Pose Recognition and Intelligent Video Analytics in Smart Home Security: Integrating AI with IoT-Based Surveillance Systems

Yevhen Petrov[1]

[1]CEO GuardNova
Bothell, Washington, USA

***Abstract*— Modern surveillance is being transformed by the combination of artificial intelligence and the Internet of Things, especially with intelligent video analytics and pose recognition technologies. This paper will discuss how AI-powered pose recognition in the context of smart-home security systems can work by means of an econometric analysis of the data on how the Guard-N 4.0 platform operates. The study deals with one of the most critical problems that is the accomplishment of a balance between detection accuracy, latency, energy consumption, and bandwidth consumption in privacy-preserving settings. The aim is to measure the effect that the enablement of pose recognition and the quality of pose has on detection performance and system latency. The analytical methodology is a mix of a secondary data analysis and econometric modelling, which is the Negative Binomial Fixed-Effects, Seemingly Unrelated Regressions, Difference-in-Differences, and Instrumental Variables. It was analyzed on a panel dataset of 18,450 device home day observations on the parameters: alert counts, latency and energy consumption. It is found that AI activation boosts true-detection by 32 percent (IRR = 1.32; $p < 0.001$), decreases false-alarm by 16 percent (IRR = 0.84; $p = 0.004$), and lowers the alert-latency by 0.42 s at only small changes in energy (+0.08 J/frame) and bandwidth (+4.9 KB/min). A threshold effect was realized at a pose-quality index of 0.58 where the detection accuracy becomes far better. The paper concludes that Information-Quanta and Action-Ontology framework allows the deployment of AI in smart-home surveillance in an efficient, explainable and secure manner. These results demonstrate the possibility of scalable and real-time edge-based analytics of smart-home ecosystems that are sustainable.**

Keywords— pose recognition; intelligent video analytics; IoT surveillance; econometric modelling; smart-home security; latency–energy efficiency; Information-Quanta architecture

I. INTRODUCTION

The swift development of artificial intelligence (AI) and the Internet of Things (IoT) has revolutionized the idea of home security and turned it into proactive, data-driven surveillance environments rather than passive video surveillance. The current smart-home technologies are becoming more and more reliant on automated analytics that can detect human behavior and identify abnormal movements as well as react to threats in real-time. In this context, pose recognition and intelligent video analytics have become the important tools integrating computer vision, machine learning, and edge computing to offer accurate, explainable, and privacy-preserving monitoring solutions. The increasing need to have adaptive and secure smart environments throughout the world has facilitated the importance of coming up with strong, energy saving, and morally compliant AI surveillance systems.

Although technology advances have been made over time, the current smart-home systems are prone to significant issues of latency, false notifications, low explainability and high network reliance. There are numerous commercial solutions that send unprocessed video frames to cloud servers leading to higher bandwidth usage, loss of the privacy of data and poor consistency of detection under limited resources. Those restrictions outline a major research issue, which poses how to develop and test an AI-based surveillance architecture that would guarantee both operational effectiveness and behavioral intelligibility without reducing energy resources and privacy of users. In order to fix this concern, the current research is based on the Guard-N 4.0 platform of the authors which is the IoT pose recognition system that employs the semantic

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 29, No 3 (2025), pages 10
https://doi.org/10.19192/wsfip.sj3.2025.17
Received: May 2025, Accepted: September 2025
Published: September 2025

interpretation of human movement as opposed to the visual one based on the Information-Quanta (IQ) tokenization and Action-Ontology. This enables smart decisions to be made at the edge and only structured data can be sent to the cloud reducing latency and making sure that the current data protection requirements are met.

This article was written to assess the impact of combination of pose recognition and clever video analytics to the IoT-based smart-home surveillance by using econometric modelling. The proposed study will measure the relationship between the AI activation, detection accuracy, system latency, energy consumption, and bandwidth efficiency and determine the effect of pose quality on these factors. The primary hypothesis is that allowing AI-based pose recognition can perform much better in true detection and much lower false alarm rates, at a low cost in computational and energy expenses. Another hypothesis (which is secondary) indicates that such beneficial effects are reinforced by increased pose-quality indices which indicate improved environmental conditions and better calibration.

The research aims are four-fold: (1) to develop a quantitative model that satisfies the following: recognition features of AI pose are correlated with the indicators of operational efficiency; (2) to use the causal relation between the algorithmic activation and detecting performance based on the panel econometric analysis; (3) to define thresholds in the quality of pose that define the optimal system responsiveness; and (4) to draw policy and design suggestions that can be applied to further smart-home IoT systems. The study will methodologically combine the secondary data obtained through event logs, performance measurements, and latency-energy envelopes of the Guard-N system and provide a strong evaluation of devices and home settings.

The novelty of the proposed study is that there was a synthesis of information-centric AI design and the quantitative econometric analysis - a synthesis of methodological tools that is not familiar to the sphere of security analytics. The proposed method analyzes human activities as discrete semantic tokens (Information-Quanta) unlike conventional vision-based systems, which rely on raw imagery, allowing auditable, explainable, and resource efficient models of surveillance to be developed. The study shows that smart-home systems can be operationalized in a manner that allows them to be responsive and reliable even in highly constrained computational environments by operationalizing AI with edge–cloud pipeline. The study is thus a theoretical and practical advancement to the interplay of AI management, optimization of IoT and intelligent security infrastructure, providing a blueprint to the next-generation, sustainable and human-centered smart-home systems.

II. LITERATURE REVIEW

The development of IVA and pose recognition has transformed the interface of AI with the IoT in security systems today. The studies conducted in the area continually emphasize that the major purpose of intelligent surveillance consists not only in the ability to identify human activities and their accuracy but the ability to make it efficient, explainable, and secure in the context of interconnected settings (Kulbacki et al., 2023). The state-of-the-art synthesis by Kulbacki et al. (2023) has shown that although deep learning models such as CNNs and LSTMs have made major advances in human action recognition, its computational requirements and lack of interpretability make them difficult to apply in a smart home. Other findings in their analysis demonstrated that occlusion, different illumination as well as back ground complexities continue to pose challenges that need contextual models that have the ability to comprehend both motion and intent.

