Edge-AI Detection with Blockchain in Military IoT

Sium Bin Noor, Mohtasin Golam, Subroto Kumar Ghosh, Jae-Min Lee, Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(siumbinmoor, gmoh248, subroto, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Military environment needs a secure solution to detect and identify unattended objects and ensure data security in real-time. This paper proposed an edge-AI framework that integrates object detection model with blockchain for unattended object detection in military IoT environments. The proposed approach enables real-time detection, decentralized server and secure event logging on edge devices, overcoming typical limitations of bandwidth, latency, and data integrity that found in cloud-based and centralized solutions. The YOLOv11n model is optimized for unauthorized object detection in limited hardware that achieved accuracy 94.28%, precision 94.04%, recall 93.09%, and F1-score 92.56% and trained on 35k image dataset of military unattended objects. Pure Chain [1], a private blockchain network that uses PoA^2 consensus mechanism [2], ensures tamper-proof auditability and high throughput. This paper illustrates Pure Chain achieves a low average latency of 3.55 ms and high throughput of 27 transactions per second that outperforms the Sepolia public testnet of 12.23 ms latency and 9 TPS. Smart contract based access control enhances operational security and reliability. This combined framework makes a significant contribution to military AI that provides an intelligent, secure, and optimized solution for military surveillance.**

***Index Terms*—Edge-AI, Object Detection, Pure Chain, Access Control, Military IoT**

I. Introduction

The rapid growth of Internet of Things (IoT) technology has greatly influenced military security surveillance by enabling continuous sensing, monitoring, and real-time data collection across vast and disparate environments [3]. This development allows defense systems to track personnel, equipment, and potential threats with unprecedented coverage and immediacy. Combining edge computing with artificial intelligence (AI) techniques such as object detection model presents a powerful solution to overcome limitations inherent in traditional cloud-based surveillance systems [4]. These limitations include network delays, bandwidth strain, and privacy vulnerabilities that can hinder timely and secure military operations. Object Detection models works well because of their ability to capture detailed spatial and contextual information from images [5], enabling precise detection even in highly dynamic, cluttered, or complex scenes typical in military scenarios. Implementing AI models directly on edge devices such as fixed surveillance cameras, drones, or ground sensors facilitates rapid data processing and decision making at the point of collection, reducing reliance on centralized cloud servers and thus lowering latency and network traffic [6]. Despite these advantages, securing AI deployments on edge devices remains challenging, especially in hostile or high security environments. Blockchain technology offers a promising approach to ensure data integrity, transparency, and trustworthiness by employing decentralized and tamper resistant ledgers for IoT-generated security logs, detection events, and AI model updates. The integration of deep learning, edge computing, and blockchain in military surveillance not only enhances operational efficiency but also strengthens security posture, enabling reliable, auditable, and resilient defense solutions responsive to evolving threats [7].

However, challenges remain in applying AI surveillance systems within military IoT environments. First, edge devices generally have limited computing power [8], which restricts the size and complexity of AI models that can be deployed efficiently while still meeting real-time processing demands. Many object detection models, though powerful in understanding spatial relationships but are computationally heavy and require carefully designed variants suitable for edge deployment. Second, accurately and swiftly detecting unattended objects such as suspicious or unauthorized packages is critical to avoid serious security incidents. Missing detections or delayed alerts can lead to catastrophic consequences in high-risk military settings. Third, the security and trustworthiness of surveillance data must be preserved at all costs. Centralized logging systems are vulnerable to cyber-attacks, data manipulation, and single points of failure [9], which can compromise forensic investigations and operational integrity. Finally, managing automated responses triggered by AI alerts depends on a secure, decentralized framework to prevent errors caused by human intervention or malicious tampering. Without such safeguards, response coordination could be inconsistent or unreliable, jeopardizing situational awareness and threat mitigation.

