wall penetration compared to Zigbee at 2.4 GHz in concrete residential structures [22]. This makes Z-Wave particularly attractive for deeply embedded sensors (e.g., in basements or behind reinforced walls).

Wi-Fi, by contrast, typically employs a star topology with access points at the center. It offers high throughput and broad device support, which is crucial for video transmission. However, its relatively high power consumption and contention-based medium access make it less suitable for low-power, battery-operated sensors.

A practical residential security deployment often combines these technologies: low-power sensors communicate over Zigbee, Z-Wave, or Thread, while video streams rely on Wi-Fi or Ethernet. A central hub or gateway bridges these domains and interfaces with cloud or edge services.

4.2. The Role of Matter and Thread

The industry is converging towards the Matter standard running over Thread and other IP-capable transports [9]. Thread provides a low-power IPv6 mesh network with self-healing capabilities and no single point of failure at the routing level. Matter, in turn, standardizes the application layer, enabling devices from different vendors to interoperate securely.

Unlike several legacy consumer protocols, Matter mandates strong cryptographic primitives, including AES-128 encryption and authenticated commissioning, together with secure device attestation [11]. Furthermore, by adopting an IP-based stack, Matter facilitates direct and secure end-to-end communication between edge devices, local controllers, and cloud services, simplifying integration into larger CPS architectures. From a systems engineering viewpoint, this convergence significantly eases the design of scalable, interoperable, and security-enhanced residential systems.

5. Edge Intelligence and Video Analytics

5.1. Deep Learning at the Edge

Traditional video-based motion detection, relying on simple pixel differencing or background subtraction, is increasingly inadequate in complex residential environments subject to lighting changes, shadows, and dynamic backgrounds. Modern systems instead employ CNN-based object detectors and classifiers deployed at the edge.

Lightweight CNN architectures such as MobileNet and YOLO Nano can distinguish between humans, vehicles, and pets in real time on embedded platforms with constrained computational and energy budgets [23]. Deploying these models on edge devices (e.g., smart cameras or local hubs) offers several benefits:

- Reduced latency: Decisions can be made locally without round-trip communication to the cloud.
- Improved privacy: Raw video can remain on-premises; only alerts or anonymized features are transmitted.
- Resilience to connectivity loss: Intrusion detection and local actuation continue to function in the absence of Internet connectivity.

For active deterrence mechanisms such as sirens, strobes, or fog generators, end-to-end latency is critical. We define the total system latency $\mathbf{L_{total}}$ as:

$L_{total}=T_{capture}+T_{trans}+T_{proc}+T_{act}$

where $T_{capture}$ is the sensing/capture time, T_{trans} is the communication delay, T_{proc} is the processing (inference) time, and T_{act} is the actuation delay.

5.2. Latency Modeling: Edge vs Cloud

Table 2. Latency Comparison Between Cloud and Edge Architectures

Architecture	Transmission Time (ms)	Processing Time (ms)	Capture / Actuation Time (ms)	Total Latency (ms)
Cloud Architecture	500	100	50	650
Edge Architecture	10	40	50	100

Note: The above values are intended only to illustrate the significant latency gap between cloud-based and edge-based deployments.

Table 2 compares cloud-centric and edge-centric architectures using these representative values. In a cloud-centric design, T_{trans} often dominates, with uplink latency easily reaching or exceeding several hundred milliseconds under real-world network conditions. In contrast, an edge-centric architecture keeps T_{trans} small by processing data locally, reducing L_{total} to well below 100 ms in typical residential scenarios.

Table 2. Comparative latency analysis of cloud-centric and edge-centric processing architectures.

As illustrated conceptually in Fig. 2, cloud-based architectures may yield total latencies on the order of hundreds of milliseconds (or more) due to network variability, which can be unacceptable for instant deterrence. Edge architectures, by minimizing dependence on wide-area networks, enable near-deterministic responses that are essential for immediate threat mitigation [24].