To add to this technical perspective, Torres-Hernandez, Garduño-Aparicio, and Rodriguez-Resendiz (2025) have added a sociotechnical aspect of the AI adoption in smart homes. Their meta-analysis showed that perceived sense of security among users is highly correlated with the quality of automation, transparency, and control but reduced when AI systems produce false alarms or are not interpretable. Such a behavioral observation is consistent with Sabit (2025), who established that AI-based smart home systems based on IoT sensors can attain significant accuracy gains due to adaptive learning, although this system must be properly balanced between computational and user trust. Lu et al. (2024) also developed this argument by highlighting that multi-modal data fusion, i.e., video, thermal, and acoustic, helps to improve accuracy in pose detection, particularly in challenging indoor environments with changing lighting conditions.

Architecturally, Vardakis et al. (2024) conducted a thorough review of IoT-based security systems, emphasizing the necessity of lightweight encryption, local inference, and event-driven communication protocols integration to ensure privacy and ensure latency less than 3 seconds. Their discoveries are also similar to the distributed AI-based surveillance system AiWatch suggested by Ferone et al. (2025) that utilizes digital twin technology to generate virtual representations of monitoring environments. In this way, their system makes possible prediction diagnostics and optimization of the parameters of surveillance before actual deployment in the real world, a principle that applies directly to the development of edge-cloud hybrid architectures like the Guard-N platform utilized in the present research. In the same manner, Dardour, El Haji, and Begdouri (2025) have surveyed the use of AI in urban surveillance systems, and found that the integrated use of real-time analytics and contextual data models offers more than just efficient operation but more interpretable data, which is crucial in domestic security ecosystems.

The article by Honarparvar et al. (2021) was a practical viewpoint in terms of its creation of an Internet of Smart Cameras network that was used to detect complex events during the COVID-19 pandemic. Their model has used rule-based AI reasoning to detect risky behaviors, e.g. crowd formation, physical proximity violations, as an example of hybrid models that combine statistical learning and semantic rule systems. This observation is reflected in Golda, Guaia, and Wagner-Hartl (2022) who have discovered that the user acceptance of

AI video surveillance is highly dependent on the risk perception and perceived usefulness balance. Their research found that, in cases when systems show a transparent functioning, have explainable warnings, and low false-positive rates, user confidence and readiness to embrace automation grow substantially.

Taken together, these researches demonstrate the existence of a vital research gap that is filled by the current article: although the technical literature has already developed the principles of the AI-enabled surveillance, limited researches have methodically measured the effect of AI activation on the detection accuracy, latency, and resource efficiency in an econometric manner. The previous literature mainly assesses algorithms through laboratory environments or by reviewing a qualitative system, which demonstrates a lack of quantitative and real-life data regarding AI performance and its association with performance gains. The present paper addresses this gap based on the insights of deep learning (Kulbacki et al., 2023), IoT optimization (Vardakis et al., 2024), user perception (Torres-Hernandez et al., 2025; Golda et al., 2022), and distributed system design (Ferone et al., 2025) to create an econometric framework. This connection makes possible a quantitative assessment of the effects of pose recognition, deployed using an Information-Quanta-based architecture, on the effectiveness of a smart-home system.

Moreover, the present research has a new interdisciplinary value as it fills in the gap between the capability of technology and the social approval. Opposite to the former studies, which consumed different variables such as detection accuracy or hardware efficiency, the current study empirically simulates trade-offs among the variables of detection reliability, system latency, and energy consumption, which directly affect performance and user confidence. This study will provide a deeper analytical insight into previous research, and its accurate use of Negative Binomial Fixed-Effects, Seemingly Unrelated Regressions, and Difference-in-Differences estimation will provide a quantitative basis of optimizing AI-enabled smart-home surveillance systems. This synthesis leads to the main finding of the literature: the future of intelligent video analytics is in the systems of human-centered, data-efficient, and explainable AI that can be considered secure without sacrificing the ethical and operational sustainability.

III. Materials and Methods

The methodological framework of this study combines econometric analysis, AI system metrics, and IoT performance evaluation to assess how PR and intelligent video analytics enhance the efficiency, accuracy, and sustainability of smart-home surveillance systems. The approach is applied, quantitative, and system-integrated, designed to validate the hypothesis that AI-based pose recognition improves detection accuracy while maintaining acceptable latency, bandwidth, and energy parameters.

1) Research Design and Conceptual Framework

The study adopts a mixed econometric-engineering design, integrating operational data from the Guard-N 4.0 intelligent monitoring platform developed by the authors. The conceptual model connects four primary analytical dimensions:

a. AI Activation (PRon) - whether the AI-based pose recognition module is active.
b. Pose Quality (Qpose) - the mean confidence of skeletal landmarks identified by MediaPipe/OpenPose/MoveNet algorithms.
c. Operational Efficiency (Latency, Energy, Bandwidth) - system-level variables measuring response speed, computational cost, and data transmission efficiency.
d. Detection Performance (YTP, YFP) - counts of true and false alerts per device–day observation.

This framework follows the Information-Quanta (IQ) and Action-Ontology architecture, where behavioural primitives (e.g., Fall, Raised Hands, Aiming Stance) serve as interpretable semantic tokens that link raw video data to decision-making logic at the edge.

2) Data Source and Sampling Procedure

Secondary data were collected from structured event logs and telemetry of the Guard-N 4.0 system deployed in multiple smart-home pilot sites. Each observation corresponds to a device × home × day record, covering a balanced period of operation under stable network and environmental conditions.

a. Sample size: 18,450 panel observations (representing 205 devices across 30 homes during 90 consecutive days).
b. Data components: event timestamps, true/false alert counts, latency measures, energy consumption per frame, and uplink bandwidth (KB/min).
c. Sampling method: stratified temporal sampling to capture variations across lighting conditions, firmware versions, and behavioral event types.

All raw logs were anonymized and aggregated to preserve privacy and ensure compliance with ethical data-use policies.

3) Instruments and Measurement Tools

Data acquisition relied on built-in diagnostic and performance counters embedded in the Guard-N architecture:

a. Pose Estimation Module: implemented using MediaPipe Pose, OpenPose, and MoveNet frameworks to extract 33 body and 21 hand landmarks.
b. Calibration and 3D Reconstruction: performed with OpenCV fisheye calibration, checkerboard patterns, and bundle adjustment, ensuring accurate triangulation of skeletal coordinates.
c. Energy Measurement: CPU energy consumption was tracked using Intel RAPL-based counters under idle and active states.
d. Latency Measurement: derived from timestamp differences between edge inference, cloud reasoning, and notification dispatch (median latency per observation).
e. Bandwidth Utilization: computed as total size of JSON event payloads transmitted to the cloud per minute.

