A Hybrid AI–Fuzzy Logic Framework for Infrared Imaging–Based Intrusion Detection in Power Transmission Systems

Mazadu Abdullahi Adamu[1] and Umar Abubakr Saleh[1]

[1]Department of Electrical and Electronic Engineering, Federal Polytechnic N'yak, Shendam
*Corresponding author: ***abubakarumarsaleh1982@gmail.com***

Abstract: This paper presents a hybrid artificial intelligence (AI) and fuzzy logic framework for infrared (IR) intrusion monitoring in power transmission environments. To address low visibility, background clutter, and ambiguous target appearance, the proposed pipeline integrates IR frame preprocessing, YOLO-based person detection, and a Mamdani-type fuzzy inference system that produces an interpretable frame-level threat score. Detected regions of interest are converted into normalized threat descriptors capturing intrusion magnitude (bounding-box area), proximity, and thermal evidence computed from the IR data within the detection window. These descriptors drive the fuzzy decision layer, which maps heterogeneous spatial and thermal cues into a continuous threat score suitable for operator decision support. A Simulink realization is included to demonstrate real-time deployability of the fuzzy module, while MATLAB–Simulink agreement is reported strictly as implementation verification. Experimental evaluation is conducted on an independently labeled subset of 80 IR frames annotated in Robo flow, where the positive class corresponds to frames containing a visible human intruder. Detection performance is summarized using precision, recall, F1-score, and a confusion matrix, and the resulting threat-score trajectory is visualized to illustrate coherent risk variation during intrusion periods. Additionally, the results demonstrate the functional integration, internal analytical consistency, and interpretability of the proposed architecture, establishing a scalable foundation for future model training, quantitative performance evaluation, and deployment-oriented optimization.

Keywords: Power line security, infrared imaging, YOLO, fuzzy logic, hybrid AI–fuzzy framework, intrusion monitoring, Simulink.

NJST Preprint

1. Introduction

Power transmission corridors are vulnerable to intrusion events such as unauthorized access, vandalism, theft, and accidental encroachment (Zhou et al., 2023). Conventional surveillance approaches relying on visible spectrum cameras, patrols, or basic motion sensing often degrade under low illumination, adverse weather, background clutter, and long monitoring distances (Chen & Li, 2024). Infrared (IR) imaging improves visibility by capturing thermal contrast, but effective protection still requires automated detection and a decision layer that can translate detections into actionable threat assessments.

Deep learning-based object detectors, particularly YOLO variants, have demonstrated strong performance in real time detection across challenging scenes (Wang et al., 2024). However, detector outputs typically provide bounding boxes and confidence scores, which may be insufficient for operator decision support in safety critical environments because they do not explicitly encode threat severity or uncertainty. Fuzzy logic provides interpretable rule-based reasoning and is effective for handling

ambiguity in security decision systems where inputs can be noisy or incomplete (Sharma & Kumar, 2023). A hybrid AI and fuzzy approach is therefore well suited to power infrastructure protection, where both detection performance and decision transparency are important for operational use (Okoro et al., 2024).

This paper proposes a hybrid AI–fuzzy framework for real time intrusion monitoring using IR imagery. The framework integrates IR preprocessing, YOLO based intruder localization, threat feature construction, and a Mamdani type fuzzy inference system that produces an interpretable frame level threat score. Importantly, the fuzzy inputs are derived from detection regions of interest and include intrusion magnitude, proximity, and empirical thermal evidence extracted from the IR data, enabling the decision layer to fuse spatial and thermal cues rather than relying on a distance derived thermal proxy. The framework is evaluated on labeled IR frames using standard metrics, with detection precision, recall, and F1 score reported in Table X and threat level assignment assessed using a confusion matrix in Table Y. Figure X provides representative infrared frames with YOLO detections used in the evaluation. A Simulink realization is included to demonstrate real time deployability of the fuzzy decision layer, while MATLAB and Simulink agreement is reported only as implementation verification.

2. Main contributions

The main contributions of this paper are as follows:

1. A modular hybrid architecture that integrates IR preprocessing, YOLO based intrusion detection, and fuzzy threat inference through a well-defined feature interface suitable for real time deployment.
2. A threat feature construction strategy that converts detection outputs into normalized descriptors capturing intrusion magnitude, proximity, and thermal evidence computed from the infrared ROI, enabling complementary fusion of spatial and thermal cues.
3. A Mamdani type fuzzy inference system that maps the engineered descriptors to a continuous threat score and interpretable linguistic threat levels, supporting transparent operator decision making.
4. An experimental evaluation on labeled IR frames reporting standard detection metrics, precision, recall, and F1 score, and threat level assignment performance using a confusion matrix, alongside a Simulink implementation to support real time execution.

3. System Design

This section presents the hybrid AI–fuzzy framework developed to integrate infrared image processing, deep learning–based intrusion detection, and fuzzy logic inference for intelligent surveillance and real-time decision-making in power infrastructure security. Infrared (IR) surveillance footage from a power line corridor or similar outdoor environment is used as the primary visual

NJT Preprint

input. A Python-based pre-processing script reads the IR video, decodes and samples frames, resizes them to the required network resolution, and stores them as sequential images suitable for deep learning analysis. Infrared imaging is particularly effective for low-light and night-time detection, as evidenced by recent studies on thermal and multispectral imaging (Deng et al., 2024; You et al., 2022; Zhang, 2022).

Figure 1 illustrates the overall hybrid AI–fuzzy architecture, detailing the progression from IR image acquisition through YOLO-based detection, threat-oriented feature engineering, and fuzzy threat inference to final threat-level output. The framework is structured as a four-stage pipeline:

1. Infrared (IR) frame acquisition and pre-processing

   At a high level, the framework can be expressed as a composition of three mappings: deep learning–based detection, feature construction, and fuzzy inference.

