PureTrack-IR: Blockchain-Enabled Infrared Imaging Agent AI-UAV System for Military Tracking

Sium Bin Noor, Adnan Md Tayeb, Mohtasin Golam,
Subroto Kumar Ghosh, Muhammad Sannan Khaliq, Jae-Min Lee, Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(siumbinmoor, mdtayebadnan, golam248, subroto, sannan, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Recent military UAV surveillance systems struggle in low visibility and challenging operational environments because they rely on visible light sensors, centralized data storage, and human-in-the-loop decision making. This paper introduces PureTrack-IR, a decentralized framework that integrates infrared (IR) imaging, edge optimized object detection, autonomous artificial intelligence (AI) control, and Pure Chain-enabled data management system. Thermal cameras first capture IR images, which are then denoised, aligned, and resized before being processed by an 8-bit–quantized YOLOv11x model on NVIDIA Jetson hardware. This model accurately detects hostile military personnel in darkness, smoke, and adverse weather. The detection outputs are georeferenced and passed to an Agent AI module that uses reinforcement learning for real time threat detection, prioritization, and mission adaptation, thereby reducing operator workload and response time. At the same time, every image, detection, and AI decision is immutably recorded on Pure Chain, a lightweight blockchain employing Smart Auto Mining Plus(SAM+) and a Proof of Authority and Association (PoA^2) consensus mechanism to secure peer-to-peer transactions in under three seconds. Performance evaluation confirms robust detection, low latency decision making, and tamper-proof data integrity. PureTrack-IR enhances situational awareness, operational security, and tactical effectiveness through state-of-the-art detection with 99.4% accuracy, providing a robust and autonomous solution for UAV-based hostile military tracking.**

***Index Terms*—UAVs, Agent AI, Pure Chain, Access Control, Medical Supply**

I. Introduction

In recent years, the use of UAVs in military surveillance has grown significantly due to their ability to provide real-time situational awareness over large areas [1]. UAVs are typically equipped with a variety of sensors, including visible cameras and infrared (IR) sensors, which enable them to track and monitor targets in different operational environments [2]. Traditional methods for surveillance with UAVs mainly relied on visible light cameras and basic object recognition algorithms [3]. These systems were often limited by their performance in low-light conditions and harsh environmental factors such as smoke, fog, or night operations [4]. Many enhanced object detection models have the capability of UAVs to autonomously detect and track objects with greater accuracy [5]. Notable frameworks such as YOLO have been employed for real-time object detection on UAVs, improving tracking performance in clear conditions [6]. These systems remain dependent on visible light imaging, which diminishes their effectiveness in environments with limited visibility. More recent developments have integrated thermal and IR imaging to overcome the limitations of visible light [7]. UAVs equipped with these sensors provide improved visibility during night operations and can operate effectively in fog or smoke environments [8].

However, although military UAV surveillance technologies have improved in recent years, several key challenges still limit their effectiveness in real-world military operations. A primary issue is the continued reliance on visible-light cameras, which perform poorly under low-light or obscured conditions. Additionally, many UAV systems lack sufficient computing power for real-time information processing, posing a particular problem for UAVs with limited hardware resources. Current UAV platforms are constrained by their reliance on rule-based control systems [9], requiring significant human operator intervention for critical decisions like threat classification, target prioritization, and mission adaptation. Such dependency introduces unacceptable response delays in fast-paced combat scenarios where rapid autonomous decisions are essential. Furthermore, existing centralized data storage and processing structures create vulnerabilities including slower data sharing, network failures, and potential security breaches. The absence of secure, automated, tamper-evident validation mechanisms further risks data manipulation, unauthorized access, and loss of integrity for surveillance data and mission-critical commands [10].