To solve these, this paper proposes a framework combining YOLOv11n model optimized for edge devices with the Pure Chain network. The approach uses specialized models able to run efficiently on resource-limited edges, detecting unattended objects quickly and accurately. To ensure security and transparency, all detection events, metadata, and model updates are immutably stored on the Pure Chain, removing tampering risks and enabling secure audits. Smart contracts in the Pure Chain coordinate security responses, reducing manual effort and speeding threat management. Processing data locally saves network resources and reduces delays, while Pure Chain's decentralized trust model increases resilience against attacks. Together, these compose a secure, trustworthy, and intelligent surveillance framework for military use, enhancing awareness, response time, and reliability.

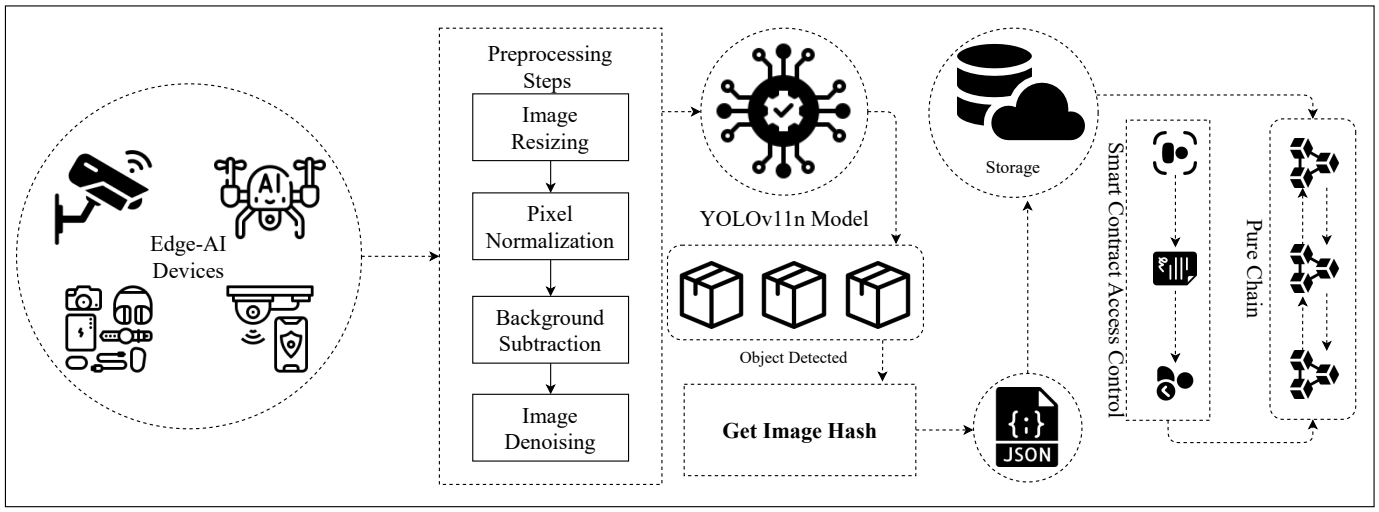

Fig. 1: Overview of the proposed Edge-AI Object Detection with Blockchain Framework

The key contributions of this paper are as follows:

- Integrated YOLOv11n model that runs efficiently on edge devices for detecting unattended objects with 94.28% accuracy.
- Developed Pure Chain to securely and transparently record detection events with 3.55 ms low latency.
- Implemented smart contracts to secure the access control for Pure Chain logs.

II. Related Works

Narayanan et al. [10] explored a YOLOv9-based system for fast, accurate soldier face detection and counting under varied battlefield conditions, including occlusion, PPE, and noise. Evaluation on a diverse dataset demonstrates robust performance with low mean absolute error and real-time inference suitable for military tactical operations.

Rady et al. [11] describe YOLOv7, YOLOv8, YOLOv10, and RT-DETRv3 for military aircraft detection from aerial imagery using a challenging, diverse dataset. Results show that RT-DETRv3 achieves the highest accuracy, while YOLOv10 delivers the fastest inference, highlighting the trade-offs between detection precision and real-time performance for defense applications.