   Equation $k_x \in \mathrm{R}^{\mathrm{H\times W\times C}}$:infrared frame at time/frame index k

$D_k = f_{YOLO}(x_k)$: set of detections for frame k,

$$\boldsymbol{\phi_K} = (\mathbf{D_K}) = \begin{bmatrix} \mathbf{threat_size_k} \\ \mathbf{threat_distance_k} \\ \mathbf{threat_temp_k} \end{bmatrix} \in [\mathbf{0}, \mathbf{1}]^{\mathbf{3}} \quad (1)$$

$y_k = f_{FIS}(\Phi_K) \in [0,1]$: fuzzy threat level.

   Equation (1) shows the end-to-end mapping from infrared frame $x_k$through deep learning detectionsD_k, normalized feature vector ϕ_k, and fuzzy inference to the scalar threat levely_k.

2. YOLO-based intrusion detection
3. Threat-oriented feature construction and normalization
4. Fuzzy logic–based threat-level estimation and Simulink implementation

At a high level, the end-to-end data flow can be expressed as:

NST Preprint



Figure 1: Overall hybrid AI–fuzzy framework for infrared intrusion monitoring in power line corridors.

The system integrates infrared (IR) frame acquisition and pre-processing, YOLO-based deep learning intrusion detection, MATLAB-based threat-oriented feature construction, and a Mamdani-type fuzzy inference system (FIS) implemented in MATLAB/Simulink to generate a frame-wise threat level.

This modular structure decouples the deep learning detector from the fuzzy decision layer while preserving a clear, reproducible interface based on CSV tables and time-series signals.

3.1 Infrared Pre-Processing and YOLO Detection

Infrared surveillance footage representing a power line corridor or similar outdoor environment is used as the primary visual input. A Python-based pre-processing script reads the IR video and:

- **Decodes and samples frames** at a fixed rate suitable for near-real-time monitoring.
- **Resizes** each frame to the spatial resolution required by the YOLO network (e.g., 640×640 pixels).
- **Formats and saves** frames as image files (e.g., PNG/JPEG) with sequential names (000001.jpg, 000002.jpg …), preserving their temporal order. Figure 3.1 shows representative infrared frames with YOLO person detections that define the regions of interest used for downstream threat feature extraction.

Each pre-processed frame $x_k \in \mathrm{R}^{\mathbf{H}\times\mathbf{W}\times\mathbf{C}}$ is passed into a YOLO-style detector (e.g., via detect_yolo_cpu.py). A pre-trained YOLOv5 model is initially used to validate the workflow due to its favorable balance between accuracy and speed (Khanam & Hussain, 2024), but this is replaceable with a model trained on infrared intrusion imagery.

For each frame k, the detector returns a set of N_k candidate detections formalized as:

$$\mathbf{D_K} = \left\{(\boldsymbol{b_k^i}, \boldsymbol{c_k^{(i)}}, \boldsymbol{l_k^{(i)}})\right\}_{\boldsymbol{i}}^{\boldsymbol{N_k}}, \tag{2}$$

Where each bounding box b_k^i is defined by its pixel coordinates and dimensions:

$$\boldsymbol{b_k^i} = (\boldsymbol{u_k^{(i)}}, \boldsymbol{v_k^{(i)}}, \boldsymbol{w_k^{(i)}}, \boldsymbol{h_k^{(i)}}) \tag{3}$$

NIST Preprint

The area of the i-th detection is computed as:

$$A_k^i = w_k^{(i)}, h_k^{(i)} \quad (4)$$

And the largest detected bounding box per frame—used later as a proxy for threat size—is:

$$A_k^{max} = \underbrace{\max}_{1 \le i \le N_k} A_k^i. \quad (5)$$

The detector also provides a frame-level confidence score:

$$c_k^{max} = \underbrace{\max}_{1 \le i \le N_k} c_k^i. \quad (6)$$

and human-intruder count is defined by:

$$N_k^{\text{person}} = \left|\left\{i : l_k^{(i)} = \text{“person”}\right\}\right| \quad (7)$$

These structured detection statistics are stored in yolo_outputs.csv, with one row per frame containing:

- filename – identifier of the processed frame
- confidence – c_k^{max}
- max_bbox_area – A_k^{max}
- cnt_persons – N_k^{person}
- proximity_est_m, mean_temp – optional geometric/thermal indicators derived from IR characteristics

This file forms the interface between the Python inference layer and the MATLAB-based feature engineering and fuzzy inference stages.

3.2 Threat Feature Construction and Normalization

The fuzzy inference system does not operate directly on raw YOLO detections. Instead, the detections are transformed into higher-level, normalized descriptors that encode threat-relevant information. This transformation is performed in MATLAB via the script process_yolo_data.m. Figure 2 shows the Simulink implementation of the fuzzy threat inference system.

NST Preprint



Figure 2: YOLO person detections on infrared frames.

To begin, simple logical indicators are derived from YOLO outputs. Using the detected person count N_k^{person}

$$\boldsymbol{has_person_k} = \begin{cases} \mathbf{1}, & \boldsymbol{N_k^{\text{person}}} > \mathbf{0} \\ \mathbf{0} & \boldsymbol{N_k^{\text{person}}} = \mathbf{0} \end{cases} \quad (8)$$

and

$$\mathbf{any_detection_k} = \mathbf{has_person_k} \quad (9)$$

These binary flags distinguish intrusion frames from background frames.

Next, three continuous descriptors in the interval [0,1] are constructed to represent threat magnitude, proximity, and thermal intensity.

- **Threat size (threat_size)**

  Threat size encodes the perceived "magnitude" of the intrusion. It is derived from the maximum bounding-box area A_k^{max} (defined earlier in Equation 5) via min–max normalization:

$$\text{threat_size}_k = \frac{A_k^{max} - A_{min}}{A_{max} - A_{min}}, \quad \textbf{(10)}$$

with the final value clipped to [0,1]. Frames with human intruders therefore yield values in a high range (e.g., 0.75–1.000), while empty frames map to very small values (e.g., 0.00–0.050).

NIST Prep

Threat distance (threat_distance)

Because threat_distance is derived from bounding-box geometry, it is expected to be correlated with threat_size; both are retained to preserve explicit proximity semantics in the fuzzy rule base, while thermal evidence is measured independently from infrared ROI intensity (Section 3.2).