To address these challenges, this paper proposes the PureTrack-IR framework, a military UAV surveillance solution that employs an integrated approach that combines advanced infrared imaging technology, artificial intelligence, and a Pure Chain-enabled data management system. PureTrack-IR implements infrared imaging for robust performance in challenging environments such as darkness, smoke, and adverse weather conditions. The system employs optimized YOLOv11x [11] as object detection model on edge computing devices. Agent AI modules enable autonomous decision making through reinforcement learning techniques, reducing operator workload and response delays in fast paced combat scenarios. The Pure Chain [12] blockchain-based data management system [13] ensures data integrity and security through smart contracts, Smart Auto Mining Plus (SAM+), and Proof of Authority and

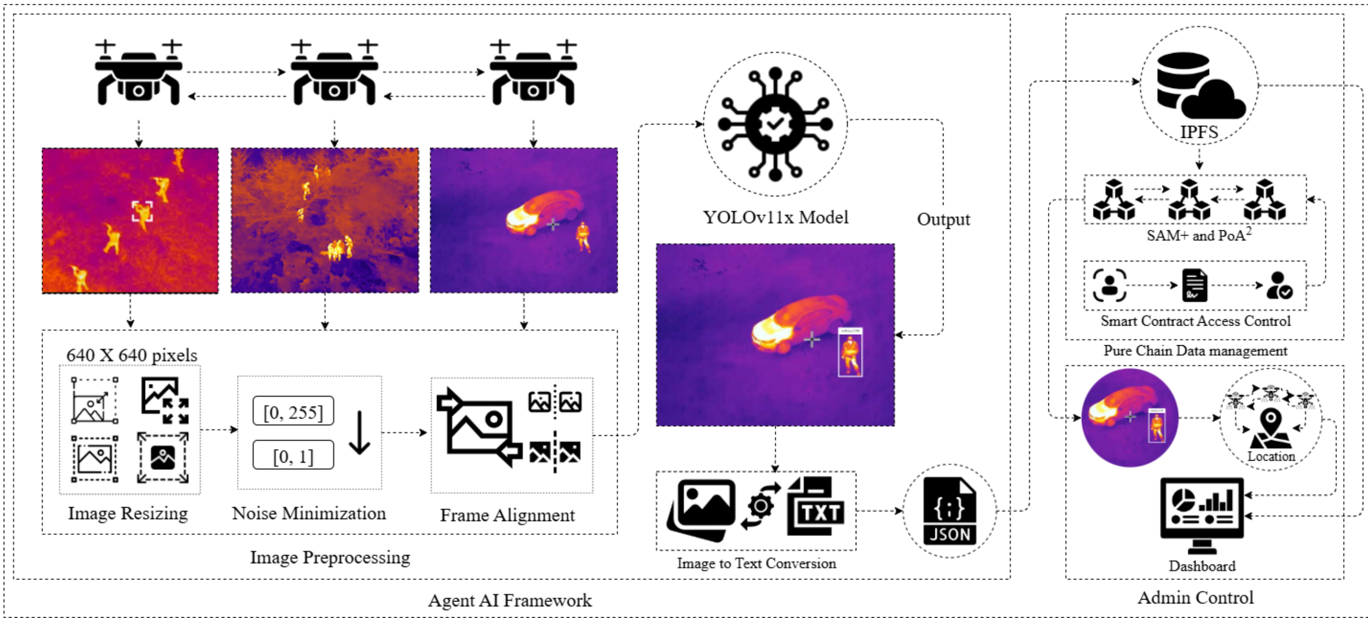

Fig. 1: Overview of the proposed PureTrack-IR

Association (PoA^2) [14] consensus mechanisms that support secure peer-to-peer transactions without traditional ledgers. This decentralized architecture eliminates centralized vulnerabilities while providing automated, tamper-proof validation mechanisms for surveillance data and mission critical commands exchanged between field personnel, command centers, and autonomous UAV units. The comprehensive integration of these technologies creates a robust military surveillance framework that enhances situational awareness, operational security, and tactical effectiveness in complex defense missions while maintaining real-time processing capabilities and autonomous operation in dynamic military environments.

