International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 08 August-2026 | Impact Factor: 3.5

SENTINEL-X: An Edge-AI Command-and-Control Framework for Real-Time Perimeter Surveillance and Border Security in India

Author Name: **Saurab Singh[1]**
[1]Military College of Telecommunication Engineering, Mhow, India Saurab18singh@gmail.com

How to Cite this Article:

Singh, S. (2026). SENTINEL-X: An Edge-AI Command-and-Control Framework for Real-Time Perimeter Surveillance and Border Security in India. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(8), 1-9. https://doi.org/10.55041/ijcope.v2i8.145

https://doi.org/10.55041/ijcope.v2i8.145

Abstract**—**India guards over 15,106.7 km of land border and 7,516.6 km of coastline across terrain ranging from Himalayan glaciers to riverine floodplains, a diversity that limits the effectiveness of physical fencing and manual patrolling alone. This paper presents SENTINEL-X, a prototype edge-artificial-intelligence (edge-AI) command-and-control (C2) gateway that fuses commodity camera feeds, a YOLOv8-based object-detection pipeline, and an automated alert-dispatch chain into a single tactical dashboard for perimeter monitoring. The design is contextualised against India's Comprehensive Integrated Border Management System (CIBMS) and the Border Electronically Dominated QRT Interception Technique (BOLD-QIT), and is compared with analogous smart-border programmes in the United States, Israel, and the European Union. We describe the system architecture, implementation choices, and the constitutional and statutory constraints on state surveillance under the Puttaswamy judgment and the Digital Personal Data Protection Act, 2023. The paper concludes that edge-AI perimeter systems can materially reduce detection-to-response latency, but only as an augmentation of — not a substitute for — trained personnel, physical infrastructure, and statutory oversight.

Index Terms**—***border security, computer vision, edge computing, object detection, YOLO, surveillance systems, unmanned aerial vehicle detection, data privacy.*

I. INTRODUCTION

Border security has historically rested on three pillars: physical infrastructure such as fencing, floodlighting and roads; standing manpower at Border Out Posts (BOPs); and human intelligence. India's land frontier spans seven neighbouring countries and traverses an unusually wide range of terrain, from the high-altitude glaciated stretches of Ladakh to the arid Thar desert and the braided river channels of the Brahmaputra along the border with Bangladesh [1]. Each terrain type defeats a uniform physical-barrier strategy in a different way, and adversaries have adapted accordingly: infiltration under cover of winter fog, boat crossings through unfenceable riverine gaps, and, increasingly since 2019, the use of small commercial drones to smuggle narcotics and weapons across the western border without approaching the fence line at all [2], [3].

Artificial intelligence changes the economics of this problem. Computer-vision models can monitor many camera feeds concurrently without fatigue, and edge computing allows that inference to run physically at the outpost rather than in a distant data centre, which matters where backhaul bandwidth is limited or intermittent [4]. This paper makes three contributions. First, it documents the evolution and current state of India's principal technology-led border programmes — CIBMS and BOLD-QIT — as the operational context for AI-assisted perimeter defence. Second, it presents SENTINEL-X, a working prototype that demonstrates a full detection-to-dispatch pipeline built from commodity hardware and open computer-vision models. Third, it examines the system against the constitutional and statutory limits on state surveillance in India, an aspect frequently omitted from purely technical treatments of this problem.

The remainder of this paper is organised as follows. Section II reviews related work and existing government programmes. Section III describes the SENTINEL-X architecture. Section IV details the implementation. Section V discusses observations, an international comparison, and identified limitations. Section VI addresses legal and ethical considerations. Section VII concludes with directions for future work.

II. RELATED WORK

A. India's Integrated Border Management Programmes

The Comprehensive Integrated Border Management System (CIBMS) originated from a 2012 Ministry of Home Affairs Expression of Interest and a subsequent 2014 Border Security Force (BSF) report, but implementation was not sanctioned until after the January 2016 terrorist attack on the Pathankot Air Force Station exposed gaps in an unfenced approach route [5]. Following recommendations of the Madhukar Gupta Committee, two pilot stretches — approximately 10 km on the India-Pakistan border in Jammu and 61 km on the India-Bangladesh border in Dhubri, Assam — were completed and formally inaugurated in March 2019 [6], [7]. CIBMS integrates thermal imagers, battlefield surveillance radars, fibre-optic and seismic intrusion sensors, day/night pan-tilt-zoom cameras, and a three-dimensional GIS layer into a single command-and-control picture [1], [8]. Its riverine-specific variant, the Border Electronically Dominated QRT Interception Technique (BOLD-QIT), was purpose-built for the Brahmaputra's braided channels, where the BSF guards a 4,096 km frontier that cannot be physically fenced [7], [9].