In this study, the proximity proxy is defined from the maximum detected bounding-box area as:

$$\widetilde{d_k} = \frac{1}{\sqrt{A_k^{max} + \epsilon}} \tag{11a}$$

where A_k^{max} is the maximum person bounding-box area in frame k (Eq. 5) and $\epsilon>0$prevents division by zero. The proxy is then min–max normalized to the unit interval:

$$\mathbf{threat_distance}_k = \frac{\widetilde{d_k} - \widetilde{d_{min}}}{\widetilde{d_{max}} - \widetilde{d_{min}}} \tag{11b}$$

Lower values indicate nearer intruders (larger bounding boxes), whereas background or far-distance cases yield higher values corresponding to distant or empty scenes.

- **Threat temperature (threat_temp)**

To ensure the temperature-related descriptor reflects measured infrared evidence, thermal evidence is computed directly from the infrared frame. For each detected person in frame k, the region of interest Ω_k is defined by the YOLO bounding box. The mean infrared pixel intensity within the ROI is computed as

$$T_k = \frac{\mathbf{1}}{|\boldsymbol{\Omega_k}|} \sum_{(\boldsymbol{u},\boldsymbol{v})\in\boldsymbol{\Omega_k}} \boldsymbol{I_k}(\boldsymbol{v},\boldsymbol{u}) \tag{12a}$$

where $\boldsymbol{I_k}(u, v)$ denotes the infrared intensity at pixel location (u, v). The resulting value is min max normalized to obtain a unit interval descriptor

$$\text{threat_temp}_{\boldsymbol{k}} = \frac{\boldsymbol{T_k} - \boldsymbol{T_{min}}}{\boldsymbol{T_{max}} - \boldsymbol{T_{min}}} \tag{12b}$$

with values clipped to [0,1]. Background frames without a detected person are assigned $\text{threat_temp}_{\boldsymbol{k}} = 0$.

The resulting per-frame descriptors $\text{threat_size}_{\boldsymbol{k}}$, $\text{threat_distance}_{\boldsymbol{k}}$ and $\text{threat_temp}_{\boldsymbol{k}}$ form the input vector to the fuzzy inference system. Because thermal evidence is extracted directly from infrared ROI intensity, $\text{threat_temp}_{\boldsymbol{k}}$ is not deterministically implied by the distance proxy, reducing redundancy and supporting complementary fusion of spatial and thermal cues.

NST Preprint

3.3 Fuzzy Threat Inference System

The decision layer is implemented using a Mamdani-type fuzzy inference system (FIS) constructed in MATLAB's Fuzzy Logic Toolbox and stored as threat_detection.fis. The FIS maps three normalized descriptors into a single threat-level output.

The input variables are:

x_1 =Threat Size ∈ $[0,1]$, x_2 =Threat Distance ∈ [0,1], Threat Temperature ∈ [0,1] (13)

and the output is:

where x_3 is computed from the mean infrared ROI intensity within the YOLO bounding box and then normalized to [0,1] as described in Section 3.2. This ensures that the temperature descriptor is derived from measured infrared evidence and is not a deterministic function of the distance proxy, reducing redundancy in the fuzzy input space.

y =Threat Level ∈ [0,1], (14)

where values near 1 represent high perceived threat.

Each input is described by a small number of linguistic terms (e.g., {Small, Medium, Large} for size; {Near, Medium, Far} for distance; {Cool, Warm, Hot} for temperature), with triangular and trapezoidal membership functions μ (·) defined over the unit interval.

Mamdani Rule Base

The rule base specifies expert surveillance logic. A typical rule takes the form:

R_m:IF x_1 isA_m, x_2 is B_m, x_3 is C_m THEN y is D_m, (15)

A_m, B_m, C_m, D_m are linguistic labels. The complete rule base used in this study is summarized in Table 1

Table 1: Fuzzy Rule Base for Infrared Intrusion Threat Assessment

Rule	Threat Size	Threat Distance	Threat Temperature	Threat Level
R1	Small	Far	Low	Low
R2	Small	Far	Medium	Low
R3	Small	Far	High	Low
R4	Small	Medium	Low	Low
R5	Small	Medium	Medium	Medium

NIST Preprint

R6	Small	Medium	High	Medium
R7	Small	Near	Low	Medium
R8	Small	Near	Medium	Medium
R9	Small	Near	High	High
R10	Medium	Far	Low	Low
R11	Medium	Far	Medium	Low
R12	Medium	Far	High	Medium
R13	Medium	Medium	Low	Medium
R14	Medium	Medium	Medium	Medium
R15	Medium	Medium	High	High
R16	Medium	Near	Low	Medium
R17	Medium	Near	Medium	High
R18	Medium	Near	High	High
R19	Large	Far	Low	Medium
R20	Large	Far	Medium	Medium
R21	Large	Far	High	High
R22	Large	Medium	Low	Medium
R23	Large	Medium	Medium	High
R24	Large	Medium	High	High
R25	Large	Near	Low	High
R26	Large	Near	Medium	High
R27	Large	Near	High	High

For an input triple (x_1, x_2, x_3), the firing strength of rule mmm is computed using the standard Mamdani min operator:

$$\boldsymbol{\alpha_m(x_1, x_2, x_3), = \min\ (\mu A_m(x_1), \mu B_m(x_2), \mu C_m(x_3)\ ).} \quad (16)$$

The aggregated fuzzy output set is produced by **max** composition over all fired rules:

$$\mu_Y(y]x_1, x_2, x_3) = \underbrace{max}_{m} \min\ (\alpha_m(x_1, x_2, x_3),\ \mu D_m(y)). \quad (17)$$

Finally, a crisp threat level is obtained using centroid defuzzification:

$$y^* = \frac{\int_0^1 y\mu_Y(y]x_1,x_2,x_3)dy}{\int_0^1 \mu_Y(y]x_1,x_2,x_3)dy}. \quad (18)$$

This mapping defines the complete fuzzy transformation from the three input descriptors to a single risk-level output.