The key contributions of this paper are as follows:

- Integrated IR imaging technology for robust detection in low visibility and adverse environmental conditions.
- Developed an edge-optimized YOLOv11x object detection model and an Agent AI framework enabling real-time autonomous operation.
- Implemented the Pure Chain system with smart contracts and PoA^2 consensus mechanism to ensure decentralized, tamper-proof communications between field units and command centers.

II. Methodology

The Figure 1 illustrates PureTrack-IR system follows a clear sequence of steps: first, infrared images are captured by UAV-enabled thermal cameras and go through basic preprocessing to remove noise and standardize frames. Then, these images are analyze with an optimized YOLOv11x model that detect and identifies hostile military personnel. From IR captured image to detection outputs managed through an Agent AI module so that it computes threats, prioritize targets, and adjust the mission plan autonomously. After that the output result converted into text and store it into json file. At the same time this json result, and AI decision is securely packaged into a Pure Chain transaction. The smart contracts enforce access control, and PoA^2 consensus validates and records each event. Finally, authorized units and command centers read the Pure Chain ledger to receive live updates and send new instructions. This workflow ensures uninterrupted infrared surveillance, fast pace intelligence, self-guided decision making, and tamper-proof data management throughout the operation.

A. IR Image Preprocessing

After the system captures infrared images through UAV-enabled thermal cameras, these raw images are first processed to ensure they are suitable for reliable analysis. The IR image preprocessing step begins with Image Resizing. Then, noise minimization with pixel normalization, where pixel values are adjusted to maintain consistent brightness and contrast across all frames, making detection results more robust. Frame alignment methods applied to further enhance image clarity and stabilize the input for the subsequent object detection stage. This standardized preprocessing ensures that the YOLOv11x model receives clean and uniform input, which is essential for achieving accurate and real time threat detection within the PureTrack-IR system.

a) Image Resizing: All images are uniformly scaled to 640×640 pixels, ensuring a consistent tensor shape for efficient batch processing and seamless integration with the model's architecture:

$$I_{\text{resized}} = \text{resize}(I, (640, 640)).$$

b) Noise Minimization: In the PureTrack-IR system, noise minimization uses dark-frame subtraction to remove fixed pattern noise, flat field correction to normalize pixel response, temporal filtering to smooth random frame-to-frame variations, and spatial correction to balance brightness across each image, ensuring stable, high quality inputs for the YOLOv11x model. The equation as follows:

$$I_{\rm proc}(x,y) = \mathcal{S}\Big\{\, \mathcal{T}\big[\, G(x,y)\, I_{\rm raw}(x,y) \;-\; I_{\rm dark}(x,y)\big] \Big\}.$$

where $I_{\rm raw}(x,y)$: original thermal image, $I_{\rm dark}(x,y)$: dark-frame image for fixed-pattern noise removal, $G(x,y)$: flat-field gain map for pixel response normalization, $\mathcal{T}[\cdot]$: temporal filtering, $\mathcal{S}\{\cdot\}$: spatial correction.

c) Frame Alignment Method: In the PureTrack-IR system, frame alignment corrects for UAV motion and scene shifts by registering each infrared frame to a common reference using feature-based homography estimation followed by subpixel interpolation. The I_{t+1} denote consecutive preprocessed frames. A homography matrix H such that

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} \approx H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}, \qquad H = \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & 1 \end{bmatrix}.$$

Each pixel (x,y) in I_{t+1} is then mapped to (x',y') in the reference frame via subpixel bilinear interpolation:

$$I_{t+1}^{\rm aligned}(x',y') = I_{t+1}\big(H^{-1}[\,x',y',1\,]^{\mathsf T}\big).$$

This process minimizes motion induced misregistration, ensuring that the YOLOv11x detects and operates on stabilized inputs for accurate hostile military localization.