B. The Emerging Drone Threat

Since approximately 2019, smuggling networks operating from across the western border have increasingly used small quadcopters carrying payloads of a few hundred grams to drop narcotics, weapons and cash deep inside Indian territory, bypassing ground-based defences entirely [2]. Official figures placed before Parliament recorded 53 drone-smuggling incidents in Punjab between 2020 and mid-2023, rising to 294 drones seized in Punjab in 2024 alone, and 278 rogue drones intercepted nationwide in 2025 [3], [10], [11]. In response, the BSF established a dedicated drone-forensics laboratory in Amritsar, which had examined more than 200 recovered drones by 2025, and the Punjab state government separately approved approximately ₹51.4 crore for nine anti-drone units across its six border districts [12], [13].

C. Comparable International Programmes

India's approach parallels "smart wall" programmes elsewhere. The U.S. Customs and Border Protection agency has deployed Integrated Fixed Towers combining radar and long-range cameras along stretches of its southwest border, in several cases using Israeli defence-industry technology [14]. Israel's own layered smart-fence systems combine cameras, radar, motion sensors and, in some deployments, remote-operated response systems, and have been exported through Frontex contracts to the European Union [14], [15]. Notably, Israeli military commentary on the Gaza-perimeter smart fence has warned that heavy reliance on remote sensors, absent continued physical observation by troops, can produce a false sense of security [16] — a caution directly relevant to any AI-heavy border deployment.

D. Edge Computer Vision

The YOLO ("You Only Look Once") family of object detectors, introduced by Redmon et al. [17], treats detection as a single regression problem, predicting bounding boxes and class probabilities in one forward pass. This design underlies its suitability for real-time video analysis on resource-constrained hardware. Subsequent benchmarking on NVIDIA Jetson-class edge accelerators reports YOLOv8 inference at roughly 10–30 frames per second on HD video depending on model variant and board [4], [18], which is the performance envelope this paper assumes rather than independently reproduces.

III. PROPOSED SYSTEM: SENTINEL-X ARCHITECTURE

A. System Overview

SENTINEL-X is structured as four cooperating modules: a multi-camera registry and streaming gateway, a per-camera edge-inference engine, a real-time command-and-control (C2) telemetry channel, and an automated tactical-dispatch module. Fig. 1 summarises the data flow. Cameras are registered dynamically against a FastAPI backend, which exposes REST endpoints for adding, removing and toggling camera sources without restarting the service.

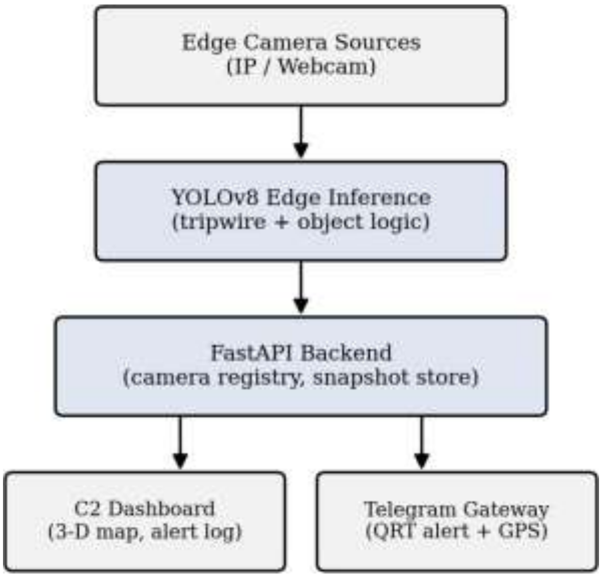

Fig. 1. SENTINEL-X system architecture and data flow.

B. Edge Inference Engine

Each active camera is processed in an independent thread running a YOLOv8n model. A configurable virtual tripwire line is drawn across the frame, and detections belonging to a human-class label that cross within a threshold distance of that line, subject to a minimum re-alert interval, trigger an intrusion event. A second detection path tracks candidate abandoned-object classes (bags, suitcases, packages) against a spatial grid; an object stationary beyond a duration threshold is flagged as unattended and, if the condition persists, raises a separate alert.

C. Command-and-Control Telemetry

A WebSocket endpoint distributes three categories of event — confirmed threat alerts, camera-registry state changes, and detection-engine status — to every connected dashboard session simultaneously, so that operators share a single, consistent operating picture, mirroring the unified command-and-control principle used in CIBMS [1].

D. Automated Tactical Dispatch

On a confirmed detection, the system packages the threat class, model confidence, camera identifier, sector, GPS coordinates and timestamp into a structured message and pushes it to a Quick Reaction Team (QRT) channel through the Telegram Bot API, alongside an evidentiary snapshot saved to disk for later review.

