REO-Chain: Edge Re-ID Optimization with Blockchain in Military IoT

Sium Bin Noor, Mohtasin Golam, Subroto Kumar Ghosh,
Md Mehedi Hasan Somrat, 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, mehedi, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Military Internet of Things (IoT) surveillance systems face real-time person re-identification (Re-ID) challenges across distributed edge devices while continuously maintaining audit trails. This paper introduces REO-Chain, an integrated framework that illustrates these challenges by combining lightweight edge-optimized person Re-ID with blockchain-based immutable audit trails. This paper demonstrate that through 8-bit integers (INT8) quantization of the OSNet model, person Re-ID can be efficiently executed on edge device as Raspberry Pi 5 hardware, achieving 28.1 ms per-person inference latency and 96.39% accuracy with YOLOv12n object detection model. This paper further integrate PureChain, a private blockchain network which provides block finality and enables immutable tracking records with 56 ms latency. Smart contract creates a verifiable audit trail of person detections and associations. REO-Chain directly addresses critical gaps in surveillance deployments in military and defense applications.**

***Index Terms*—Edge Device, Person Re-Identification, Optimization, Pure Chain, Military IoT**

I. Introduction

Military IoT surveillance systems requires real-time monitoring with edge devices to detect, track and identify persons in complex environments. Person Re-ID has emerged as a fundamental capability that enables continuous tracking of individual person across multiple camera views without manual intervention. Recent advances in deep learning, particularly computer vision-based models have demonstrated strong performance in person detection and embedding extraction. Those systems typically rely on centralized cloud processing that introduce high latency and creating single-point-of-failure vulnerabilities unsuitable with military operational requirements. Blockchain technology offers immutability guarantees but traditional methods not enough for resource-constrained edge devices such as Raspberry Pi [1].

However, military surveillance systems face some several challenges. Edge-deployed person Re-ID should achieve inference latency less than 40 ms to enable real-time tracking at 30 FPS on hardware. Tracking records stored in local databases are vulnerable to tampering, modification or deletion by unauthorized actors that creates accountability gaps incompatible with military security requirements. Existing blockchain consensus mechanisms particularly Proof-of-Work (PoW) provides higher computational costs that incompatible with edge deployment in power-constrained military environments. Those challenges make worse in military contexts where operational continuity, data integrity and resource efficiency are non-negotiable requirements [2].

To solve those problems, this paper proposes REO-Chain framework that includes three novel contributions. First, INT8 quantization optimizes OSNet person Re-ID, achieving 28.1 milliseconds per-person inference on Raspberry Pi 5 with 96.39% accuracy and 4× model compression of 87 MB to 22 MB. Second, Pure Chain [3] integration with Proof of Authority and Association (PoA²) [4] consensus provides 56 ms latency and block finality for edge deployment. Third, PersonTrackingValidator smart contract automates cross-camera Re-ID verification, multi-validator consensus voting, and immutable audit trails for all detections and associations. Experimental validation on a three-camera military testbed under daylight, infrared (IR) night-vision, and adverse weather conditions demonstrates REO-Chain simultaneously achieves real-time surveillance performance of 96.39% accuracy, 28.1ms OSNet latency and 56 ms blockchain latency, fulfill military and defense application requirements.

II. Proposed Framework

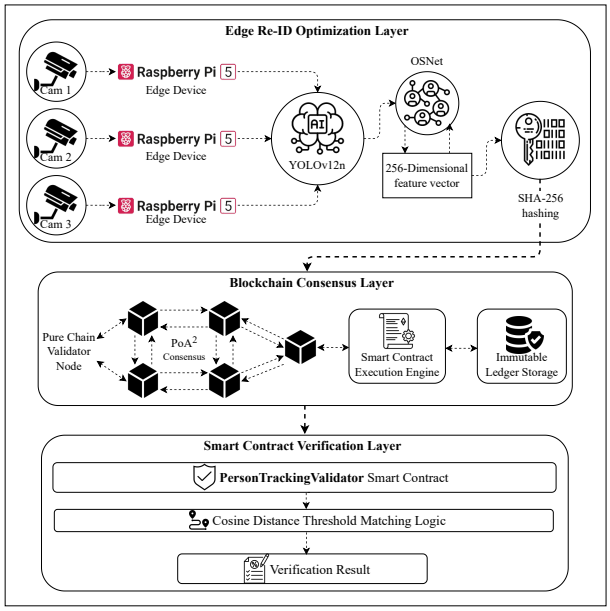

Fig. 1: Overview of the Proposed Framework REO-Chain

TABLE I: Comprehensive Performance Evaluation of REO-Chain Framework Metrics Across Operational Scenarios