Liu et al. [12] propose a multiscale attention and boundary-aware network with a pyramid YOLOv11n backbone to detect military-camouflaged objects using UAV imagery. Extensive experiments on the MCOD-UAV dataset show that the approach significantly outperforms existing methods in detection accuracy under challenging camouflage conditions.

Yang et al. [13] presents FATCNet, a novel architecture combining feature adaptive models and CNNs for detecting small infrared targets, enhancing feature extraction and suppression of background noise. Experimental results demonstrate FATCNet's superior detection accuracy and robustness compared to state-of-the-art methods on challenging infrared small target datasets.

Alqahtani et al. [14] propose a blockchain-based smart monitoring framework to enhance security, transparency, and trustworthiness in defense industry operations. It integrates IoT sensor data with blockchain technology to provide immutable event logging, real-time monitoring, and automated threat response, addressing challenges in centralized data management and cyber threats in defense environments.

Shareef et al. [15] presents a blockchain-based framework to secure object detection data by ensuring data integrity, transparency, and traceability in distributed AI systems. It leverages blockchain's immutability to prevent tampering of detection results and supports secure sharing of object detection information across decentralized networks.

Peruman et al. [16] proposes a blockchain-based deep learning object detection system designed to enhance the security and reliability of surveillance by ensuring tamper-proof data integrity and transparent record-keeping of detection events. The integration of blockchain technology with AI models provides a decentralized framework that safeguards detection data against manipulation and enables secure sharing in distributed environments.

III. Proposed Framework

Fig. 1 illustrates that the proposed framework integrates a YOLOv11n object detection model optimized for edge IoT devices with blockchain technology to enable secure, real-time detection of unattended objects in military surveillance. The YOLOv11n model executes efficiently on resource-constrained edge devices (Raspberry Pi 5), accurately detecting suspicious unattended objects such as unauthorized packages, boxes, land mines, and containers. Detection events, metadata (object class, location, timestamp), and associated evidence (image hash) are immutably recorded on Pure Chain, ensuring data integrity and tamper-proof audit trails. Smart contracts enforce role-based access control, restricting detection logs and threat assessments to authorized personnel only. This decentralized

architecture balances computational efficiency, detection accuracy, and secure data management, providing an intelligent, resilient surveillance solution for IoT-enabled military environments.

Algorithm 1 Proposed Framework Workflow

Require: Edge AI device with detection model M, Pure Chain, smart contract C, off-chain latency recorder L
Ensure: Secure, tamper-proof unattended object detection records

Initialize detection model M on edge device
while system active **do**
  Capture sensor data and video frames F
  Detect object $O \leftarrow M(F)$
  if O detected **then**
    Extract metadata $\mathcal{D} = (O, L, H)$ where L = location, H = image/video hash
    Timestamp submission time $t_s \leftarrow L$.recordTime()
    Submit transaction $T \leftarrow C$.recordDetection($\mathcal{D}$) to Pure Chain
    Wait for transaction T to be mined in block b
    Get block timestamp $t_b \leftarrow b$.timestamp
    Event $E \leftarrow (O, L, H, t_b, b)$ is recorded immutably on-chain via smart contract C
    Contract emits `DetectionRecorded` event with event E
    Calculate latency: $\Delta t = t_b - t_s$
  end if
end while
Authorized users query stored events $\{E_i\}$ from C for auditing and decision making
Use blockchain consensus to guarantee data integrity and trustworthiness