IV. IMPLEMENTATION

The backend is implemented in Python using the FastAPI framework, with an in-memory camera registry, an MJPEG re-streaming endpoint per camera, and a WebSocket manager that maintains the set of active dashboard connections. The edge-inference engine uses OpenCV for frame acquisition and the Ultralytics YOLOv8 implementation for detection, with one

Python thread per active camera to allow independent start/stop control. Detected frames are annotated with the tripwire line, bounding boxes, and unattended-object timers before being re-encoded and posted back to the backend for live viewing.

Reviewing the prototype for this paper surfaced two implementation issues worth recording for completeness. The Telegram bot token is currently embedded directly in the backend source rather than loaded from an environment variable or secrets manager, and Cross-Origin Resource Sharing (CORS) is configured to permit all origins with credentials enabled. Both are acceptable for local demonstration but must be remediated — via externalised secrets and an origin allow-list — before any networked or field deployment.

V. OBSERVATIONS AND DISCUSSION

A. Comparative Positioning

Table I situates SENTINEL-X's design principles against the government programmes and international systems reviewed in Section II. The comparison is included for context; it is not a claim of equivalent scale, maturity, or operational deployment.

TABLE I
Comparative Approaches to AI-Assisted Border Surveillance

System	Core Approach
CIBMS / BOLD-QIT (India)	Multi-sensor fusion (thermal, radar, fibre-optic) for unfenceable terrain
CBP Virtual Wall (USA)	Integrated Fixed Towers: radar + long-range cameras
Smart Fence (Israel)	Layered cameras, radar, and in some cases remote weapon stations
Frontex (EU)	Contracted aerial / maritime surveillance
SENTINEL-X (this work)	Commodity cameras + edge YOLOv8 + automated QRT dispatch

B. Motivating Threat Data

Fig. 2 plots officially reported drone-interception counts that motivate the counter-drone direction of future work (Section VII). These figures span different scopes and time windows — a cumulative multi-year state figure and two single-year counts of differing geographic scope — and are presented together only to illustrate the scale of escalation, not as a continuous single-series trend.

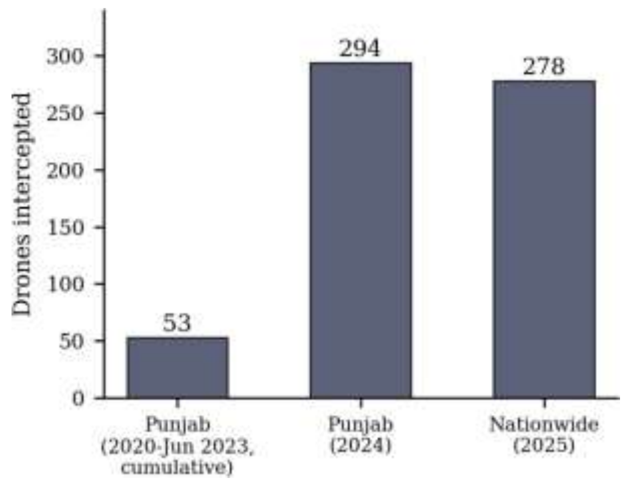

Fig. 2. Officially reported drone-smuggling interceptions along India's western border [3], [10], [11].

C. Limitations

Several limitations qualify the present work. First, SENTINEL-X has been evaluated only functionally, on local webcam and IP-camera streams, and has not been benchmarked under field conditions such as extended fog, monsoon rain, or dust; the FPS figures cited for Jetson-class hardware in Section II-D are literature-reported values for the underlying model family, not measurements taken on this system in a fielded setting. Second, the tripwire and abandoned-object heuristics are class-based and threshold-driven, and are consequently susceptible to false positives from animals, foliage motion and lighting changes, a known failure mode of heavily sensored perimeter systems. Third, the system addresses only camera-based intrusion detection and does not, in its current form, incorporate radar or radio-frequency sensing, which is necessary for the drone threat discussed in Section II-B and V-B.

VI. LEGAL, ETHICAL, AND PRIVACY CONSIDERATIONS

Any camera-based system operating near populated border areas will capture images of Indian citizens as well as potential infiltrators, bringing it within the scope of India's privacy jurisprudence even where its stated purpose is national security. In Justice K.S. Puttaswamy (Retd.) v. Union of India [19], a nine-judge Supreme Court bench held that the right to privacy is a fundamental right under Article 21 of the Constitution, subject to a proportionality standard requiring legality, a legitimate aim, necessity, and proportionality. Legal commentary has noted that Section 17 of the Digital Personal Data Protection Act, 2023 grants broad exemptions to state agencies for purposes connected to sovereignty and security, substantially narrowing the Act's practical reach over systems such as CIBMS or a future SENTINEL-X-class deployment [20], [21]. A private member's Facial Recognition Technology (Regulation of Police Powers) Bill, pending since 2023, would require prior magisterial approval for police use of facial recognition, but remains unenacted [22].