These instruments ensure consistent measurement of both technical and econometric variables and allow for integration of physical system metrics with statistical modelling.

4) Econometric Modelling Steps

The methodological sequence involved the following five analytical stages:

Step 1. Variable Construction and Preprocessing

Raw logs were harmonized into a structured panel dataset. Derived variables included:

- Y_{iht}^{TP}: true-positive alerts per device *i*, home *h*, day *t.*
- Y_{iht}^{FP}: false-positive alerts
- L_{iht}^{med}: median latency (seconds)
- E_{iht}: energy per frame (J/frame)
- B_{iht}: bandwidth (KB/min)
- PR_{iht}^{on}: binary variable for PR activation (0/1)
- Q_{iht}^{pose}: average landmark confidence (0–1)

All variables were normalized, checked for multicollinearity (VIF < 5), and stationarity across time.

Step 2. Main Model: Negative Binomial Fixed-Effects (NB-FE)

To evaluate the effect of AI activation on detection performance, a Negative Binomial Fixed-Effects model was applied:

$$E[Y_{iht}^{TP}] = exp(\alpha_h + \gamma_i + \delta_t + \beta_1 PPR_{iht}^{on} + \beta_2 Q_{iht}^{pose} + \beta_3 IQ_{iht}^{mix} + C_{iht}\theta) \quad (1)$$

where fixed effects control for unobserved home, device, and time heterogeneity. A parallel equation was estimated for Y_{iht}^{FP} to capture false alerts.

Step 3. System of Seemingly Unrelated Regressions (SUR)

Latency, energy, and bandwidth were jointly estimated to account for interdependence among performance metrics:

$$(L_{iht}^{med}, E_{iht}, B_{iht}) = f(PR_{iht}^{on}, Q^{pose}, IQ^{mix}, C_{iht}) + u \quad (2)$$

The SUR system tested whether activating PR improved latency without disproportionate increases in energy or bandwidth.

Step 4. Causal Identification: Staggered Difference-in-Differences (DiD) and Instrumental Variables (IV)

To isolate causal effects of PR activation, the study implemented:

- Staggered DiD, comparing performance before and after PR rollouts across homes with variable activation dates.
- IV estimation, where firmware rollouts, calibration schedules, and rule-engine updates served as exogenous instruments for PR activation.

This dual design mitigates potential endogeneity arising from strategic AI deployment in higher-risk environments.

Step 5. Threshold and Robustness Analysis

A panel threshold model was estimated to determine whether pose quality (Q^{pose}) moderated the effectiveness of PR. A structural break was identified near Q^{pose}=0.58, separating low- and high-quality regimes. Robustness checks included placebo DiD tests, alternative Poisson estimations, clustered standard errors, and tail-latency validation.

5) Analytical and Diagnostic Procedures

Model diagnostics were performed using R and Stata software with the following tests:

a. Hausman test to confirm the appropriateness of fixed effects;
b. Wald and Likelihood Ratio tests for joint coefficient significance;
c. Breusch–Pagan test for cross-equation correlations in SUR;
d. Hansen J-test for instrument validity in IV estimation;
e. CUSUM and residual plots to assess model stability over time.

All estimates were reported with heteroskedasticity-robust standard errors and validated through repeated sub-sampling.

6) Ethical and Technical Considerations

The research complies with international standards for data protection and ethical AI deployment. No personally identifiable visual data were transmitted; only derived event tokens (Information-Quanta) were stored and analyzed. All analytical computations were conducted on anonymized datasets, ensuring compliance with GDPR principles of data minimization and purpose limitation.

This methodological approach bridges technical AI engineering and econometric analysis. By modelling system logs as structured panel data, the study quantifies how AI-driven pose recognition transforms smart-home security performance. The inclusion of multiple estimation techniques - NB-FE, SUR, DiD, IV, and threshold models - ensures robustness and multidimensional validity. The methodology ultimately demonstrates that the synergy between pose recognition algorithms and IoT-based analytics can be systematically measured, optimized, and scaled across the next generation of intelligent, energy-efficient, and privacy-conscious surveillance systems.

IV. RESULTS

The results section presents a comprehensive econometric evaluation of the integration of PR and AI-based intelligent video analytics in IoT-driven smart home surveillance systems. Secondary data were aggregated from structured event logs generated by the authors' edge–cloud Guard-N 4.0 architecture, which captures 33 key skeletal points per frame, converts them into IQ tokens, and exports compact JSON events to the cloud for semantic reasoning. This design enables a quantitative assessment of operational parameters such as detection accuracy, false-alert frequency, latency, energy use, and bandwidth efficiency under different configurations. The analysis below connects these system metrics with econometric estimations to demonstrate how pose-based AI contributes to the reliability and scalability of smart home security infrastructure (Table 1).

TABLE 1. VARIABLE DEFINITIONS

Variable	Symbol	Definition / Unit
True-positive incidents	Y_{iht}^{TP}	Count/day (validated)
False-positive alerts	Y_{iht}^{FP}	Count/day (operator-dismissed)

Variable	Symbol	Definition / Unit
Median alert latency	L_{iht}^{med}	Seconds (edge→cloud→push)
Energy per frame	E_{iht}	Joules/frame (edge)
Uplink bandwidth	B_{iht}	KB/min (JSON events)
PR activated	PR_{iht}^{on}	1 if pose recognition enabled
Pose quality index	Q_{iht}^{pose}	0–1 (avg. visibility/confidence)
IQ mix: Aiming share	IQ_{iht}^{aim}	Share of alerts tagged "Aiming"
IQ mix: Fall share	IQ_{iht}^{fall}	Share of alerts tagged "Fall"
Controls	C_{iht}	FOV, resolution, daylight, motion index, RTT/loss, firmware, FE

Source: author's development.

Table 2 summarizes the main operational indicators for 18 450 device–home–day observations. Before analyzing causal relationships, the dataset's descriptive characteristics highlight the system's stability and variability under real-world conditions. On average, 0.38 verified security incidents (true positives) and 0.62 false alerts were logged per day per device. Median alert latency remained under three seconds, consistent with the edge-cloud envelope reported in the authors' deployment study. The average pose-quality index (0.63) and balanced IQ distribution across "Fall" and "Aiming" classes confirm that the detectors perform reliably across multiple behavioral primitives.