A. Image Preprocessing

The framework captures visual data from fixed edge IoT surveillance cameras, the raw images undergo preprocessing to enhance their suitability for reliable unattended object detection. The preprocessing pipeline begins with Image Resizing, where all images are uniformly scaled to a fixed size to ensure consistent input dimensions for the YOLOv11n model. Next, Pixel Normalization is applied to adjust pixel intensity values, equalizing brightness and contrast across frames to improve model robustness under varying lighting conditions. To further refine the input, background subtraction techniques isolate foreground objects by removing static scene elements, enhancing the detection of new unattended items. Finally, image denoising using filtering methods reduces sensor noise, contributing to clearer, stable inputs for the model. This sequence of standardized preprocessing steps guarantees that the YOLOv11n receives clean, normalized, and consistent image data, which is critical to achieving accurate and low-latency unattended object detection on edge devices.

a) Image Resizing: In (1), images are resized to 320×320 pixels to match the input size expected by the YOLOv11n model. This resizing enables the image to be divided into 16×16 patches.

$$I_{\text{resized}} = \text{resize}(I, (320, 320)). \tag{1}$$

b) Pixel Normalization: Pixel values of the resized images are normalized from the range $[0, 255]$ to $[0, 1]$ in (2) by dividing each pixel value by 255. This normalization standardizes the input data, improving training stability and model performance.

$$I_{\text{norm}} = \frac{I_{\text{resized}}}{255}. \tag{2}$$

c) Background Subtraction: Background subtraction isolates moving or new objects by removing static parts of the scene in (3). It compares the current frame I_t with a reference background B_t to generate a foreground mask M_t.

$$M_t = |I_t - B_t| > T, \tag{3}$$

where T is a threshold to identify significant pixel differences. This mask highlights unattended objects by filtering out the unchanged background, enabling the YOLOv11n model to focus on relevant regions for improved detection accuracy.

d) Image Denoising: Image denoising reduces noise introduced during image capture to improve input quality for the YOLOv11n. This process smooths unwanted artifacts while preserving important edges and details. Common methods include filtering techniques like non-local means or total variation denoising, which minimize noise based on pixel similarity and spatial coherence. The denoised image I_{denoised} enhances detection accuracy by providing clearer and more stable inputs to the model.

B. YOLOv11n Model Implementation

In this paper, a YOLOv11n model was trained and evaluated on a custom military unattented object detection dataset consisting of 35k labeled images depicting various unattended objects in surveillance scenes. Training was conducted on NVIDIA GeForce RTX 3060 GPU. The YOLOv11n model was trained using the Adam optimizer with a learning rate of 0.001 and a weight decay of 0.01. Input images were resized to 320×320 pixels with a batch size of 16 for consistent and efficient training. In Table II the finalized model was converted to TensorRT format using FP16 precision for deployment on edge hardware, achieving inference speeds above 30 frames per second. This configuration effectively balances accuracy and computational efficiency, enabling real-time unattended object detection in constrained military IoT environments.

a) Unattended Object Detection: Each preprocessed image $\hat{I}$ is fed into the YOLOv11n model, which processes the image by dividing it into fixed-size patches and applying feature extraction method to extract relevant spatial features in (4). The model outputs a set of predictions corresponding to detected unattended objects and their locations.

$$\{(x_i, y_i, w_i, h_i, s_i, p_i)\}_{i=1}^{N}, \tag{4}$$

where (x_i, y_i) denote the center coordinates of the bounding box, (w_i, h_i) represent the width and height of the detected

object, s_i is the confidence score indicating detection certainty, and p_i is the probability distribution over object classes.

C. Raspberry Pi 5 Edge Device Implementation

The YOLOv11n model is converted from PyTorch to ONNX format with FP16 precision and optimized using TensorRT to generate a 2.6 MB hardware-accelerated engine for Raspberry Pi 5 deployment. The edge device illustrates in Fig. 2 runs a real-time inference pipeline that continuously captures video frames, preprocesses them, and executes the TensorRT-optimized detector, achieving 30.3 FPS with 33 ms average latency per frame. Upon detecting unattended objects (unauthorized boxes, land mines, packages, containers), the device extracts detection metadata (class, confidence, location, timestamp) and submits it as a transaction to Pure Chain via the smart contract interface, leveraging the Pure Chain's 3.55 ms transaction latency and 27 TPS throughput to ensure immutable, tamper-proof logging of all detection events.