Figure shows the Simulink implementation. The three pre-processed features (x_1, x_2, x_3), are concatenated with a Mux

NJST Preprint

block and fed into a Fuzzy Logic Controller block configured with threat_detection.fis.

The output threat level y^* is visualized via a Scope and stored in the workspace as out.threat_level_sim.

Min–max composition and centroid defuzzification (Equations 17–18) ensure a smooth and interpretable threat-surface.

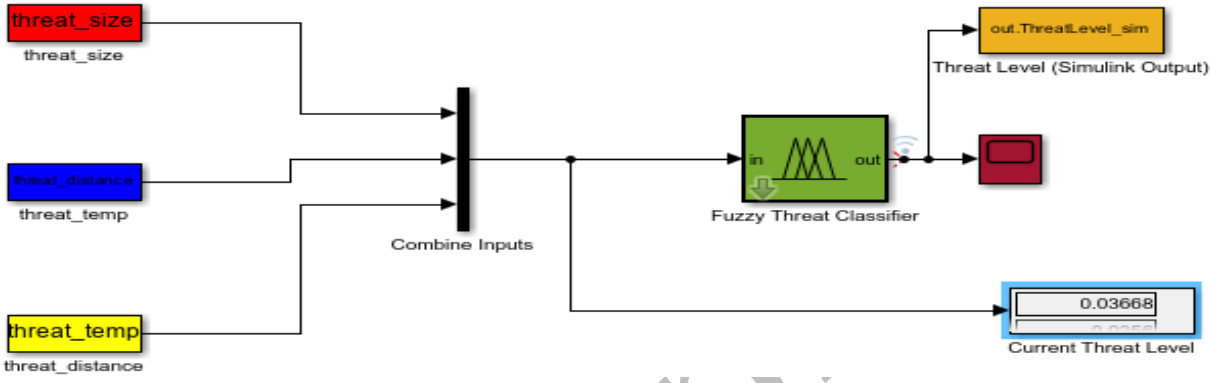

Figure 3: Simulink implementation of the fuzzy threat inference system

To further examine the internal behaviour of the fuzzy threat-classification layer, the Mamdani inference system was evaluated over a two-dimensional grid of input values while holding thermal intensity at a fixed medium level. This evaluation produces a continuous threat-surface representation that visualizes how the system interpolates threat levels across combinations of object size and distance. Such qualitative analysis is essential for verifying that the designed rule base produces coherent and interpretable behaviour across the entire domain of possible detections.

The resulting 3-D surface plot (Figure 4) reveals smooth and monotonic trends consistent with the intended decision policy for power-line surveillance. Threat level increases whenever detected objects become larger or approach the camera, while remaining minimal for small or distant thermal signatures. This confirms that the fuzzy system encodes the expected operational logic and behaves consistently across the full input range, even in the absence of explicit training data.

NJST Prep

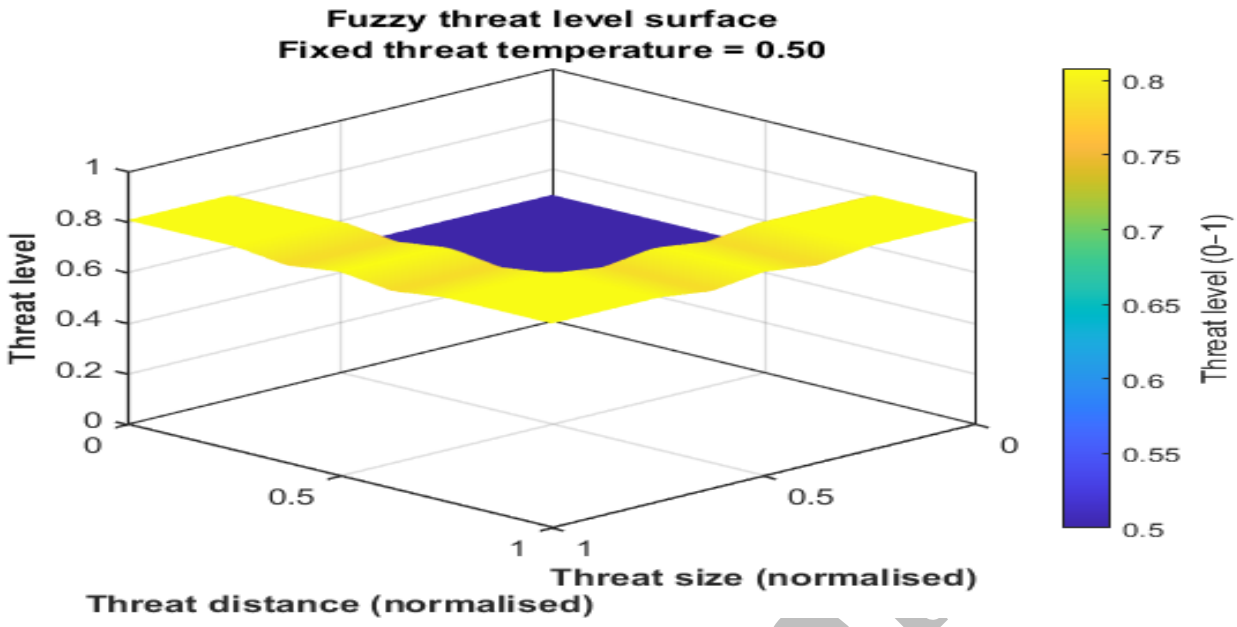

Figure 4: Fuzzy threat-level surface for a fixed mid-level thermal condition (temperature = 0.50)

3.3.1 Membership Functions

Each input and the output of the Mamdani fuzzy inference system (FIS) is partitioned into three linguistic terms defined over the normalized interval [0,1]. Threat size is described by $\{\boldsymbol{Low}, \boldsymbol{Medium}, \boldsymbol{High}\}$, threat distance by $\{\boldsymbol{Near}, \boldsymbol{Medium}, \boldsymbol{Far}\}$, and the temperature proxy by $\{\boldsymbol{Low}, \boldsymbol{Medium}, \boldsymbol{High}\}$. The output variable, threat level, is similarly defined by $\{\boldsymbol{Low}, \boldsymbol{Medium}, \boldsymbol{High}\}$. Triangular and trapezoidal membership functions are used to ensure smooth transitions between adjacent linguistic regions and robust behaviour near category boundaries.