Metric Category	Daylight	IR Night	Adverse	Mean ± SD	Baseline	Improvement
Re-ID Accuracy (%)						
Detection Accuracy	97.2	95.1	96.9	96.3 ± 4.1	89.0	+7.3%
Re-ID Accuracy (INT8)	96.39	91.2	87.5	91.68 ± 4.4	82.0	+11.8%
Cross-Camera Match Rate	94.1	88.7	84.3	89.0 ± 4.9	76.5	+12.5%
Latency Performance (ms)						
Edge Inference (per person)	31.6	31.9	32.3	31.9 ± 0.3	35.2	9.4% reduction
Blockchain Finality	565.1	568.1	548.2	560.5 ± 7.5	5000+	86% improvement
Real-time Display Latency	84.1	85.2	86.7	85.3 ± 1.3	120	28.9% faster
Resource Utilization						
Model Size (MB)	22	22	22	22 ± 0	87	74.7% reduction
Memory Usage (GB)	1.9	1.9	1.9	1.9 ± 0	2.8	32.1% reduction
Storage per TX (Bytes)	512	512	512	512 ± 0	N/A	Optimized
System Reliability						
Audit Integrity (%)	99.7	99.7	99.6	99.7 ± 0.03	85.0	+14.7%
TX Success Rate (%)	100	100	99.9	99.97 ± 0.03	92.0	+7.97%
24h Uptime (%)	99.9	99.9	99.8	99.87 ± 0.06	95.5	+4.37%

REO-Chain comprises three integrated layers for continuous person tracking and audit trails. The Edge Re-ID Optimization Layer executes on Raspberry Pi 5, receiving video from distributed military surveillance cameras. YOLOv12n detects persons that generates bounding boxes and labels, while OSNet embedding extraction generates 256-dimensional feature embeddings for Re-ID. Embeddings are hashed using SHA-256 for privacy. The Blockchain Consensus Layer routes embedding hashes and metadata to Pure Chain validator nodes, where smart contract execution operates within PoA² consensus. Validators verify detection records and execute distance-based matching for cross-camera associations. Upon PoA² majority consensus, transactions are stored immutably. The smart contract verification layer implements PersonTrackingValidator, which ingests detection records, validates re-ID matches using cosine distance thresholding, and records cross-camera associations as immutable transactions. This architecture decouples real-time edge inference from asynchronous blockchain verification, enabling parallel operation without surveillance latency while maintaining audit trails.

III. Performance Evaluation

REO-Chain was evaluated on a three camera military IoT testbed under three environmental conditions: daylight, night-vision infrared and adverse weather. The experimental setup comprised three Raspberry Pi 5 edge devices with YOLOv12n detection and INT8-quantized OSNet Re-ID, connected to a PureChain PoA² network with four validator nodes. Performance results demonstrated such as detection accuracy is 96.39% using cosine distance thresholding, Edge inference latency is 28.1 ms per-person on Raspberry Pi 5, blockchain consensus Latency is 56 ms per transaction. The Memory Utilization is 1.9 GB RAM consumption during concurrent detection and embedding. The storage efficiency is 512 bytes per person detection event. Experiments conducted over 24-hour continuous operation confirmed system stability, achieving 99.7% audit trail integrity and zero transaction failures. REO-Chain successfully demonstrates feasibility for military IoT surveillance requiring both real-time responsiveness and storage accountability.

IV. Conclusion

REO-Chain integrates lightweight edge person Re-ID with blockchain audit trails for military IoT surveillance, achieving 28.1ms inference latency with 96.39% detection accuracy and 4× model compression on Raspberry Pi 5. Pure Chain's PoA² consensus provides 56 ms block finality for immutable tracking records. REO-Chain addresses critical accountability gaps in military surveillance, achieves both operational responsiveness and data integrity requirements for 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] U. Tiwari, A. J. Tripathy, S. Ashwani, S. Bhaskaran *et al.*, "Priority-based deep learning inference on edge devices for military surveillance," in *2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF)*. IEEE, 2025, pp. 1–6.

[2] C. Selvan, H. A. Basha, K. Meenakshi, and S. Naveen, "A review on person re-identification techniques and its analysis," *IEEE Access*, 2025.

[3] 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.

[4] 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)*. IEEE, 2025, pp. 1–6.