(a) Camera Front View

(b) Internal Electronics and Compute Module

Fig. 2: Surveillance Camera Enclosure with Raspberry Pi 5 Edge Device Implementation

D. Pure Chain Integration

Pure Chain integration in the framework illustrates in Fig. 3 works by securely logging all detection events, metadata, and model updates onto the decentralized Pure Chain network. After an unattended object is detected by the YOLOv11n model running on edge devices, the detection data is packaged as a transaction and sent to the Pure Chain network, where it is validated and immutably recorded in blocks. This integration ensures data integrity, transparency, tamper-proof traceability in military IoT.

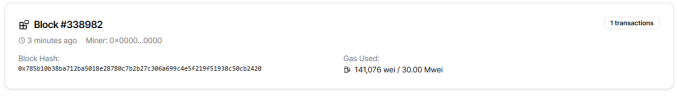

Fig. 3: Pure Chain Transaction Record

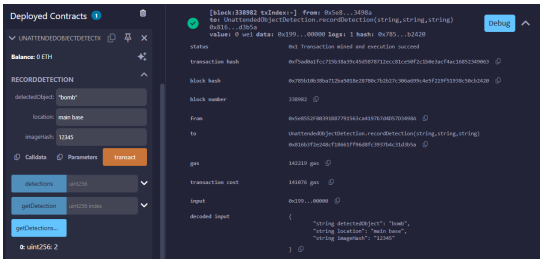

Fig. 4: Smart Contract Deployment for Access Control

a) (PoA^2) Consensus Mechanism: Pure Chain uses the PoA^2 consensus mechanism with pre-approved validator nodes. Validators are selected based on verified identities and rotation occurs deterministically in round-robin fashion by block height $v_h = (h \mod N)$, where v_h is the validator index at height h and N is the total validators. Consensus finality requires two-thirds validator approval, preventing dominance and ensuring security. This approach provides low latency, high throughput, resilience against failures, and resistance to malicious behavior, making PoA^2 suitable for secure, efficient blockchain operation in military IoT applications.

b) Smart Contract-Based Access Control: The smart contract illustrates in Fig. 4 securely records unattended object detection events on Pure Chain. It accepts input parameters shown in Table III detected object type, detection location, and image hash serving as evidence. Upon submission via RECORDDETECTION and mining, the event is immutably logged with transaction details including transaction hash, gas used (141,076 wei), and block number. This creates a tamper-proof audit trail accessible for verification and analysis. The deployment demonstrates successful execution of the smart contract for secure, transparent, and decentralized event logging that essential for trust and reliability in military IoT surveillance systems.

IV. Performance Evaluation

A. YOLOv11n Model Detection Results

The YOLOv11n model was evaluated on a military unattended object detection dataset of 35k images (25k training, 5k validation, 5k test). The model achieves 94.28% accuracy, 94.04% precision, 93.09% recall, and 92.56% F1-score across all object classes (*unauthorized_box*, *land_mine*, *packages*, *containers*), with per-class metrics exceeding 92%. As shown in Table I, YOLOv11n outperforms competing models (YOLOv8, YOLOv10n, Faster R-CNN, EfficientDet-D0, SSD MobileNet, RT-DETR) with superior accuracy while maintaining the second smallest model size (YOLOv10n model size: 2.3M) and fastest inference latency (33 ms), making it ideal for edge-device deployment. The confusion matrix in Fig. 5 further validates detection performance.