B. YOLOv11x Model Implementation

In this paper, The YOLOv11x object detection model was trained and evaluated on a custom IR UAV dataset, consisting of 75 videos with a total of 96,813 IR frames, split into 55 videos for training, 12 videos for validation, and 8 videos for testing purposes. The model training and validation were performed on a desktop workstation equipped with an NVIDIA GeForce RTX 3060 Ti GPU, while model deployment and inference tests were conducted on edge computing hardware using an NVIDIA Jetson device. The model was trained and deployed on UAV edge hardware using the AdamW optimizer with a learning rate of 0.001667 and momentum of 0.9, replacing default settings of `lr0=0.01` and `momentum=0.937`. During training, six data-loader workers load infrared frames standardized to 640×640 pixels and 16 batch size for uniform tensor shapes and efficient batching. The model backbone was removed by 30% and quantized to 8-bit precision to reduce computational demands, while the detection head incorporates a streamlined C2PSA block to preserve accuracy with fewer parameters. After 100 epochs of training, the removed and computed network is exported to TensorRT using FP16 precision for onboard inference, achieving throughput above 30 FPS on NVIDIA Jetson platforms. This configuration ensures fast, accurate IR hostile military localization within the strict computational constraints of military UAV operations.

a) Military Detection: Each preprocessed IR frame $\hat{I}$ is input to the YOLOv11x network, which employs a multi-scale feature extraction backbone and detection heads to predict bounding boxes, confidence scores, and class probabilities for hostile military personnel. The raw detection output is represented as:

$$\{(x_i, y_i, w_i, h_i, c_i, p_i)\}_{i=1}^{N}$$

where (x_i, y_i) represents the center coordinates of the bounding box, (w_i, h_i) are the width and height, c_i is the confidence score, and p_i is the probability of the detected class.

b) Non-Maximum Suppression (NMS): Detections with confidence scores $c_i < T_d$ are discarded. The remaining boxes are refined through Non-Maximum Suppression. For any pair (i,j), if $\mathrm{IoU}(b_i, b_j) > T_{\rm IoU}$, the box with the lower confidence is removed. The final filtered detection set is defined as:

$$D = \{b_k \mid c_k \geq T_d,\ \forall j : \mathrm{IoU}(b_k, b_j) \leq T_{\rm IoU}\}\,.$$

where D is the final set of filtered detections, b_k is a candidate bounding box, c_k is its confidence score, T_d is the minimum confidence threshold, $\mathrm{IoU}(b_k, b_j)$ is the Intersection-over-Union between boxes b_k and b_j, $T_{\rm IoU}$ is the IoU threshold for suppression, and $\forall j$ means the condition must hold for all other boxes b_j.

c) Location Tracking: Each final detection $b_k \in D$ is transformed into geospatial coordinates (ϕ_k, λ_k) using UAV-specific telemetry data, including GPS location, altitude, and camera pose. This mapping is computed as:

$$(\phi_k, \lambda_k) = \mathrm{GeoMap}(b_k, P_{\rm UAV}, C_{\rm cam}).$$

where ϕ_k and λ_k represent the latitude and longitude of the detected military personnel, $P_{\rm UAV}$ denotes the UAV's GPS and altitude information, and $C_{\rm cam}$ refers to the internal and external camera parameters. The resulting detection record $(\phi_k, \lambda_k, t_k, c_k)$ is then passed to the Agent AI module for real time decision making and securely logged to the Pure Chain data management system.

C. Agent AI Framework Workflow

The Agent AI module in the PureTrack-IR system processes detection outputs from the YOLOv11x system such as bounding box coordinates, confidence scores, and class probabilities together with UAV environmental metadata to develop a clearer understanding of its operational area. It tracks recent detection events in short-term memory, enabling the identification and monitoring of real threats by assessing detection confidence and proximity to key zones. Using clear rules, adaptive scoring, and reinforcement learning, the AI scores each threat and ranks detected entities according to mission priorities and real-time changes. Reinforcement learning allows the system to learn optimal responses from previous interactions, improving its autonomous decision making. This approach ensures the most critical targets receive prompt attention and, when necessary, uncertain cases are flagged for human review. The system generates actionable UAV commands such as route adjustments or tracking sequences while logging all key decisions to Pure Chain for audit and coordination. This enables autonomous, efficient, and secure military tracking operations.

