IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155207

A Literature Survey on AI-Based Secure Border Intrusion Detection Systems Using Deep Learning, IoT, and Encrypted Communication

Dakshayini G R[1], Manya BM[2], Meghana KJ[3], Rida Shariff[4], Sneha GK[5]

Assistant Prof., Dept of CSE, K.S.School of Engineering & Management, Bengaluru, India[1]

Student., Dept of CSE, K.S.School of Engineering & Management, Bengaluru, India[2-5]

Abstract: Border intrusion detection is a highpriority national security concern, as unauthorized crossings can facilitate smuggling, trafficking, and terrorism. Conventional surveillance systems relying on continuous human monitoring are limited by operator fatigue, delayed response, and degraded performance under poor environmental conditions such as fog, rain, and low light. This paper presents a literature survey of five recent studies that address AIdriven solutions for border and perimeter security, covering deep learning-based object tracking, hybrid encryption for secure image transmission, integrated surveillance pipelines, machine learning for wireless sensor network protection, and drone-based real-time monitoring. The survey critically analyses the advantages and limitations of each approach and proposes a conceptual integrated framework that combines multi-modal sensing, lightweight deep learning models, and encrypted communication for more reliable and efficient border surveillance.

Keywords: Border security, deep learning, YOLO, DeepSORT, object detection, encryption, IoT, wireless sensor networks, drone surveillance, intrusion detection.

I. INTRODUCTION

Border regions represent some of the most sensitive and challenging security environments worldwide. Unauthorized intrusions along national borders can enable illegal immigration, smuggling of contraband, human trafficking, and terrorist infiltration, all of which pose direct threats to national safety and sovereignty [1]. Governments and defence organizations therefore require surveillance systems capable of providing continuous, accurate, and real-time monitoring of large and often geographically difficult border areas.

Traditional surveillance methods predominantly depend on human operators who continuously monitor camera feeds and coordinate ground patrols. However, this approach is inherently constrained by human limitations. Operators monitoring multiple video streams over extended durations are susceptible to fatigue, distraction, and delayed reaction, which increase the probability of missing critical intrusion events [2]. Moreover, conventional camera-based systems frequently fail to deliver reliable performance under adverse environmental conditions such as fog, heavy rain, snowfall, smoke, and nighttime low-visibility scenarios, where image quality degrades significantly. In response to these shortcomings, there has been growing research interest in automated, AI-driven surveillance systems that can reduce dependency on human monitoring while improving detection accuracy, response speed, and communication security. Technologies such as deep learning, computer vision, machine learning, Internet of Things (IoT), and cryptographic encryption collectively offer powerful tools for constructing more intelligent and robust border surveillance solutions. This survey reviews five recent research contributions that represent different but complementary layers of this problem. The first paper proposes a real-time multi-object tracking architecture using YOLO and DeepSORT. The second examines hybrid encryption for the secure transmission of dynamic surveillance images. The third presents a comprehensive deep learning pipeline for integrated image and video surveillance. The fourth addresses machine learning-based intrusion detection in wireless sensor networks. The fifth demonstrates a drone-assisted border monitoring system with CNN-based classification and IoT integration. Together, these works cover detection, transmission security, behavioural analysis, network protection, and mobile surveillance — the key functional layers of a modern border security architecture.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155207

II. DEEP LEARNING FOR REAL-TIME OBJECT TRACKING

Gaadhe et al. [2] propose a real-time surveillance and tracking architecture that integrates two complementary deep learning components: YOLO (You Only Look Once) for object detection and DeepSORT (Deep Simple Online and Realtime Tracking) for multi-object tracking. The system is designed to identify and continuously follow humans, vehicles, and drones across consecutive video frames in dynamic surveillance environments.

The pipeline encompasses data acquisition, video preprocessing, YOLO-based per-frame object detection, feature extraction using appearance descriptors, and DeepSORT-based identity association across frames using motion prediction and reidentification. The combined approach is intended to address challenges such as target occlusion, rapid motion, and varying illumination conditions that commonly degrade traditional tracking methods including Kalman filters and optical flow techniques.

The system achieves high tracking accuracy with a Multiple Object Tracking Accuracy (MOTA) of approximately 78.6% and operates at real time processing speeds of around 45 frames per second. It demonstrates strong performance under low-light conditions and partial occlusion scenarios, which are particularly relevant for border surveillance at night or in dense environments.