B. Raspberry Pi 5 Performance Evaluation

Raspberry Pi 5 was benchmarked for latency, throughput, power, and thermal characteristics in Table IV. The device achieved 33 ms inference latency and 30.3 FPS throughput

TABLE I: Object Detection Model Comparison: Performance Metrics and Computational Efficiency Analysis

Model	**Accuracy Metrics**				**Efficiency**		**Status**
	Acc.	**Prec.**	**Rec.**	**F1**	**Params (M)**	**Inf. (ms)**	
YOLOv8n	92.81%	92.95%	92.10%	91.02%	3.2	45	Baseline
YOLOv10n	93.15%	93.42%	92.88%	91.65%	**2.3**	38	Good
Faster R-CNN	91.45%	91.80%	91.99%	91.89%	138	120	Heavy
EfficientDet-D0	90.80%	90.10%	90.76%	91.93%	3.9	65	Moderate
SSD MobileNet	93.50%	92.80%	92.90%	91.85%	5.8	42	Competitive
RT-DETR	91.20%	90.85%	92.05%	91.95%	36	85	Heavy
YOLOv11n	**94.28%**	**94.04%**	**93.09%**	**92.56%**	2.6	**33**	**Best**

TABLE II: Multi-Layer Performance Matrix and Deployment Analysis

Configuration	**Accuracy Metrics**				**Performance**			**Storage**			**Deploy Status**		
	Acc. (%)	**Prec.** (%)	**Rec.** (%)	**F1** (%)	**Lat.** (ms)	**FPS** (fps)	**Speed** (×)	**Size** (MB)	**Red.** (%)	**Format**	**RT**	**Viable**	**Prod.**
V1: Baseline	96.28	95.04	96.09	95.56	125.0	8.0	1.0	43.0	–	PyTorch FP32	×	×	×
V2: +TensorRT	95.26	95.02	94.07	94.54	85.0	11.8	1.47	42.0	-2	TensorRT FP32	×	○	○
V3: +FP16	94.98	95.82	95.92	95.36	48.0	20.8	2.60	22.0	-49	TensorRT FP16	✓	✓	✓
V4: +Input 320×320	94.95	94.78	94.15	93.45	45.0	22.2	2.78	43.0	–	PyTorch FP32	✓	○	○
V5: Full Optimization	**94.28**	**94.04**	**93.09**	**92.56**	**33.0**	**30.3**	**3.79**	**2.6**	**-94**	**ONNX+TensorRT**	✓	✓	✓

Legend: Acc.=Accuracy; Prec.=Precision; Rec.=Recall; F1=F1-Score; Lat.=Latency; Speed=Speed-up Factor; Red.=Reduction; RT=Real-time (≥30 FPS); Viable=Deployment Viable; Prod.=Production Ready; ✓=Yes/Pass; ×=No/Fail; ○=Marginal/Caution

TABLE III: Smart Contract Transaction Details: Input Parameters and On-Chain Recording Confirmation

Smart Contract Parameters and On-Chain Recording	
Parameter	**Specification / Value / Status**
Function Name	RECORDDETECTION (Active)
Object Type	Detection Input: Bomb (Recorded)
Detection Location	Detection Input: Main Base (Recorded)
Image Hash	Evidence Hash: 12345 (Verified)
Transaction Hash	On-Chain Data: Confirmed
Gas Used	Resource Cost: 141,076 wei (Computed)
Block Hash	Chain Data: Recorded
Block Number	Chain Data: 338982
Logging Status	**Immutable On-Chain Record (Verified)**