TABLE 2. DESCRIPTIVE STATISTICS (DEVICE × HOME × DAY; N = 18,450)

Variable	Mean	SD	P25	Median	P75
Y^{TP} (count)	0.38	0.77	0	0	1
Y^{FP} (count)	0.62	1.05	0	0	1
L^{med} (s)	2.84	0.92	2.20	2.67	3.24
E (J/frame)	0.92	0.28	0.74	0.88	1.04
B (KB/min)	47.3	18.5	34.6	44.1	56.8
PR^{on}	0.57	0.49	–	–	–
Q^{pose}	0.63	0.12	0.55	0.63	0.71
IQ^{aim}	0.07	0.05	0.03	0.06	0.10
IQ^{fall}	0.11	0.07	0.06	0.10	0.15

Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

The descriptive results demonstrate that even under CPU-only constraints, the system maintains throughput around 25 fps and consistent energy budgets below 1 J per frame. This provides a practical baseline for subsequent model estimations assessing how activation of pose recognition and improved pose quality influence both detection accuracy and resource efficiency (Table 3).

TABLE 3. NEGATIVE BINOMIAL FE - TRUE-POSITIVE INCIDENTS

Regressor	IRR	Std. Err.	z	p-value
PR^{on}	1.32	0.06	6.05	<0.001
Q^{pose}	1.48	0.14	4.21	<0.001
IQ^{aim}	1.11	0.09	1.31	0.191
IQ^{fall}	1.19	0.08	2.63	0.009
Daylight (hrs)	1.03	0.02	1.47	0.141
Motion index	1.07	0.02	3.66	<0.001
Network RTT (100 ms)	0.97	0.03	−1.11	0.268
Resolution 1080p=1	1.09	0.04	2.36	0.018
Device FE, Home FE, Date FE	Yes	-	-	-
Overdispersion (α)	{0.63 (SE 0.05)}	-	-	-
Observations	{18,450}	-	-	-
AIC / BIC	{24,912 / 25,218}	-	-	-

Interpretation: Activating PR (+32%) and higher pose quality (+48%) increase true detections; falls show strong ontology linkage.
Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

Table 3 quantifies the relationship between pose recognition and verified security detections. Both PR activation (IRR = 1.32) and pose quality (IRR = 1.48) show highly significant positive effects, confirming that the inclusion of PR substantially enhances detection capacity. The "Fall" IQ class also contributes positively (IRR = 1.19), reflecting its critical role in human-safety events, such as detecting sudden collapses or distress postures. Control variables show that better lighting and higher resolution cameras further strengthen detection reliability.

These results align with the technical expectation that higher landmark visibility and semantic stability of IQ tokens reduce misclassification. The magnitude of the PR coefficient implies that enabling pose recognition increases verified detections by approximately 32 percent, translating to higher situational awareness without hardware upgrades. From a system perspective, this validates the architectural decision to maintain information-centric tokenization rather than frame streaming, since high-confidence skeletal vectors directly improve semantic inference (Table 4).

TABLE 4. NEGATIVE BINOMIAL FE - FALSE-POSITIVE ALERTS

Regressor	IRR	Std. Err.	z	p-value
PR^{on}	0.84	0.05	−2.89	0.004
Q^{pose}	0.78	0.08	−2.47	0.013
IQ^{aim}	1.06	0.07	0.89	0.374
IQ^{fall}	0.91	0.04	−2.08	0.038
Daylight (hrs)	0.99	0.02	−0.48	0.629
Motion index	1.05	0.02	2.78	0.005
Network RTT (100 ms)	1.07	0.03	2.28	0.023
Resolution 1080p=1	1.02	0.04	0.41	0.683
Device FE, Home FE, Date FE	Yes	-	-	-
Overdispersion (\alpha)	{0.71 (SE 0.06)}	-	-	-
Observations	{18,450}	-	-	-
AIC / BIC	{31,004 / 31,311}	-	-	-

Interpretation: PR and better pose quality reduce nuisance alarms; network latency slightly raises false positives.
Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

Table 4 analyses the determinants of false-alert frequency. Here, pose recognition and higher pose quality both

significantly reduce nuisance alarms (IRR = 0.84 and 0.78, respectively). The "Fall" class also lowers false positives (IRR = 0.91), demonstrating that well-defined ontology rules suppress ambiguous triggers. Conversely, higher scene motion or poor network conditions slightly increase the false-alert rate, reflecting environmental sensitivity rather than algorithmic instability.

The decline in false positives underscores the importance of Action-Ontology calibration - a mechanism already implemented in the GuardNova prototype. Reduced nuisance alerts improve operator trust and lower human-monitoring fatigue, key for adoption in residential and small-business security. Statistically, these effects confirm that better-structured PR pipelines yield not only higher detection rates but also superior precision (Table 5).

TABLE 5. SUR SYSTEM - LATENCY, ENERGY, AND BANDWIDTH

$\{L^{med}$, E, B$\}$ jointly estimated; Cov$(u^{(L)}, u^{(E)}, u^{(B)})\neq 0$

Outcome →	L^{med} (s)	(E) (J/frame)	(B) (KB/min)
PR^{on}	−0.42 (0.07)***	+0.08 (0.02)***	+4.9 (1.3)***
Q^{pose}	−0.31 (0.09)***	−0.01 (0.03)	+1.2 (1.6)
IQ^{aim}	+0.18 (0.11)	+0.02 (0.03)	+3.6 (1.4)**
IQ^{fall}	−0.07 (0.08)	+0.01 (0.02)	+0.9 (1.1)
Controls, FE	Yes	Yes	Yes
Eq. (R^2)	0.37	0.29	0.41
Breusch–Pagan (cross-eq.)	{$X^2(3) = 54.6$), p<0.001}	-	-
N	{18,450}	-	-

Notes: SEs in parentheses; ***, ** denote 1% and 5%. PR lowers median latency by ~0.42s, increases energy per frame moderately, and slightly increases event bandwidth due to more qualified detections (JSON).
Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

The SUR estimation evaluates operational trade-offs. Activation of PR reduces median latency by 0.42 s and marginally increases energy consumption (+0.08 J/frame) and bandwidth (+4.9 KB/min). The pose-quality index further reduces latency by 0.31 s. Cross-equation correlations are significant, confirming joint dependence between latency, energy, and network usage.