Figure 5 summarizes the membership functions used for all three inputs and the threat-level output. These partitions act as model-configuration parameters that operationalize expert semantics (e.g., “near” versus “far” and “low” versus “high” threat) and provide the interpretability required for rule-based surveillance decision support.

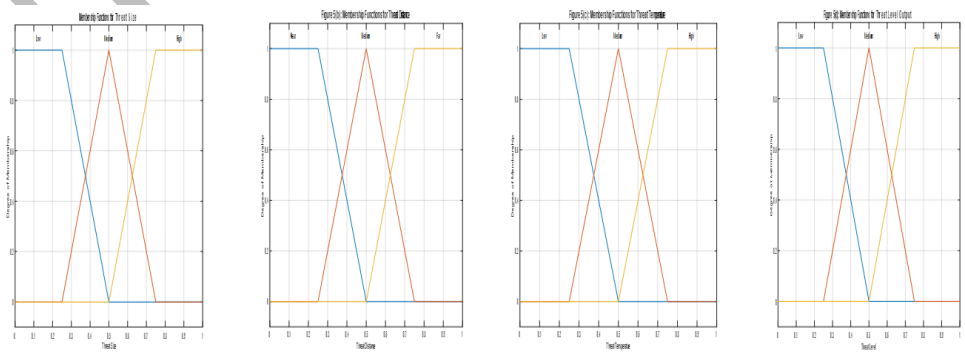

Figure 5: Membership functions for the fuzzy inference system: (a) threat size, (b) threat distance, (c) thermal evidence (ROI mean infrared intensity, and (d) threat level output.

NJST Preprint

3.4 Simulink Based Realization

The three pre processed features (x_1, x_2, x_3) are concatenated using a Mux block and supplied to a Fuzzy Logic Controller block configured with threat_detection.fis. The output threat level y∗ is visualized via a Scope and logged to the workspace as out.threat_level_sim as shown in Figure 2.

This Simulink realization is included to demonstrate deployability of the fuzzy decision layer within a real time monitoring pipeline. To verify correctness of the implementation, the Simulink output is compared against the MATLAB reference evaluation (*evalfis*) under identical inputs. The resulting trajectories are numerically consistent, confirming that the Simulink block realizes the designed fuzzy mapping. This comparison is reported as implementation verification and is not treated as primary performance evidence.

Min max composition and centroid defuzzification are implemented internally by the fuzzy controller consistent with Equations (17) and (18), enabling smooth and interpretable threat score variation over time.

4. Experimental Evaluation

This section reports experimental evaluation results for the proposed hybrid AI–fuzzy pipeline. In addition to demonstrating real-time system integration, we quantify intruder detection using standard metrics (precision, recall, and F1) on a labeled subset of infrared frames and summarize outcomes using a confusion matrix. We also visualize the resulting fuzzy threat score trajectory over time to illustrate how detections are converted into an interpretable risk signal. MATLAB–Simulink consistency checks are presented as implementation verification rather than performance evidence.

4.0 Intruder Detection Performance

Intruder detection performance is quantified on the labeled subset using standard binary-classification metrics. Table 2 reports precision, recall, F1-score, and accuracy for person-presence detection, where the positive class corresponds to frames containing a human intruder. Figure 6 summarizes the corresponding confusion matrix, indicating the distribution of true positives, true negatives, false positives, and false negatives. Figure 7 provides a compact visualization of precision, recall, and F1-score for the same evaluation.

Table 2: Intruder detection metrics on the labeled subset.

Precision	Recall	F1-score	Accuracy
1.000	1.000	1.000	1.000

NJT Preprint

Although all metrics are unity on this 80-frame subset, this result should be interpreted in the context of the limited sample size; larger independently annotated evaluations are reserved for future work.

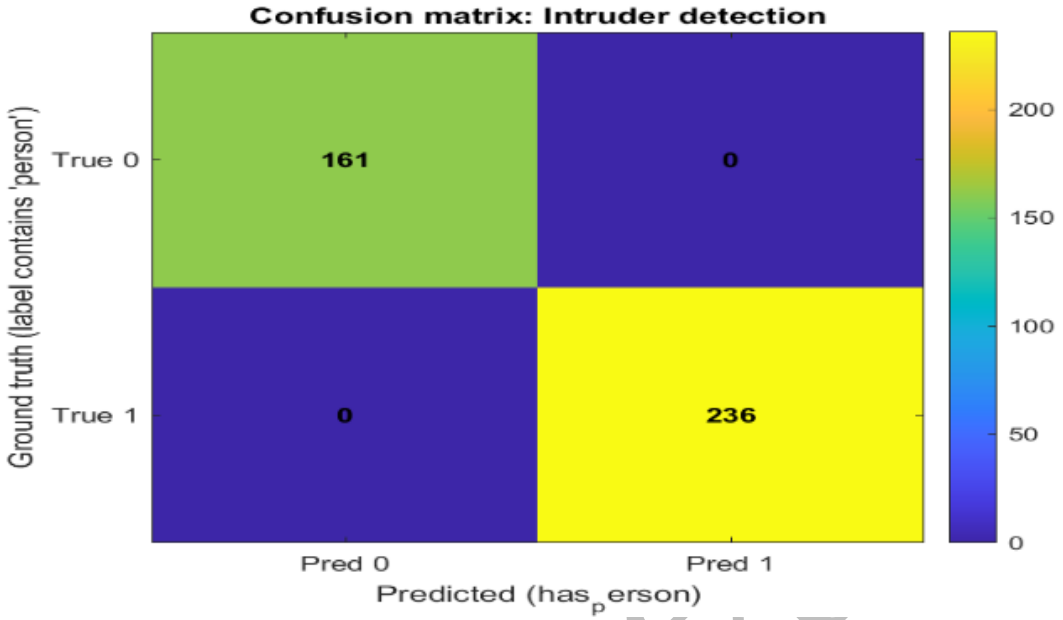

Figure 6: Confusion matrix for intruder (person) presence detection on the labeled subset.