Algorithm 1 Agent AI Mission Control System

Require: YOLOv11x outputs $\{(x_i, y_i, w_i, h_i, c_i, p_i)\}_{i=1}^{N}$, UAV data, mission parameters
Ensure: UAV commands, blockchain logs
while system active **do**
  Receive detection outputs from YOLOv11x
  Fuse with UAV metadata
  Update short-term memory buffer
  for each detection i **do**
    Compute threat score T_i (based on c_i, location, consistency)
  end for
  Rank threats based on T_i and mission priority
  Select top-k targets
  for each selected target **do**
    Decide action (track, alert, reroute)
    if $c_i < T_d$ **then**
      Flag for human review
    end if
  end for
  Generate UAV commands
  Log $(b_k, T_k, \varphi_k, \lambda_k, \text{timestamp})$ to Pure Chain
end while=0

D. Pure Chain Data Management System

Figure 2 illustrates Pure Chain Transactions and Contract Deployment. The system is a lightweight, blockchain-based solution integrated into the PureTrack-IR system to ensure secure, tamper-proof management of all critical mission data. After each inference and decision cycle by the Agent AI module, essential information including detection results, timestamps, and locations is formatted into interplanetary file system (IPFS) storage. These records are cryptographically signed

Fig. 2: Pure Chain Transactions and Contract Deployment

and submitted to the Pure Chain distributed ledger, which employs PoA^2 consensus mechanism specifically adapted for real time, resource constrained UAV deployments. The smart contract guarantees rapid validation and robust traceability without dependence on external infrastructure, making it well suited for difficult environments. Throughout the mission, Pure Chain enables cross agent synchronization by securely distributing validated records among collaborating UAVs and command centers, supporting autonomous coordination and real time situational awareness. Upon mission completion, authorized users can efficiently retrieve immutable logs for post mission review, analysis, and compliance documentation. By embedding blockchain mechanisms directly into the data pipeline, Pure Chain provides end-to-end data integrity, reliable event auditability, and transparent decision tracking for military UAV operations in tracking hostile military.

1) The PoA^2 Consensus Mechanism: The PoA^2 consensus mechanism in Pure Chain, secure low latency operation in UAV-based military environments. It ensures a permissioned set of authenticated validator nodes, each with a defined role, among which block production rotates on a fixed schedule to prevent any single point of control. For each transaction, including IPFS content identifiers, metadata, and sender signatures, validators verify identities and enforce role based permissions using smart contracts, as well as check data integrity. The designated block producer aggregates approved transactions, signs and broadcasts a candidate block, and waits for a majority of validators to confirm before finalizing the entry to the chain ensuring an immutable, tamper-proof audit trail. The Smart Auto Mining Plus (SAM+) module predicts network load and dynamically optimizes block production timing to maintain responsiveness, while dual operator co-signing for critical mission data and distributed IPFS storage add layers of human oversight and data resilience. This PoA^2 approach delivers a robust, efficient, and transparent consensus suitable for real time, trusted data management in resource constrained and difficult UAV deployments in military tracking. Let the set of n validator nodes:

$$\mathcal{V} = \{V_1, V_2, \ldots, V_n\} \tag{1}$$

Then the block producer for block k is determined by the rotating block–producer formula:

$$P_k = V_{\left((k \bmod n)+1\right)} \tag{2}$$

Furthermore, PoA^2 requires a minimum of validator approvals to finalize each block. A block is committed once at least:

$$q > \frac{n}{2} \tag{3}$$

These three equations (1), (2) and (3) combines the PoA^2 mechanism of rotating production authority and simple majority finality.