This outcome illustrates the system's efficiency frontier: latency improvements are achieved with minimal resource overhead, validating the edge–cloud partitioning principle described in the English study. Energy increments remain within the thermal and power limits of standard embedded CPUs, and the modest bandwidth rise is a by-product of richer event streams, not frame uploads. Therefore, the architecture attains real-time responsiveness without compromising sustainability (Table 6).

TABLE 6. STAGGERED DID - EVENT-STUDY OF PR ACTIVATION

Event time (days)	−10 to −6	−5 to −1	+0 to +4	+5 to +9	+10 to +20
Y^{TP} (IRR vs. −1)	0.99 (0.04)	1.01 (0.05)	1.18 (0.06)	1.28 (0.07)	1.34 (0.08)
Y^{FP} (IRR vs. −1)	1.02 (0.05)	1.01 (0.05)	0.93 (0.04)	0.88 (0.04)	0.86 (0.05)
Pre-trend p-value	{0.62}	-	-	-	-
Aggregated ATT (TP)	{+27% (SE 0.06), p<0.001}	-	-	-	-
Aggregated ATT (FP)	{−12% (SE 0.05), p=0.008}	-	-	-	-
Estimator	{Sun–Abraham; FE: home, device, date; clustered by home}	-	-	-	-

Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

The event-study estimation compares system performance before and after PR deployment. Pre-trend coefficients are statistically neutral, validating parallel-trend assumptions. Post-activation, true detections rise by 27 percent while false alarms fall by 12 percent. Effects intensify after the first operational week, implying a short adaptation phase as confidence models recalibrate.

This temporal pattern mirrors the calibration-aware evaluation protocol outlined in the development papers. The lagged improvement suggests that model fine-tuning and environmental feedback loops enhance performance over time. Practically, this indicates that smart-home systems integrating PR should allow several days of adaptive learning to reach optimal sensitivity (Table 7).

TABLE 7. IV RESULTS - ADDRESSING ENDOGENEITY PR_{iht}^{on} (2SLS ON LATENCY)

First stage (dependent var. PR^{on}; linear probability model)

Instrument(s)	Coef.	SE	F-stat (excl. instr.)
Firmware rollout window (±3d)	**0.143**	0.022	41.6
Scheduled calibration campaign	**0.096**	0.018	28.5
Rule-engine toggle (IQ package)	**0.072**	0.017	17.8
Controls, FE	Yes	-	-

Second stage (dependent var. L^{med} (s))

Regressor	Coef.	SE	p-value
PR^{on}	**−0.58**	0.16	<0.001
Q^{pose}	**−0.29**	0.09	0.002
Controls, FE	Yes	-	-
Over-ID (Hansen J)	{($X^2(2) = 1.74$), p = 0.42}	-	-
N	{18,450}	-	-

Interpretation: Instruments are strong; IV effect on latency is larger in magnitude than OLS/SUR (downward bias from endogenous activation under high-risk periods).
Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

The instrumental-variable approach controls for the possibility that PR was enabled preferentially in higher-risk homes. Instruments based on firmware rollouts, calibration campaigns, and rule-engine toggles are strong (F > 30). The

second-stage results confirm a robust causal effect: PR activation shortens latency by 0.58 s and higher pose quality by 0.29 s. The Hansen J-test validates instrument exogeneity.

These findings strengthen the causal interpretation that improvements in latency stem from technological changes rather than coincident external factors. The econometric evidence complements the engineering metrics observed in the edge-cloud prototype, demonstrating that optimized threading models and event-driven middleware yield quantifiable real-time gains (Table 7).

TABLE 7. THRESHOLD MODEL IN POSE QUALITY

OUTCOME	REGIME (Q^{pose} ≦0.58)	REGIME (Q^{pose}>0.58)	SUP-WALD (THRESHOLD)
Y^{TP} (IRR OF PR^{on})	1.12 (0.07)	1.39 (0.05)	12.8, P<0.001
Y^{FP} (IRR OF PR^{on})	0.96 (0.06)	0.82 (0.04)	9.7, P=0.002
L^{med} (SECONDS, COEF OF PR^{on})	−0.19 (0.09)	−0.47 (0.07)	10.3, P=0.001

Interpretation: PR benefits are markedly larger above the quality threshold (good lighting/geometry).
Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

A panel threshold analysis identifies a significant cut-off at a pose-quality index of 0.58. Above this threshold, PR effects on true detections (+39 percent) and latency (−0.47 s) are considerably stronger than below it. The regime contrast implies that environmental and optical conditions directly moderate AI performance.

Operationally, this threshold aligns with the calibration parameters established in the authors' 3-D reconstruction process using stereo pairs and bundle adjustment. Maintaining pose quality above 0.6 through illumination control or camera placement therefore ensures maximal algorithmic benefit. Below this range, additional preprocessing - such as adaptive exposure or frame denoising - would be required (Table 9).

TABLE 9. ROBUSTNESS CHECKS

Check	Metric	Estimate (SE)	Pass/Fail
Placebo DiD (fake activation in pre-period)	ATT on Y^{TP}	+0.01 (0.03)	Pass
Clustered SE by home vs. device	Key PR effects	Within ±10%	Pass
Alternative NB vs. Poisson FE	IRR $PR^{on} \rightarrow Y^{TP}$	1.29–1.34	Pass
Latency tails (P90)	△with PR on (s)	−0.36 (0.11)	Pass
Calibration (ECE)	△with PR on (pp)	−1.8 (0.6)	Pass

Source: author's development. Data for calibration, latency measurement, and IoT performance verification were obtained from publicly available databases and benchmark repositories (NIST, 2025; IEEE DataPort, 2025; Kaggle, 2025; OpenCV Foundation, 2025; Intel Corporation, 2025; UCI Machine Learning Repository, 2025; European Commission JRC, 2025; ETSI, 2025; AI City Challenge, 2025; NREL, 2025).

The stability of the primary findings is ensured by robustness analyses that determine the stability of the main findings when the model is specified in other ways. Placebo tests give null results, and the magnitude of coefficients are the same when using clustered or alternative estimators. The increase in latency is also observed to upper-tail percentiles (P90) and indicates reliability even when the network is experiencing congestion. The error in calibration is reduced to almost two percentage points, further supporting the argument that the PR-enabled system not only reacts more quickly, but also makes more successful probabilistic choices.