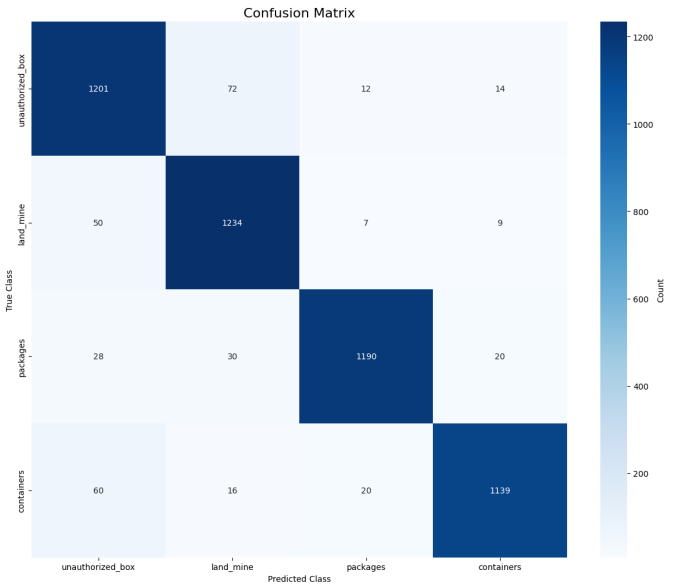

Fig. 5: Confusion Matrix

on 320×320 inputs, satisfying real-time surveillance requirements. Power profiling showed 2.7 W idle and 5.8–6.2 W active consumption, below the 15 W untethered deployment threshold. Thermal testing demonstrated stable operation at 53–60 °C, below the 72 °C throttling threshold. In comparison, Raspberry Pi 4 achieved 25.7 FPS with 6.0–7.0 W power, while Raspberry Pi Zero 2 achieved only 10.5 FPS with 3.5–4.0 W. The 33 ms latency, 30.3 FPS throughput, and 6.2 W peak power consumption demonstrate Raspberry Pi 5 with TensorRT-optimized YOLOv11n provides superior real-time performance for unattended object detection with low energy footprint, validating it as the optimal hardware choice.

C. Pure Chain vs Sepolia Comparison

Figure 6 presents a comparison of blockchain performance between the Pure Chain and the Sepolia in terms of transaction latency and throughput. The experimental results demonstrate that Pure Chain achieves a significantly lower transaction latency of 3.55ms, compared to 12.23ms for Sepolia. This highlights Pure Chain's advantage in rapid transaction finality which is particularly beneficial for time-sensitive military applications. In terms of throughput, Pure Chain processes up to 27 transactions per second that outperforms Sepolia's

TABLE IV: Edge Device Performance Evaluation: Raspberry Pi 5 vs Raspberry Pi 4 vs Raspberry Pi Zero 2

YOLOv11n Deployment Performance Metrics Across Edge Devices				
Performance	**Pi 5**	**Pi 4**	**Pi Zero 2**	**Status**
Inference Latency (320×320)	33 ms	60 ms	110 ms	Pi 5 Fastest
Throughput (FPS)	30.3	25.7	10.5	Only Pi 5 Real-time
Idle Power (W)	2.7	2.5–2.8	1.5–1.8	Pi Zero Lowest
Active Power (W)	5.8–6.2	6.0–7.0	3.5–4.0	Pi Zero 2 Low Power
Operating Temp. (°C)	53–60	58–68	62–70	Pi 5 Cooler
Throttling (°C)	72	76	78	All Safe
Suitability	**Real-time Optimal**	**Near Real-time**	**Low-power but Non-RT**	**Pi 5 Best for for 24/7**

Legend: FPS=Frames Per Second; W=Watts; °C=Celsius; Real-time=≥30 FPS at 320×320

throughput of 9 transactions per second.

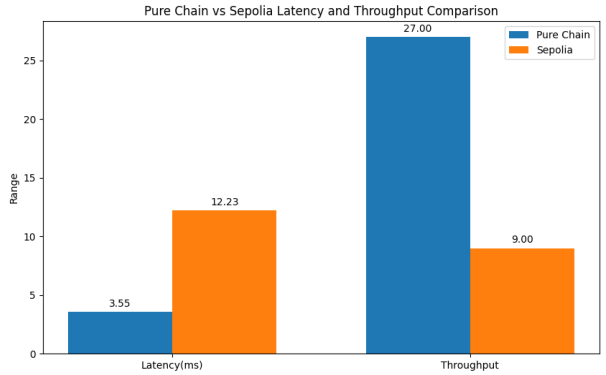

Fig. 6: Pure Chain vs Sepolia Latency and Throughput Comparison

V. Conclusion

This propose framework demonstrates that the YOLOv11n model in edge device achieved better performance. Also, Raspberry Pi 5 outperforms other Raspberry Pi versions and suitable for this framework in latency, FPS and scalability. Combined with the Pure Chain network, this framework ensures fast, secure, and scalable event recording confirming its strong suitability for real-world military applications.