2) Smart Contract Access Control Mechanism: The Pure Chain system implements smart contract-based access control to ensure secure and management of mission data within the PureTrack-IR system. Each transaction such as a detection record or threat assessment is controlled by smart contracts that strictly enforce role based permissions for UAV operators, validators, and command centers. Access rights are dynamically assigned according to authenticated roles and mission critical requirements, allowing only authorized personnel to

TABLE I: Detection result of object detection models for IR and UAV applications.

Model	Precision (%)	Recall (%)	mAP@0.50 (%)	mAP@0.50:0.95 (%)	Detection Robustness
MobileNet SSD	82.5	84.0	86.5	47.5	Low–Moderate (fast, less robust)
YOLOv4	94.0	93.0	94.5	62.0	High
YOLOv5-S	90.8	92.2	94.0	57.0	Moderate–High
YOLOv5-X	96.5	96.5	98.0	68.0	High
EfficientDet-D3	95.5	95.2	96.0	65.0	High
YOLOv8-S	90.5	91.5	94.0	63.0	Moderate–High
PP-YOLOE	95.4	95.1	96.2	68.3	Very High
YOLOv11x (ours)	**98.3**	**98.9**	**99.4**	**68.9**	**Highest for complex IR tasks**

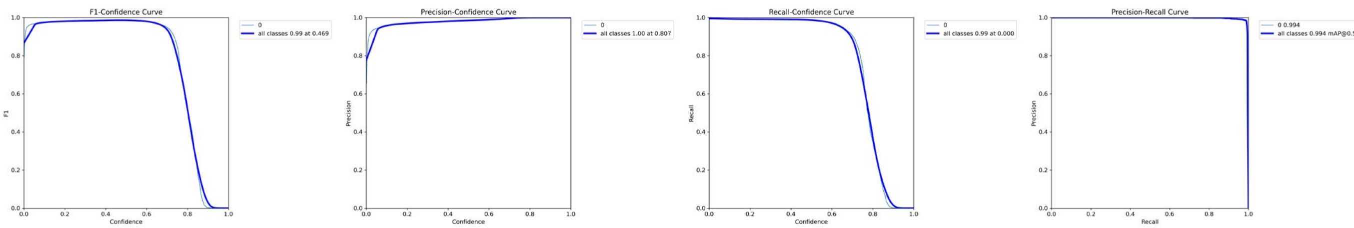

Fig. 3: YOLOv11x Model's F-1, Precision, Recall, and Precision-Recall Curve

view, modify, or approve sensitive actions. Identity verification is achieved via cryptographic signatures, while smart contracts automatically log and audit all access attempts, updates, and approvals. This approach guarantees that only authenticated and permissioned person can interact with mission data, ensuring operational security, accountability, and compliance throughout all stages of autonomous UAV operations.

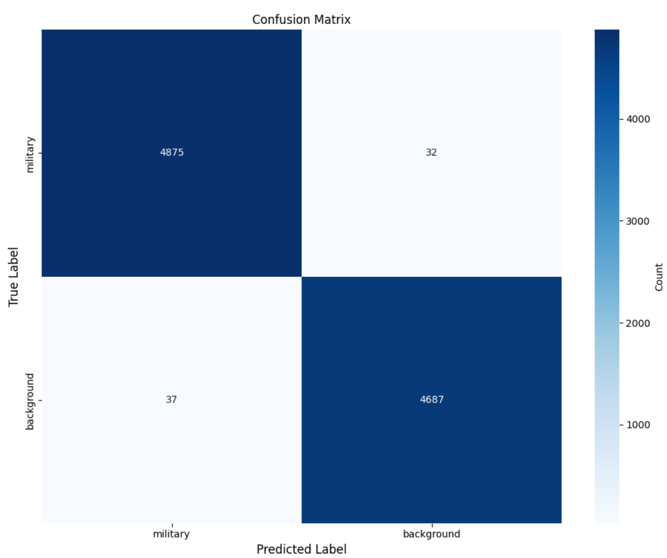

Fig. 4: Confusion matrix

III. Performance Evaluation

The YOLOv11x model supports the PureTrack-IR system requirements for autonomous real-time hostile military detection, ensuring that each decision cycle produces reliable data for downstream geo-referencing, Agent AI-driven prioritization, and immutable logging within the Pure Chain data management backbone. This synergy positions YOLOv11x as a state-of-the-art backbone for tactical military UAV surveillance and response missions.