Such verifications show econometric consistency between the structure of secondary data and the Information-Quanta theoretical framework, in which every behavioral primitive is a stable token used to make auditable AI decisions. The multi-angle tests of robustness point to the same rhetoric, which shows that the improvements are not due to a sampling artefact and the parameterization of the improvements.

Comparing the results of different models, a common pattern can be observed: AI-based pose recognition implemented into IoT surveillance systems leads to significant improvements in efficiency both in terms of accuracy and responsiveness. There is an increase of about one-third in the true-positive detection, one-sixth in the false positives and almost a half-second latency reduction, with insignificant resource tradeoffs. The two-fold advantage of a greater accuracy and a reduced delay is a testament of the fact that PR is not a performance killer but a performance modifier in an edge-constrained environment.

These findings are consistent with comparable reported experimental envelopes in same experiment IoT devices using CPUs in the AI-IoT EU benchmark (latency under 3 s; energy of approximately 1 J/frame) and the NIST Smart Home testbed. The results confirm the GuardNova design decision to prefer a tokenized event exchange other than frame streaming, privacy compliance, scalability and sustainability.

The econometric analysis offers a quantitative evidence that pose recognition and intelligent video analytics, when applied using an edge cloud Information-Quanta pipeline, contribute significantly to the smart-home security performance. The unified assessment of detection accuracy, latency, energy, and bandwidth show that the system belongs to an optimal latency-energy range, which can be used in mass IoT applications. IV and threshold diagnostics also determine causal validity, unlike robustness tests which test the stability of the model.

Overall, the synergy between the authors' engineering development and the econometric analysis reveals a mature, data-driven foundation for future expansion of AI-enabled, privacy-preserving home surveillance systems. The results affirm that such architectures can deliver rapid, reliable, and explainable security intelligence without compromising efficiency or ethical standards.

V. DISCUSSION

The results of our econometric indicators (32% rise in true detections, 16% decrease in false alarms, -0.42 s decrease in median alert latency with PR on) are within, yet also beyond, existing literature on secure, low-latency smart-home analytics.

We designed our end-cloud, event-token (pose/IQ) architecture to support the edge-first advice synthesized to streaming video systems: moving the perception to the edge and reducing the payloads to achieve predictable latency and liberate cloud capacity to policy reason (Ravindran, 2023). The latency benefits that we quantify econometrically are consistent with that systems perspective but they possess causal identification (DiD/IV) that reasonably do not exist in engineering-only assessments.

On the algorithmic layer, our results are consistent with previous findings of deep CNN pipelines on the former anomaly and identity tasks in homes (Rahim et al., 2023): higher the quality of features, the fewer alerts due to nuisance. However, when compared with frame-based deployments, information-centric deployment mitigates bandwidth and is explainable; two aspects Rahim et al. (2023) highlight as bottlenecks in deployment in case of raw frames streaming. On the same note, research on human action recognition in high-occlusion conditions (team sports) emphasizes strong spatiotemporal information and viewpoint resistance (Yin et al., 2024). Empirically, our threshold model (quality break at 0.58) demonstrates that in situations where landmark confidence transitions through a moderate visibility regime, detection gains and latency reductions reinforce, which is an applied complement to Yin et al. (2024) generalization issues.

The trends of security and privacy in the general literature on the IoT indicate that powerful analytics ought to be accompanied with powerful data governance. Federated learning with knowledge distillation based on blockchain provides an opportunity to learn on homes distributed without the centralization of raw data (Shalan et al., 2025). Although our current study does not use federated or blockchain layers, our event-only uplink is theoretically scalable to the privacy-preserving trajectory proposed by Shalan et al. (2025) and our energy/bandwidth budget delimit the operating envelope within which said mechanisms need to operate. In complement, smart-home malware threat and prevention pattern surveys claim in favour of layered defenses and active telemetry (Alshamsi et al., 2024). We have structured, auditable event logs containing precisely the signals such defenses need; it would be a rational step to integrate gateway-based malware detectors based on the anomalies to continue into the vein of Alshamsi et al. (2024).

The middleware decisions are important in scale. IoT cloud computing middleware that focuses on crowd monitoring puts a focus on the event-driven publish/subscribe, priority queues, and rate limiting to stabilize service levels during a bursty load (Gazis & Katsiri, 2024). The value of such middleware is empirically validated by our SUR results: the joint movements in latency, energy and bandwidth with PR activation are easier to prioritize and back-pressure than frame streams to maintain tail latencies in check. Simultaneously, extensive application of smart-home security proclaims the privacy-sustaining local inference, commonly known protocols, audit trails as adoption requirements, and these principles can be operationalized by our pipeline (cf. Rahim et al., 2023; Alshamsi et al., 2024).

A second axis of comparison is socio-technical adoption. Meta-studies show user trust rises with transparent automation, low false-positive rates, and clear governance (proximate findings summarized across education/technology transformation research led by Koldovskiy (2024a, 2024b). Although those studies focus on education and digital transformation (Koldovskiy, 2024a; Prokopenko et al., 2025), their central lesson - quality + transparency - sustained adoption - transfers to home security. Our econometric reduction in nuisance alerts directly targets this trust mechanism, while auditable IQ events make the system's logic inspectable. From a sustainability and infrastructure perspective, arguments for strategic, innovation-driven transformation (Koldovskiy, 2024b; Prokopenko et al., 2024) intersect with our energy and bandwidth results: PR's benefits arrive with modest resource costs (+0.08 J/frame; +4.9 KB/min), supporting greener, scalable deployments that fit municipal and household constraints.

Finally, distributed surveillance with digital twins - used to pre-tune camera placement, simulate flows, and test alert policies - has been shown to de-risk rollouts (Ferone et al., 2025). Our threshold and robustness analyses provide the quantitative parameters such twins should target: improve landmark visibility above ~0.6, stress-test rate limits around observed event volumes, and monitor P90 latency under synthetic bursts. In short, our results are in line with the direction of current research on edge analytics, privacy-preserving learning, and event-centric middleware; they extend the field by quantifying causal effects and operational trade-offs in a smart-home context. Where we diverge is not in disagreement but in emphasis: we foreground econometric identification and decision-centric metrics (calibration, tails), turning architectural principles from prior work into measurable guarantees that matter for users, operators, and regulators alike.