6. Cybersecurity and Threat Landscape

Residential security systems themselves are attractive targets for attackers, as compromising them provides both privacy-sensitive information and potential physical access. The integration of wireless communication, cloud connectivity, and third-party mobile applications introduces a broad and heterogeneous threat landscape.

6.1. Attack Vectors in Residential CPS

Key attack vectors include:

- **Wireless protocol attacks:** Jamming, eavesdropping, replay, and key extraction on Zigbee, Z-Wave, Wi-Fi, or Thread links [7], [8].
- **Device compromise:** Exploitation of vulnerabilities in firmware, bootloaders, or exposed debug interfaces, enabling persistent malware or unauthorized control.

- **Cloud and API abuse:** Attacks on cloud backends, REST APIs, or MQTT brokers to manipulate device states or exfiltrate data.
- **Mobile app exploitation:** Reverse-engineering of mobile applications, reuse of hard-coded keys, or abuse of weak authentication flows.

A systems engineering approach requires modeling these threats at the architectural level rather than treating security as a set of isolated patches.

6.2. Security Requirements

From this threat analysis, we can derive key security requirements for residential CPS:

- End-to-end confidentiality and integrity for all control and telemetry traffic.
- Strong device identity and attestation, ensuring that only legitimate devices join the network.
- Least-privilege access control, both for cloud services and local components.
- Local fail-safe behavior: The system should degrade gracefully and safely under connectivity loss or partial compromise.
- Privacy-by-design, limiting the exposure of raw sensor data and employing techniques such as on-device processing and federated learning.

These requirements inform the design of the Autonomic Residential Security Architecture described in the next section.

7. Autonomic Residential Security Architecture (ARSA)

7.1. Architectural Overview

The proposed Autonomic Residential Security Architecture (ARSA) integrates heterogeneous sensing, edge AI, and federated learning within a layered CPS framework. The architecture comprises three principal layers:

1. Physical Sensing Layer: PIR and microwave motion sensors, magnetic contacts, glass break detectors, smart locks and actuators, and IP/thermal cameras.

2. Edge Intelligence Hub: A local gateway or home hub that aggregates sensor data, performs sensor fusion, runs CNN-based inference, and manages local policies.

3. Cloud (Federated Server) Layer: A backend that coordinates federated learning, aggregates model updates from multiple homes, and distributes improved global models.

Figure 3 provides a conceptual block diagram of ARSA, showing the data flows between sensors, the edge intelligence hub, and the federated cloud server.

To complement Fig. 3, Table 3 summarizes the main layers, their internal components, and the data flows between them.

Table 3. Layers, Components, and Data Flows in the Proposed ARSA System

3-A. Main Layers in the Proposed Architecture

Layer	Brief Description
CLOUD LAYER (Federated Server)	Central server responsible for aggregating and updating global models using federated learning.
EDGE INTELLIGENCE HUB	Home-resident edge node performing local inference and data processing.
PHYSICAL SENSING LAYER	Physical layer consisting of sensors and devices (cameras, motion sensors, smart locks, actuators).

Table 3-B. Components Within Each Layer and Their Functions

Layer	Component	Role / Function
CLOUD LAYER	Global Model Database	Stores the global model and aggregates encrypted model updates from edge nodes.
EDGE INTELLIGENCE HUB	Sensor Fusion Engine	Fuses heterogeneous sensor data to produce a unified intrusion decision.
EDGE INTELLIGENCE HUB	Local CNN Inference	Performs local CNN-based inference on image and video streams.
EDGE INTELLIGENCE HUB	Privacy & Encryption Gate	Ensures privacy by uploading only encrypted model updates to the cloud.
PHYSICAL SENSING LAYER	PIR / Microwave Sensors	Motion sensors for intrusion and human presence detection.
PHYSICAL SENSING LAYER	Smart Locks & Actuators	Execute control actions such as locking, unlocking, and alarm triggering.
PHYSICAL SENSING LAYER	IP Cameras	Provide video and image data for local edge analysis.