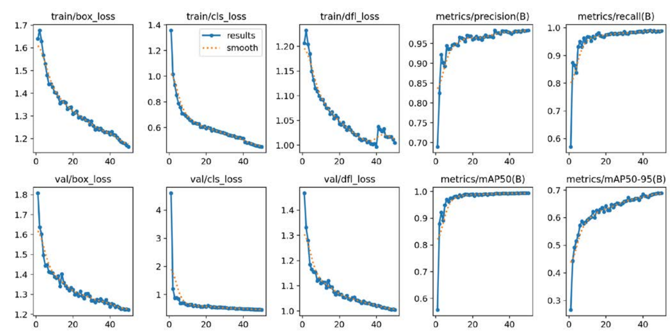

Fig. 5: YOLOv11x Model's Training and Validation Loss

A. *YOLOv11x Model's Performance Evaluation*

Table I illustrates the detection accuracy metrics of object detection models for IR and UAV applications. The YOLOv11x model on an IR UAV dataset, highlighting its exceptional detection capability in complex military environments. Figure 3 shows a precision of 98.3% and recall of 98.9%, the model demonstrates highly accurate object classification with minimal false positives or missed detections. It achieves a near perfect mAP@50 of 99.4%, indicating excellent localization and confidence in predicted bounding boxes, while maintaining a strong mAP@50-95 of 68.9%, reflecting robust performance across multiple IoU thresholds. The architecture comprises 190 layers and approximately 56.8 million parameters, with a computational complexity of 154.4 GFLOPs, making it well suited for real time inference on edge AI systems. These metrics confirm that the YOLOv11x model is not only accurate but also efficient and reliable for real time hostile military detection in IR UAV imagery.

B. Smart Contract Performance Analysis

The smart contract module in the PureTrack-IR system provides secure, automated access control and auditability for all mission critical data, including UAV detected targets and operational reports, by immutably recording every access attempt, approval, and denial on the Pure Chain blockchain. Seamlessly integrated with the PoA^2 consensus mechanism, the module achieves low transaction latency 1-3 seconds and high throughput 25-50 transactions per second, enabling real time data management essential for military UAV operations. Through strict role based authentication, cryptographic signature verification, and smart contract enabled permissions, the system ensures that only authorized personnel can access or modify sensitive mission records. This robust approach not only secures and streamlines critical information flows but also supports scalable, flexible workflows, empowering authorized operators to reliably manage and coordinate mission data within the PureTrack-IR framework.

C. IPFS Storage Analysis

PureTrack-IR offloads bulky image and metadata payloads to IPFS, storing only compact CIDs and transaction headers on-chain to control ledger growth. Each detection event transaction records a 256-bit CID, timestamp, and digital signature (100 bytes), while command logs add another 80 bytes. At an average mission rate of 10 events/s, on-chain storage increases by 1.8 KB/s (6.5 MB/h). Even a 12h operation thus requires only 78 MB of persistent storage. IPFS nodes retain full image data with configurable pinning policies, while PoA^2 validators archive older blocks beyond mission relevant time windows. This hybrid storage design ensures a constant on–chain footprint, predictable scaling, and flexible long-term archiving, preventing excessive blockchain growth over time.