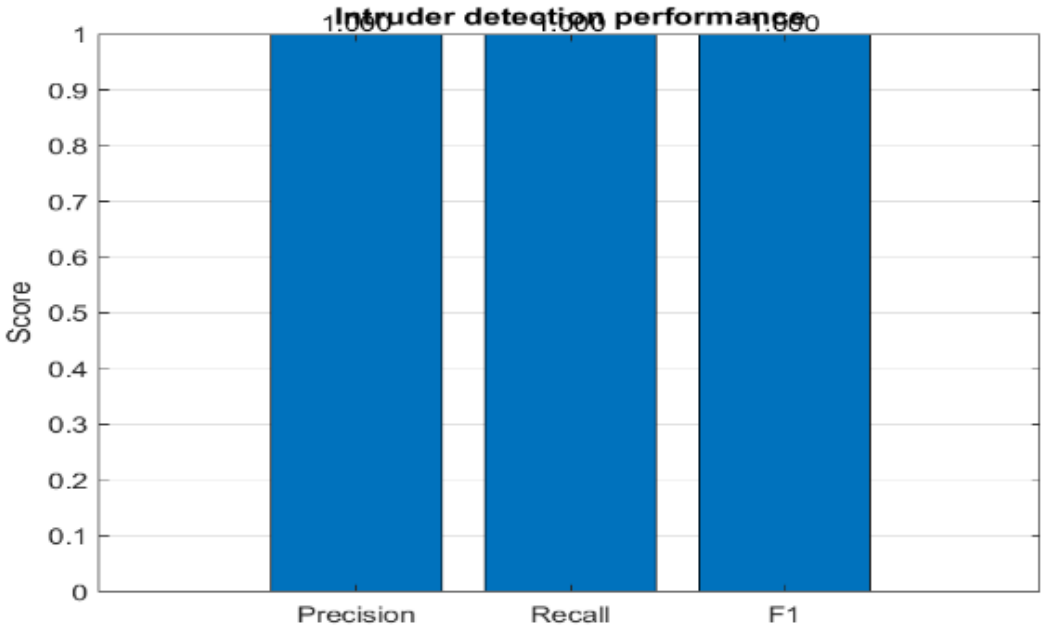

Figure 7: Intruder detection precision, recall, and F1-score on the labeled subset.

To relate detection outcomes to downstream decision support, Figure 8 presents the fuzzy threat score trajectory $y*$ over time, overlaid with the intrusion label. This plot illustrates

how the fuzzy inference layer converts frame-level detections into a continuous, interpretable threat signal that rises during intrusion periods and returns toward baseline when the scene is clear.

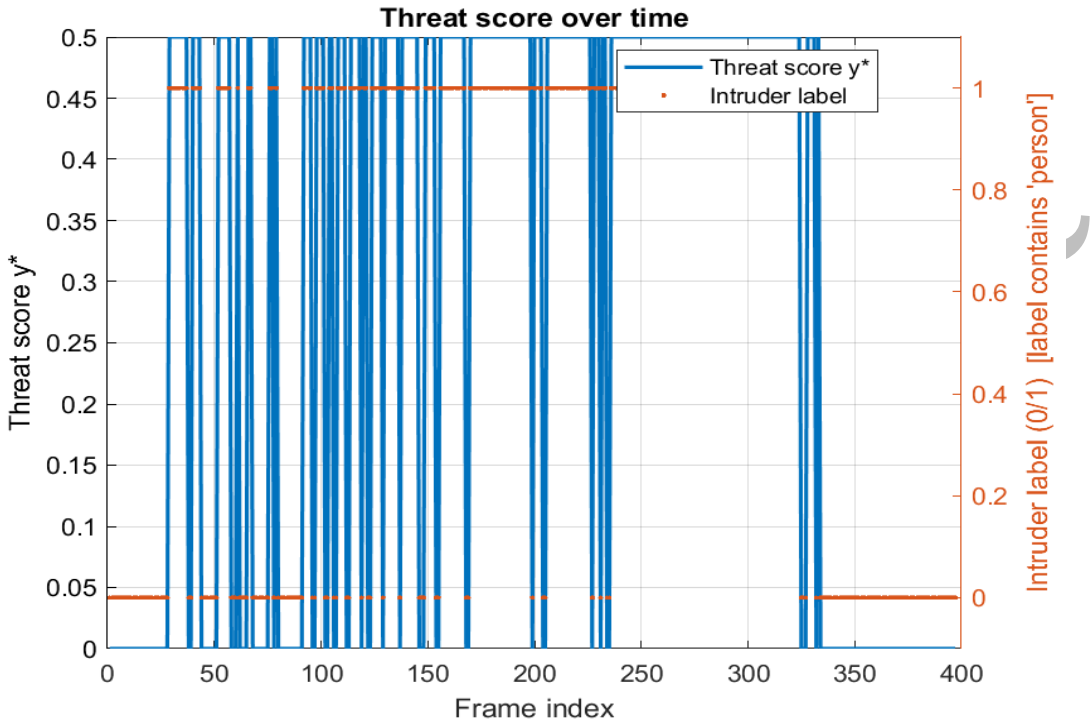

Figure 8: Fuzzy threat score trajectory **y∗** over time with intrusion label overlay.

4.1 Evaluation Protocol

Evaluation was conducted on an independently annotated subset of 80 infrared frames sampled from the study data. Ground-truth person-presence labels were produced by manual annotation in Roboflow using a single binary criterion ("person visible in frame" = 1; otherwise = 0). These labels were created independently of the YOLO detector outputs and were used only for evaluation (no tuning or threshold selection was performed on this subset). Predictions were obtained from the YOLO per-frame person-presence flag (has_person), and precision, recall, F1-score, and accuracy were computed from the standard confusion-matrix formulation.