Consistent with these constraints, we recommend four design safeguards for any operational successor to this prototype: (i) data minimisation, retaining full-resolution video only as long as operationally necessary; (ii) purpose limitation, restricting use strictly to the sanctioned perimeter-defence task; (iii) a human-in-the-loop dispatch model, in which an operator confirms a detection before a QRT is scrambled; and (iv) an independent audit and grievance mechanism, consistent with recommendations from NITI Aayog's Responsible AI framework [21].

VII. CONCLUSION AND FUTURE WORK

This paper described SENTINEL-X, a prototype edge-AI command-and-control gateway for perimeter surveillance, and situated it within India's CIBMS/BOLD-QIT programmes and comparable international smart-border systems. The prototype demonstrates that a complete detection-to-dispatch pipeline — camera ingestion, edge object detection, real-time telemetry, and automated QRT alerting — can be assembled from commodity hardware and open computer-vision models. However, the analysis in Sections V and VI indicates that the more consequential open problems are not purely technical: closing the statutory oversight gap identified in Section VI, hardening the security posture noted in Section IV, and adding non-optical sensing (radar/RF) for the drone threat characterised in Section V-B are prerequisites for any move beyond a demonstrator. Future work will pursue thermal-optical sensor fusion for all-weather operation, radar/RF integration for counter-drone detection, and an offline mesh-synchronisation layer so that command-and-control telemetry survives wide-area-network outages between outposts.

REFERENCES

[1] Ministry of Home Affairs, Government of India, "Border Management-I Division," [Online]. Available: https://www.mha.gov.in/en/divisionofmha/border-management-i-division

[2] Khalsa Vox, "Explainer: Why Punjab Is Deploying Anti-Drone Systems Along the Pakistan Border," May 2025. [Online]. Available: https://khalsavox.com/featured/why-punjab-is-deploying-anti-drone-systems-along-the-pakistan-border

[3] Press Information Bureau, Ministry of Home Affairs, "Smuggling of Arms and Narcotics," Aug. 2023.

[4] DFRobot, "YOLO Model and Edge Computing: The Future of Real-Time Object Detection," 2024. [Online]. Available: https://www.dfrobot.com/blog-13843.html

[5] Manohar Parrikar Institute for Defence Studies and Analyses, "Comprehensive Integrated Border Management System: Issues and Challenges," Issue Brief, 2025.

[6] Press Information Bureau, Ministry of Home Affairs, "Union Home Minister Launches Smart Fencing on Indo-Bangladesh Border," Mar. 2019.

[7] Press Information Bureau, Ministry of Home Affairs, "Shri Rajnath Singh to Inaugurate BOLD–QIT Project Along International Border in Dhubri, Assam," Mar. 2019.

[8] Observer Research Foundation, "Comprehensive Integrated Border Management System: Implementation Challenges," 2024.

[9] IndiaAI, Ministry of Electronics and Information Technology, "Border Electronically Dominated QRT Interception Technique (BOLD-QIT)," [Online]. Available: https://indiaai.gov.in/government/ministry-of-home-affairs

[10] The Print (PTI), "BSF Seized 294 Drones in Punjab in 2024: Govt Tells Lok Sabha," Mar. 2025.

[11] The Tribune, "BSF Integrating New Technologies to Strengthen Anti-Infiltration, Anti-Smuggling Grid in Punjab, Jammu Sectors," 2025.

[12] All India Radio News, "Punjab Launches 'Baaj Akh' Anti-Drone System to Curb Cross-Border Drug Smuggling," Aug. 2025.

[13] K. B. S. Sidhu, "Punjab's Strategic Leap in Border Security: Anti-Drone Systems to be Deployed," May 2025.

[14] Israel Trade and Economic Office, "Israel Border Security Technology: Smart Walls and All," 2022.

[15] Nexdigm, "Israel Border Security Market Outlook to 2035," Market Research Report, 2026.

[16] The Upheaval, "Hard Lessons from Israel's High-Tech Border Failure," Oct. 2023.

[17] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2016, pp. 779–788.

[18] Zbotic, "YOLO Object Detection on Jetson Nano: Setup and Demo," 2026. [Online]. Available: https://zbotic.in/yolo-object-detection-on-jetson-nano-setup-and-demo

[19] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, AIR 2017 SC 4161, Supreme Court of India.

[20] Software Freedom Law Centre India, "Analysis of the Facial Recognition Technology-Enabled Surveillance Landscape in India," 2024.

[21] amLegals, "Facial Recognition in India: Privacy, Surveillance and the Need for Regulation," 2026.

[22] Bar and Bench, "Why India Must Pass the Pending Facial Recognition Technology Bill," 2026.