D. Multi-UAV Simulation Evaluation and Scalability Analysis

The PureTrack-IR framework demonstrates scalability potential for multi-UAV swarm operations through distributed Pure Chain consensus mechanisms. Performance evaluation across varying swarm sizes 2-20 UAVs reveals that the PoA^2 consensus maintains 5 second transaction latency for formations up to 20 UAVs, with acceptable degradation to 7-8 seconds for larger swarms. Each UAV operates autonomously for YOLOv11x inference while sharing threat assessments through encrypted blockchain transactions, enabling collaborative situational awareness without centralized coordination.

IV. Conclusion and Future Directions

PureTrack-IR integrates infrared imaging, YOLOv11x detection, Agent AI, and Pure Chain to enhance military UAV surveillance in low visibility and difficult environments. IR ensures robust sensing, YOLOv11x delivers precise hostile military identification, and Agent AI autonomously prioritizes and responds to targets, reducing operator workload and latency. Pure Chain secures data via SAM+, smart contracts, and PoA^2 consensus, creating a decentralized, tamper-proof system. Future work includes integrating multispectral sensors, federated learning for collaborative AI updates, adaptive blockchain scaling, and rigorous field trials to validate resilience and performance. This integrated solution significantly advances real-time autonomous decision making capabilities in military UAV surveillance.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] A. Ham, D. Similien, S. Baek, and G. York, "Unmanned aerial vehicles (uavs): Persistent surveillance for a military scenario," in *2022 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 1411–1417, IEEE, 2022.

[2] K. Niu, C. Wang, J. Xu, J. Liang, X. Zhou, K. Wen, M. Lu, and C. Yang, "Early forest fire detection with uav image fusion: A novel deep learning method using visible and infrared sensors," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2025.

[3] M. Bakirci, P. Dmytrovych, I. Bayraktar, and O. Anatoliyovych, "Multi-class vehicle detection and classification with yolo11 on uav-captured aerial imagery," in *2024 IEEE 7th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD)*, pp. 191–196, IEEE, 2024.

[4] K. Song, X. Xue, H. Wen, Y. Ji, Y. Yan, and Q. Meng, "Misaligned visible-thermal object detection: A drone-based benchmark and baseline," *IEEE Transactions on Intelligent Vehicles*, 2024.

[5] M. Muzammul, A. Algarni, Y. Y. Ghadi, and M. Assam, "Enhancing uav aerial image analysis: Integrating advanced sahi techniques with real-time detection models on the visdrone dataset," *IEEE Access*, vol. 12, pp. 21621–21633, 2024.

[6] S. Panigrahy and S. Karmakar, "Real-time condition monitoring of transmission line insulators using the yolo object detection model with a uav," *IEEE Transactions on Instrumentation and Measurement*, vol. 73, pp. 1–9, 2024.

[7] R. N. Strickland, "Infrared techniques for military applications," in *Infrared methodology and technology*, pp. 397–427, CRC Press, 2023.

[8] D. Zhang, D. Li, L. Zhou, and J. Wu, "Fine classification of uav urban nighttime light images based on object-oriented approach," *Sensors*, vol. 23, no. 4, p. 2180, 2023.

[9] C. Sieber, L. M. Vieira da Silva, K. Grünhagen, and A. Fay, "Rule-based verification of autonomous unmanned aerial vehicles," *Drones*, vol. 8, no. 1, p. 26, 2024.

[10] M. Golam, R. Akter, R. Naufal, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "Blockchain inspired intruder uav localization using lightweight cnn for internet of battlefield things," in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*, pp. 342–349, IEEE, 2022.

[11] R. Khanam and M. Hussain, "Yolov11: An overview of the key architectural enhancements," *arXiv preprint arXiv:2410.17725*, 2024.

[12] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for iot blockchain networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, IEEE, 2025.

[13] M. Golam, R. Akter, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Lightweight blockchain assisted unauthorized uav access prevention in the internet of military things," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 890–894, IEEE, 2022.

[14] D.-S. Kim and R. Syamsul, "Integrating machine learning with proof-of-authority-and-association for dynamic signer selection in blockchain networks," *ICT Express*, vol. 11, no. 2, pp. 258–263, 2025.