4.2 Fuzzy Threat Surface and Example Time Series

To gain insight into the qualitative behaviour of the fuzzy decision layer, the FIS was evaluated over a grid of input values and plotted as a 3-D surface (Figure 2b). With threat temperature fixed at a mid-level, the surface shows that the estimated threat level increases monotonically with both threat size and proximity, while remaining low for small, distant objects. This behavior matches the intended security logic for power line corridors, where larger and closer intruders should be prioritized

Temporal behaviour is illustrated using the fuzzy threat score trajectory y∗ generated by running the complete pipeline on an infrared

sequence containing intermittent intrusions (Figure 4.3). During non-intrusion intervals, the threat score remains near baseline; when a person is detected and approaches the camera, the score increases accordingly and returns toward baseline after the intruder exits the scene. The threat surface and time-series plots indicate that the fuzzy inference stage yields a continuous, interpretable threat signal consistent with the designed rule base.

4.3 Distribution of Threat Features

To characterize the engineered descriptors used as inputs to the fuzzy inference system (FIS), the distributions of threat size, threat distance, and thermal evidence were analyzed across the processed infrared frames. Figure 3 presents histogram–density overlays for each descriptor, enabling inspection of feature scaling and separation between intrusion and non-intrusion conditions.

The threat-size distribution (Figure 9a) exhibits a distinct bimodal pattern. A dense cluster of values near zero corresponds to frames without detected intruders, while a separate cluster at high values (approximately 0.75–1.0) corresponds to frames where a person is detected. This structure indicates that the size metric provides a separable indicator of intrusion magnitude and is well suited for fuzzification into linguistic terms such as *Small*, *Medium*, and *Large*.

A similar pattern is observed in the threat-distance distribution (Figure 9b). Intruder-present frames accumulate at the lower end of the scale (0.15–0.35), indicating closer proximity, whereas non-intrusion frames dominate the higher range (0.75–0.95). This separation indicates that the distance descriptor captures relative closeness consistently and supports fuzzy categories such as *Near*, *Medium*, and *Far*.

The threat-temperature distribution (Figure 9c) reflects the thermal evidence extracted from the infrared frames. In this study, the temperature term is computed as the mean infrared intensity within the detected person region of interest (ROI) and then normalized to [0,1][0,1][0,1]. Accordingly, higher values correspond to detections with stronger thermal contrast, while lower values are associated with background or weak/absent thermal signatures. This formulation provides radiometric information that complements the geometric descriptors (size and distance) and avoids deterministic dependence on the proximity proxy.

NJST Preprint

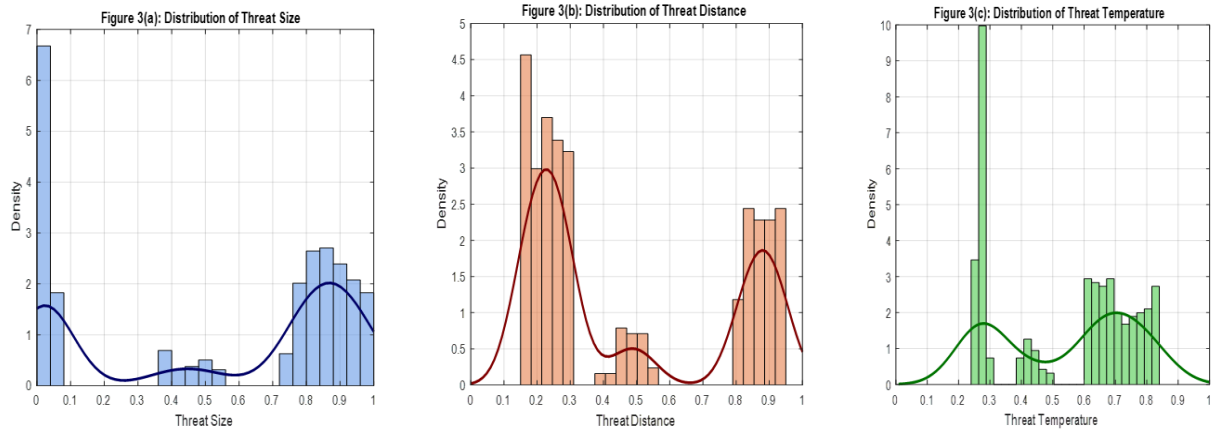

Figure 9: Distributions of the engineered fuzzy-input descriptors across processed infrared frames: **(a)** normalized threat size (from bounding-box area), **(b)** normalized threat distance, and **(c)** normalized thermal evidence computed as the mean infrared ROI intensity within the detected bounding box.

Overall, the distributions indicate stable scaling and interpretable separation for threat size and threat distance, while the thermal evidence term provides an additional radiometric cue derived directly from infrared pixel values. These properties support the suitability of the engineered descriptors for rule-based fuzzy threat scoring.

4.4 Correlation of Threat Features

The correlation structure of the engineered descriptors (threat size, threat distance, and threat temperature) was examined to assess interdependence and potential redundancy within the feature space. Figure 10 presents the resulting correlation heatmap computed over the processed infrared frames.

A strong negative correlation is observed between threat distance and threat size. This relationship is expected because the distance term is defined as a proximity proxy derived from bounding-box area: nearer targets typically occupy larger image regions, producing higher normalized size values and lower normalized distance values. Threat temperature also shows correlation with distance, reflecting the fact that nearer human targets often appear thermally stronger in infrared imagery; however, in this study the temperature term is computed from measured ROI intensity rather than being deterministically derived from the distance proxy.

Accordingly, correlations involving threat temperature should be interpreted as physically plausible co-variation (proximity and radiometric contrast) rather than as a construction artifact. Taken together, the correlation matrix confirms that (i) the geometric descriptors (size and distance) behave consistently with perspective effects, and (ii) the thermal descriptor provides complementary radiometric information that can reinforce threat scoring when targets are both close and thermally salient.