Table 3-C. Data Flow Description

From → To	Arrow Style in Figure	Purpose
PIR / Microwave Sensors → Sensor Fusion Engine	Solid black arrow	Transmits sensor measurements to the edge fusion engine.
IP Cameras → Local CNN Inference	Solid black arrow	Forwards video streams for local deep learning inference.
Privacy & Encryption Gate → Global Model Database	Dotted blue upward arrow	Uploads encrypted model updates without sharing raw data.
Global Model Database → Edge Intelligence Hub	Dotted red downward arrow	Distributes the updated global model back to edge nodes.

7.2. Sense–Analyze–Plan–Act–Learn Loop

ARSA is designed around a continuous autonomic control loop:

- **Sense:** Physical sensors and cameras capture environmental data regarding motion, door/window status, and visual scenes.
- **Analyze:** The edge hub fuses multi-modal signals (e.g., PIR + MW + visual cues) and applies CNN-based analytics to classify events (e.g., human vs pet vs vehicle).
- **Plan:** Based on policies, context (time of day, occupancy state), and threat level, the system selects a response strategy (e.g., local alarm only, silent notification, or active deterrence).
- **Act:** Smart locks, sirens, lights, and other actuators execute the selected response within tight latency constraints.
- **Learn:** Periodically, the edge hub computes gradient updates or compressed feature statistics and sends them to the federated server. The cloud aggregates these updates across many homes and disseminates improved models back to the edge.

This loop enables ARSA to adapt over time to changing environments, occupant habits, and

evolving threat patterns while minimizing manual configuration.

7.3. Privacy and Federated Learning

A core design tenet of ARSA is to avoid transmitting raw sensor data, particularly video and audio, to the cloud. Instead, model training leverages federated learning:

- Edge devices train local models on their private data.
- Only anonymized model updates or gradients, optionally protected with secure aggregation and encryption, are sent to the cloud.
- The cloud server aggregates these updates into a global model and returns it to participating homes.

This approach reduces privacy risks associated with centralized data storage while still allowing the system to benefit from cross-home learning, such as improved detection of rare or emerging intrusion patterns.

8. Discussion

The proposed ARSA framework illustrates how a systems engineering perspective can unify sensing physics, communication infrastructure, AI algorithms, and security requirements into a coherent architecture. Several practical considerations remain:

- Deployment heterogeneity: Legacy devices without Matter/Thread support will coexist with newer, IP-based nodes, requiring backward-compatible gateways.
- Resource constraints: Not all homes will have sufficient edge computing resources to run advanced CNNs; tiered deployment strategies may be needed.
- Model drift and evaluation: In federated learning, detecting concept drift and ensuring robust global model evaluation without access to raw data is challenging.
- User acceptance: System complexity must be hidden behind user-friendly interfaces, and privacy assurances must be communicated clearly to occupants.

These issues highlight promising avenues for future applied research and pilot deployments.

9. Conclusion and Future Work

This paper has presented a system-level perspective on residential electronic security in the IoT era. We developed a taxonomy of sensing modalities grounded in sensing physics, analyzed volumetric and perimetric detection logic, and discussed the implications of different communication architectures. We then examined the role of edge intelligence and CNN-based video analytics, emphasizing latency as a key design constraint. Building on these foundations, we introduced the Autonomic Residential Security Architecture (ARSA), which integrates heterogeneous sensing, edge AI, and federated learning into a continuous sense–analyze–plan–act–learn loop designed to be resilient, privacy-aware, and self-managing.

Future work includes implementing and experimentally validating ARSA in real residential testbeds, quantitatively evaluating detection performance, latency, and privacy benefits, and extending the architecture to incorporate formal verification of safety and security properties. Furthermore, integrating explainable AI techniques could improve transparency and user trust in automated security decisions.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gen. Comput. Syst., vol. 29, no. 7, 2013.