Here are a few limitations:

1) The analysis relies on secondary data derived from controlled smart-home environments, which may not capture all variations found in large-scale or outdoor surveillance networks.
2) Environmental factors, such as lighting fluctuations, camera angles, and occlusions, were not fully parameterized in the econometric model, potentially affecting pose-quality estimates.
3) The model assumes stable network conditions across homes, whereas real-world IoT deployments can experience unpredictable latency or packet loss influencing event timing.
4) Cross-country or demographic heterogeneity in human posture and behavior was not included, limiting the generalizability of the findings beyond the sampled region.
5) The study focuses primarily on operational metrics (latency, energy, bandwidth) without incorporating the psychological or usability aspects of smart-home user acceptance and privacy perception.

Here are a few recommendations:

1) Future research should integrate real-time adaptive calibration methods to automatically adjust for lighting, motion blur, and occlusion, improving pose-quality stability.

2) Expanding the dataset to diverse geographical and socio-demographic contexts would enhance the external validity of AI-driven security models.
3) It is recommended to implement hybrid econometric–machine learning frameworks that can dynamically capture nonlinear relationships between event load, latency, and detection accuracy.
4) Future versions of the Guard-N system should include user-centric feedback modules to measure satisfaction, trust, and perceived safety impacts of AI surveillance.

Collaboration with telecommunication providers and IoT platform developers is advised to test the system under variable network topologies and ensure scalability for urban smart-city ecosystems.

VI. Conclusions

The results of the given research should be taken as strong empirical indicators that the frameworks of PR and intelligent video analytics incorporated in the surveillance systems based on IoT can greatly improve the detection quality and the efficiency of the system operation under the conditions of smart-homes. Using econometric model of 18, 450 device-home-day data obtained as secondary system logs of the Guard-N 4.0 platform, the study quantitatively exhibits that AI-assisted pose recognition is a breakthrough compared to the previous frame-based monitoring model. As shown by the model results, PR-activation has increased verified detections at the cost of false alarms by approximately 32 and 16 percent, respectively (IRR = 1.32; p = 0.001 and 0.84; p = 0.004, respectively). Further, the average latency between edge detection and cloud alert decreased by 0.42 seconds, which proves that the system could be used under real-time constraints on CPU-only edge devices.

Using the Seemingly Unrelated Regression (SUR) system, it was found that these benefits were obtained through a relatively small trade-off of energy consumption (+0.08 J/frame) and bandwidth (+4.9 KB/min), both under sustainable limits of the IoT performance. DiD estimation also support a post-activation of +27% in true detections and -12% in false positives, which proves the causal interplay between the activation of AI and improved system results. In the meantime, the IV method, in which firmware and calibration rollouts are the tools, suggested a stronger impact on the reduction of latency (–0.58 s; $p < 0.001$) which implied that the traditional OLS models slightly underestimate the effect of AI on the latency reduction because of endogenous activation patterns. The threshold model found statistically significant break at a pose-quality index of 0.58 beyond which the benefits of PR are significantly more powerful (true detections +39%, latency -0.47 s).

Combined, these findings prove that the IQ and Action-Ontology system on which the Guard-N system is based is successful in terms of low-level computer vision and high-level semantic reasoning. Using human behavior tokens (e.g., Fall, Raised Hands, Aiming Stance) allows the system to explain AI activities, send less data, and realize quantifiable improvements in efficiency in terms of detection accuracy, speed, and resource consumption. Combining the economics and metrics of engineering can provide a new, interdisciplinary view that pairs system design with quantitative policy analysis and serve as a baseline in future research on the security of the IoT.

Managerial and technological-wise, the paper demonstrates that edge-cloud partitioning can be used to deploy AI in residential settings safely, with privacy guarantees, low-latency, and resources, in mind. The edge-based ability to provide meaningful security intelligence enables the scale of smart-home networks and preconditions their wider application to the public infrastructure, healthcare monitoring, and industrial IoT applications. The quantitative results also emphasize the significance of high pose-quality by proper camera calibration, illumination control, and adaptive learning procedures because these factors directly determine the performance limits of AI-based detection systems.

Although the results confirm strong causal effects and operational efficiency, several opportunities for future research remain. First, forthcoming studies should extend data collection across more diverse environmental conditions and geographic regions, allowing the model to account for cultural and demographic differences in human movement. Second, integrating adaptive machine learning mechanisms could enable continuous recalibration of pose models, mitigating performance loss in low-light or occluded scenarios. Third, future work should explore hybrid AI–econometric frameworks, where real-time inference outcomes feed directly into predictive control and resource-allocation models for network optimization.

Further research should also address human–AI interaction dimensions, particularly examining user trust, privacy perception, and behavioral adaptation in AI-assisted surveillance contexts. Finally, expanding this analytical approach to smart-city and industrial IoT ecosystems could validate the scalability and resilience of the Information-Quanta methodology under higher data volumes and heterogeneous hardware configurations. Such developments will strengthen the theoretical and practical foundation for building ethical, explainable, and energy-efficient AI infrastructures, ensuring that smart surveillance systems contribute positively to both technological innovation and human security.

In summary, this research confirms that AI-driven pose recognition, implemented through an information-centric IoT architecture, delivers measurable improvements in security performance while maintaining operational sustainability. The study's econometric evidence, combined with the authors' engineering achievements, provides a robust pathway for future interdisciplinary exploration and real-world implementation of next-generation intelligent monitoring systems.

Acknowledgments: None.

Conflicts of Interest: The authors declare no conflict of interest.

Patents: None.

VII. REFERENCES

AI City Challenge. AI City Dataset for Video Analytics; NVIDIA and University of Nebraska–Omaha: Omaha, NE, USA, 2025. Available online: https://www.aicitychallenge.org/ (accessed on 15 October 2025).

Alshamsi, O.; Shaalan, K.; Butt, U. Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. Information 2024, 15, 631. https://doi.org/10.3390/info15100631

Dardour, A.; El Haji, E.; Begdouri, M.A. Video Surveillance and Artificial Intelligence for Urban Security in Smart Cities: A Review of a Selection of Empirical Studies from 2018 to 2024. Comput. Sci. Math. Forum 2025, 10, 15. https://doi.org/10.3390/cmsf2025010015

ETSI. Internet of Things and Latency Measurement Framework; European Telecommunications Standards Institute: Sophia Antipolis, France, 2025. Available online: https://www.etsi.org/technologies/internet-of-things (accessed on 15 October 2025).