NST Preprint

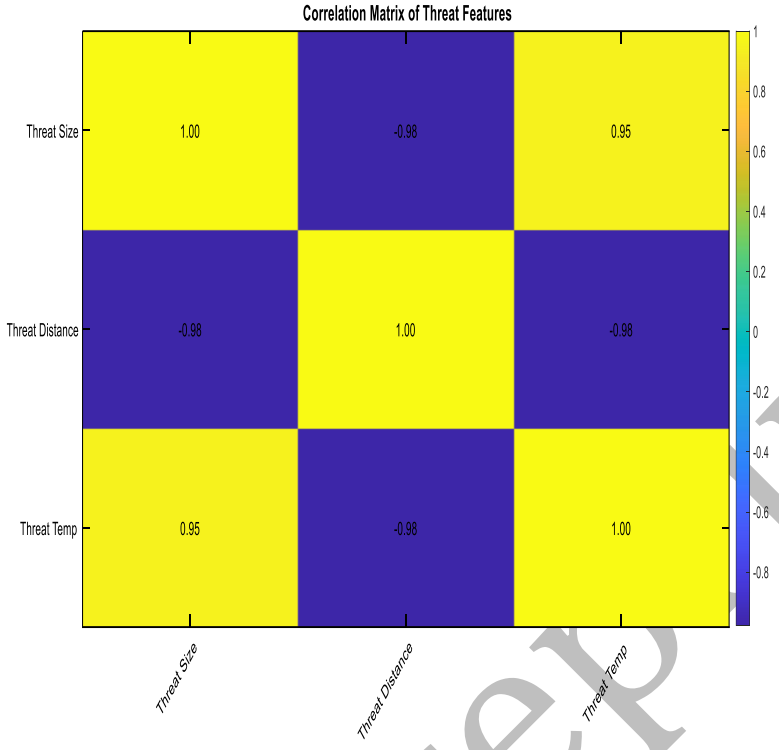

Figure 10: Correlation matrix of engineered threat descriptors (threat size, threat distance, threat temperature).

Not Preprint

4.4.1 Membership Function Configuration

The fuzzy inference system is governed by the membership functions (MFs) defined for each input and the threat-level output. Each input descriptor is partitioned into three overlapping linguistic terms to support gradual transitions under uncertainty: $\{Small, Medium, Large\}$ for threat size; $\{Near, Medium, Far\}$ for threat distance; and $\{Cool, Warm, Hot\}$ for threat temperature. The output threat level is similarly partitioned into $\{Low, Medium, High\}$ risk states.

The MF overlaps are intentionally designed to avoid brittle thresholding and to ensure that small perturbations in feature values do not cause abrupt changes in the inferred threat level. This configuration preserves interpretability while allowing smooth interpolation across mixed or borderline intrusion conditions.

5. Conclusion and Future Work

This paper presented a hybrid AI–fuzzy framework for infrared-based intrusion monitoring in power transmission corridors. The system integrates infrared preprocessing, YOLO-based person detection, threat-oriented feature construction, and a Mamdani fuzzy inference stage implemented in MATLAB/Simulink to produce an interpretable frame-wise threat score. Evaluation on a manually labeled subset (80 frames annotated using Robo flow) showed reliable person-presence detection and

coherent threat-score trajectories suitable for alarm prioritization.

Future work will (i) incorporate independent pixel-level thermal statistics and temporal cues (e.g., motion and persistence), (ii) refine the fuzzy rule base and membership functions with expert input across broader scenarios, and (iii) report end-to-end performance on larger independently annotated datasets, including false-alarm rate, latency, and computational efficiency under edge-deployment constraints.

Acknowledgement

The authors sincerely express their appreciations to the Tertiary Education Trust Fund (TETFund) for sponsoring this research under its Institution-Based Research (IBR) component, which made the study possible. We also extend our gratitude to the Federal Polytechnic, Nyak, for providing an enabling environment, that facilitated the successful execution of this work. Your combined support has been invaluable, and we are deeply grateful.

References

Chen, Q., & Li, J. (2024). Infrared-based anomaly detection using adaptive AI vision models. *IEEE Transactions on Industrial Informatics, 20*(2), 1154–1165.

Deng, L., Fu, R., Li, Z., Liu, B., Xue, M., & Cui, Y. (2024). Lightweight cross-modal multispectral pedestrian detection based on spatial reweighted attention mechanism. *Computers, Materials & Continua, 78*(3), 4071–4089. https://doi.org/10.32604/cmc.2024.048200

Khanam, R., & Hussain, M. (2024). *What is YOLOv5: A deep look into the internal features of the popular object detector* (arXiv preprint arXiv:2407.20892). https://arxiv.org/abs/2407.20892

Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of Industrial Internet of Things. *Symmetry, 15*(10), 1958. https://doi.org/10.3390/sym15101958

Mjahad, A., & Rosado-Muñoz, A. (2025). Combining deep learning architectures with fuzzy logic for robust pneumonia detection in chest X-rays. *Applied Sciences, 15*(19), 10321. https://doi.org/10.3390/app151910321

Okoro, C., Adewale, F., & Zhang, Y. (2024). Hybrid intelligent systems for autonomous power infrastructure security. *Renewable Energy and Power Systems Journal, 12*(1), 33–47.

Sharma, V., & Kumar, R. (2023). Fuzzy decision-support frameworks for surveillance and risk assessment. *Expert Systems with Applications, 229*, 120–145.

NST Preprint

Wang, T., Delgado, M., & Liu, H. (2024). Deep neural architectures for real-time intrusion tracking in low-contrast IR imagery. *Computer Vision and Intelligent Systems, 48*(1), 67–82.

You, S., Ji, Y., Liu, S., Mei, C., Yao, X., & Feng, Y. (2022). A thermal infrared pedestrian-detection method for edge computing devices. *Sensors, 22*(17), 6710. https://doi.org/10.3390/s22176710

Zhang, J. (2022). An infrared pedestrian detection method based on segmentation and domain adaptation learning. *Computers & Electrical Engineering, 99*, 107781. https://doi.org/10.1016/j.compeleceng.2022.107781

Zhou, P., Yang, L., & Hassan, A. (2023). Detection challenges and risk mitigation strategies in power line security. *Energy Infrastructure Protection Journal, 9*(4), 72–90.

NJST Preprint