[3] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” Inf. Syst. Front., vol. 17, 2015.
[4] J. Lin et al., “A survey on internet of things: Architecture, enabling technologies, security and privacy,” IEEE IoT J., vol. 4, no. 5, 2017.
[5] J. Wurm et al., “Security in the Internet of Things: A Survey,” IEEE Trans. Instrum. Meas., 2016.
[6] A. Al-Fuqaha et al., “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Comm. Surveys Tuts., 2015.
[7] D. Geneiatakis et al., “Security assessment of smart home protocols: The ZigBee case,” in Proc. IEEE CAMAD, 2017.
[8] S. Knight et al., “Home Security Systems: A Survey of Wireless Vulnerabilities,” Int. J. Adv. Comput. Sci., 2019.
[9] Connectivity Standards Alliance, “The Matter Standard Specification 1.0,” 2022. [Online].
[10] M. B. Alazzam and A. Al-Rousan, “Matter Protocol: A New Era of IoT Interoperability and Security,” J. Sens. Actuator Netw., vol. 12, no. 1, 2023.
[11] K. Smith, “Demystifying Matter: Security Architecture of the New Smart Home Standard,” IEEE Consum. Electron. Mag., 2023.
[12] W. Shi et al., “Edge computing: Vision and challenges,” IEEE IoT J., vol. 3, no. 5, 2016.
[13] X. Zhang and Y. Wang, “Edge Intelligence for Smart Home Security: A Comparative Study,” IEEE IoT J., vol. 9, no. 4, 2022.
[14] A. Howard et al., “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications,” arXiv:1704.04861, 2017.
[15] J. Redmon and A. Farhadi, “YOLOv3: An Incremental Improvement,” arXiv:1804.02767, 2018.
[16] H. B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” AISTATS, 2017.
[17] T. D. Nguyen et al., “Deep Federated Learning for Autonomous Intrusion Detection in IoT,” IEEE Access, vol. 8, 2020.
[18] S. Abdulrahman et al., “A Survey on Federated Learning for the Internet of Things,” IEEE Access, vol. 9, 2021.
[19] L. Mothukuri et al., “Federated Learning for Anomaly Detection: A Survey,” IEEE Access, vol. 10, 2022.
[20] R. Z. A. Zughaibi, “Analysis of Dual-Technology Motion Sensors in Uncontrolled Environments,” J. Eng. Sci. Tech., 2020.
[21] S. Chen et al., “Acoustic Event Detection for Glass Break in Home Security,” Proc. IEEE ICASSP, 2021.
[22] C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” IEEE Commun. Mag., 2010.
[23] F. P. Tso et al., “Edge vs. Cloud: A pragmatic analysis of video analytics,” IEEE Conf. Cloud Comput., 2019.
[24] M. Satyanarayanan, “The Emergence of Edge Computing,” Computer, vol. 50, no. 1, 2017.
[25] E. Stellios et al., “A Survey of IoT Attacks,” IEEE Commun. Surveys Tuts., 2018.
[26] NIST Special Publication 800-183, “Networks of ‘Things’,” 2016.
[27] T. Eisenbarth et al., “Lightweight Cryptography for the IoT,” IEEE Des. Test, 2018.
[28] Q. Yang et al., “Federated Machine Learning: Concept and Applications,” ACM TIST, 2019.
[29] W. Y. B. Lim et al., “Federated Learning in Mobile Edge Networks: A Comprehensive Survey,” IEEE Commun. Surveys Tuts., 2020.
[30] Y. Liu et al., “Privacy-Preserving Deep Learning for IoT Security,” IEEE IoT J., vol. 8, 2021.

[31] A. Imteaj et al., “A Survey on Federated Learning for Resource-Constrained IoT Devices,” IEEE IoT J., vol. 9, 2022.
[32] H. K. Lee et al., “Autonomic Computing in Smart Homes,” IEEE Trans. Consum. Electron., 2020.
[33] D. P. Kumar et al., “Smart Home Energy Management Systems,” Energies, 2023.
[34] J. Doe and R. Roe, “Vulnerability Analysis of Smart Locks,” Comput. Secur., 2024.
[35] S. Gupta, “AI-Driven Security for Next-Gen Smart Cities,” Elsevier Smart Cities, 2024.