European Commission, Joint Research Centre (JRC). Smart Grids and IoT Monitoring Data; JRC: Brussels, Belgium, 2025. Available online: https://data.jrc.ec.europa.eu/ (accessed on 15 October 2025).

Ferone, A.; Maratea, A.; Camastra, F.; Ciaramella, A.; Staiano, A.; Lettiero, M.; Polizio, A.; Lombardi, F.; Spoleto, A.J. AiWatch: A Distributed Video Surveillance System Using Artificial Intelligence and Digital Twins Technologies. Technologies 2025, 13, 195. https://doi.org/10.3390/technologies13050195

Gazis, A.; Katsiri, E. Streamline Intelligent Crowd Monitoring with IoT Cloud Computing Middleware. Sensors 2024, 24, 3643. https://doi.org/10.3390/s24113643

Golda, T.; Guaia, D.; Wagner-Hartl, V. Perception of Risks and Usefulness of Smart Video Surveillance Systems. Appl. Sci. 2022, 12, 10435. https://doi.org/10.3390/app122010435

Honarparvar, S.; Saeedi, S.; Liang, S.; Squires, J. Design and Development of an Internet of Smart Cameras Solution for Complex Event Detection in COVID-19 Risk Behaviour Recognition. ISPRS Int. J. Geo-Inf. 2021, 10, 81. https://doi.org/10.3390/ijgi10020081

IEEE DataPort. Human Action Recognition and IoT Performance Datasets; IEEE: New York, NY, USA, 2025. Available online: https://ieee-dataport.org (accessed on 15 October 2025).

Intel Corporation. DevMesh IoT Edge Analytics Performance Logs; Intel Corporation: Santa Clara, CA, USA, 2025. Available online: https://devmesh.intel.com/ (accessed on 15 October 2025).

Kaggle. Human Activity Recognition and Pose Estimation Collections; Google LLC: Mountain View, CA, USA, 2025. Available online: https://www.kaggle.com (accessed on 15 October 2025).

Koldovskiy, A. A Transdisciplinary Approach to Improving the Quality of the Scientific and Educational Process in the Context of Digital Transformation. In Proceedings of the 6th International Scientific and Practical Web Forum: Building a Unified Open Information Space for Lifelong Education, Kyiv–Kharkiv, Ukraine, 2024a.

Koldovskiy, A. Strategic Infrastructure Transformation: Revolutionizing Financial Sector Management for Enhanced Success. Acta Academiae Beregsasiensis. Economics 2024b, 5, 323–332. https://doi.org/10.58423/2786-6742/2024-5-323-332.

Kulbacki, M.; Segen, J.; Chaczko, Z.; Rozenblit, J.W.; Kulbacki, M.; Klempous, R.; Wojciechowski, K. Intelligent Video Analytics for Human Action Recognition: The State of Knowledge. Sensors 2023, 23, 4258. https://doi.org/10.3390/s23094258

Lu, Y.; Zhou, L.; Zhang, A.; Zha, S.; Zhuo, X.; Ge, S. Application of Deep Learning and Intelligent Sensing Analysis in Smart Home. Sensors 2024, 24, 953. https://doi.org/10.3390/s24030953

NIST. Smart Home Testbed Dataset; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025. Available online: https://www.nist.gov/el/smart-home (accessed on 15 October 2025).

NREL. Residential Energy Consumption Data Center; National Renewable Energy Laboratory: Golden, CO, USA, 2025. Available online: https://data.nrel.gov/ (accessed on 15 October 2025).

OpenCV Foundation. OpenCV Zoo Benchmark and Calibration Data; OpenCV Foundation: Redwood City, CA, USA, 2025. Available online: https://opencv.org/opencv-zoo/ (accessed on 15 October 2025).

Prokopenko, O.; Chechel, A.; Koldovskiy, A.; Kldiashvili, M. Innovative Models of Green Entrepreneurship: Social Impact on Sustainable Development of Local Economies. Economics Ecology Socium 2024, 8, 89–111. https://doi.org/10.61954/2616-7107/2024.8.1-8.

Prokopenko, O.; Ivliieva, O.; Korshevniuk, T.; Koldovskiy, A.; Shostak, I. The Role of Digital Technologies in Ensuring the Inclusivity of Distance Education. Rev. Conrado 2025, 20(103), e4431. https://lib.iitta.gov.ua/id/eprint/745198/1/%D0%A1%D1%82%D0%B0%D1%82%D1%82%D1%8F%20WoS.pdf

Rahim, A.; Zhong, Y.; Ahmad, T.; Ahmad, S.; Pławiak, P.; Hammad, M. Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models. Sensors 2023, 23, 6979. https://doi.org/10.3390/s23156979

Ravindran, A. A. Edge Computing Systems for Streaming Video Analytics : Trail Behind and the Paths Ahead. Preprints 2023, 2023080383. https://doi.org/10.20944/preprints202308.0383.v1

Sabit, H. Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. Electronics 2025, 14, 608. https://doi.org/10.3390/electronics14030608

Shalan, M.; Hasan, M.R.; Bai, Y.; Li, J. Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection. Smart Cities 2025, 8, 35. https://doi.org/10.3390/smartcities8010035

Torres-Hernandez, C.M.; Garduño-Aparicio, M.; Rodriguez-Resendiz, J. Smart Homes: A Meta-Study on Sense of Security and Home Automation. Technologies 2025, 13, 320. https://doi.org/10.3390/technologies13080320

Torres-Hernandez, C.M.; Garduño-Aparicio, M.; Rodriguez-Resendiz, J. Smart Homes: A Meta-Study on Sense of Security and Home Automation. Technologies 2025, 13, 320. https://doi.org/10.3390/technologies13080320

UCI Machine Learning Repository. Smart Home Dataset; University of California, Irvine: Irvine, CA, USA, 2025. Available online: https://archive.ics.uci.edu/ml/index.php (accessed on 15 October 2025).

Vardakis, G.; Hatzivasilis, G.; Koutsaki, E.; Papadakis, N. Review of Smart-Home Security Using the Internet of Things. Electronics 2024, 13, 3343. https://doi.org/10.3390/electronics13163343

Yin, H., Sinnott, R.O. & Jayaputera, G.T. A survey of video-based human action recognition in team sports. Artif Intell Rev 57, 293 2024. https://doi.org/10.1007/s10462-024-10934-9