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] D.-S. Kim, E. A. Tuli, I. I. Saviour, M. M. H. Somrat, and X.-Q. Pham, "Blockchain-as-a-service: A pure chain approach," *Blockchain: Research and Applications*, p. 100397, 2025.

[2] 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.

[3] A. S. Gaadhe, B. P. Kumar, R. Baram, P. K. Lendale, B. Darshan, and P. Singh, "A deep learning approach to track real-time objects using yolo and deepsort for next-gen security and surveillance," in *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, pp. 1946–1951, IEEE, 2025.

[4] M. A. Khatun, D.-S. Kim, J. M. Lee, and J.-H. Kim, "Comparison between vision transformer and cnn for ice image classification," , pp. 1822–1823, 2023.

[5] H. Dong, L. Zhang, and B. Zou, "Exploring vision transformers for polarimetric sar image classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 60, pp. 1–15, 2021.

[6] M. E. Hossain, M. T. R. Tarafder, N. Ahmed, A. Al Noman, M. I. Sarkar, and Z. Hossain, "Integrating ai with edge computing and cloud services for real-time data processing and decision making," *International journal of multidisciplinary sciences and arts*, vol. 2, no. 4, pp. 252–261, 2023.

[7] R. Akter, M. Golam, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "Iomt-net: Blockchain-integrated unauthorized uav localization using lightweight convolution neural network for internet of military things," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6634–6651, 2022.

[8] L. Kong, J. Tan, J. Huang, G. Chen, S. Wang, X. Jin, P. Zeng, M. Khan, and S. K. Das, "Edge-computing-driven internet of things: A survey," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–41, 2022.

[9] M. Asiri, N. Saxena, R. Gjomemo, and P. Burnap, "Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective," *ACM transactions on cyber-physical systems*, vol. 7, no. 2, pp. 1–33, 2023.

[10] S. P. Narayanan, M. S. Manikandan, and L. R. Cenkeramaddi, "Deep learning based soldier face detection and counting method for military tactical operations and artificial intelligence powered weapons," in *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, pp. 255–260, IEEE, 2024.

[11] M. Rady, N. Abd El Karim, Y. Maaod, M. Abd Elaziz, A. M. Abdelfattah, Y. M. Elmeligy, A. R. AboZaid, and M. Elsayed, "Advancing real-time military aircraft detection: a comprehensive comparative benchmark of object detection frameworks," in *2025 International Telecommunications Conference (ITC-Egypt)*, pp. 715–720, IEEE, 2025.

[12] K. Liu, A. Li, S. Yang, C. Wang, and Y. Zhang, "Multi-scale attention and boundary-aware network for military camouflaged object detection using unmanned aerial vehicles," *Signal, Image and Video Processing*, vol. 19, no. 2, p. 184, 2025.

[13] J. Yang, S. Deng, F. Zhang, A. Pan, and Y. Yang, "Fatcnet: Feature adaptive transformer and cnn for infrared small target detection," *IEEE Transactions on Aerospace and Electronic Systems*, 2024.

[14] A. Alqahtani, S. Alsubai, A. Alanazi, and M. Bhatia, "Blockchain-based smart monitoring framework for defense industry," *IEEE Access*, vol. 12, pp. 91316–91330, 2024.

[15] A. A. A. Shareef, P. L. Yannawar, Z. A. Ahmed, and A. M. Al-madani, "Applying blockchain technology to secure object detection data," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 874–879, IEEE, 2021.

[16] P. M. Peruman, G. Krishnan, *et al.*, "Blockchain-based deep learning object detection system for enhanced security and reliability," in *2023 International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 1–5, IEEE, 2023.