The primary limitation of this approach is its significant dependence on high-performance GPU hardware, which restricts practical deployment in resource-constrained edge environments such as remote border outposts or lightweight airborne platforms. Additionally, the system may show reduced generalization on unseen or geographically diverse datasets, and it does not natively incorporate mechanisms for secure data transmission or privacy protection.

III. HYBRID ENCRYPTION FOR SECURE IMAGE TRANSMISSION

Raman et al. [3] address a distinct but critical aspect of surveillance infrastructure: the protection of visual data during wireless or internet based transmission. In border monitoring deployments, surveillance video and images are routinely transferred across potentially insecure communication channels, creating vulnerability to interception, unauthorized access, and data manipulation.

The authors propose a hybrid cryptographic framework that combines RSA (Rivest–Shamir–Adleman) asymmetric encryption with AES (Advanced Encryption Standard) symmetric encryption operating in CBC (Cipher Block Chaining) mode. In this design, RSA is employed exclusively for secure key exchange, while AES handles the bulk encryption of image data. Images are divided into parallel processing blocks to reduce encryption latency and improve throughput for real-time communication scenarios.

The hybrid approach exploits the complementary strengths of both algorithms: RSA provides robust key distribution security without the key management vulnerabilities of purely symmetric schemes, while AES delivers computationally efficient encryption suitable for large visual data volumes. The system demonstrates strong resistance to cryptographic attacks, reduced end-to-end encryption time compared to standalone RSA, and suitability for real-time transmission pipelines.

The RSA key generation and exchange operations introduce nontrivial computational overhead that scales with image size, which may impact latency in high-throughput surveillance environments. The system also requires careful and secure key management infrastructure, and its scope is entirely confined to data security during transmission. It does not contribute any intrusion detection, classification, or behavioural analysis capabilities, and therefore functions as a supplementary security layer rather than a standalone surveillance solution.

IV. DEEP LEARNING SURVEILLANCE PIPELINES

Sudha et al. [4] present a comprehensive AI-driven surveillance framework that goes beyond single-function detection by integrating object detection, anomaly detection, behavioural analysis, and privacy-preserving processing into a unified pipeline. The architecture employs a hybrid deployment strategy, with edge devices performing initial low-latency processing and cloud servers handling computationally intensive analytics.

The framework employs CNN-based architectures, YOLO for object detection, Vision Transformers (ViT) for contextual scene understanding, and Recurrent Neural Networks (RNNs) for temporal behavioural analysis. The system is designed to detect a range of security-relevant events including unauthorized zone entry, abandoned object detection, and other

DOI: 10.17148/IJARCCE.2026.155207

anomalous activities. Data anonymization techniques are applied prior to storage and sharing to address privacy concerns inherent in largescale surveillance operations.

The system achieves high detection precision of 97.5%, a recall of 96.3%, and an F1-score of 96.9%, with an inference latency of approximately 15 milliseconds. The combination of edge and cloud processing balances real-time responsiveness with analytical depth. Privacy-preserving anonymization reflects growing ethical and regulatory requirements in surveillance system design, making this framework more suitable for civilian and smart-city deployments alongside security applications.

The framework demands substantial computational resources, including GPU or TPU support, which limits its direct applicability in low infrastructure border environments. Deep neural network models of this complexity are also susceptible to adversarial perturbations — deliberately crafted inputs that can mislead the model into incorrect classifications. The complexity of model training and multi-component integration further increases deployment and maintenance difficulty in field conditions.

V. MACHINE LEARNING FOR WIRELESS SENSOR NETWORK SECURITY

Overview Saranya et al. [5] shift focus from visual surveillance to the security of the communication infrastructure that underlies modern border monitoring systems. Wireless Sensor Networks (WSNs) are widely deployed in surveillance contexts due to their ability to provide distributed, low-power environmental monitoring. However, their open communication protocols and resource-constrained node architectures make them highly susceptible to cyber-attacks, including denial-of-service, data injection, and packet manipulation attacks.

The authors apply a suite of machine learning classifiers — including Random Forest, Decision Trees, Support Vector Machines, and Neural Networks — to the problem of network intrusion detection. A simulation environment built on OMNeT++ is used for dataset generation. Traffic features including packet size, transmission frequency, protocol type, and data rate are extracted and used to train models to distinguish malicious activity from normal network behaviour. The Random Forest classifier is identified as the primary model due to its favourable balance of accuracy and computational efficiency.

The proposed system achieves an intrusion detection accuracy exceeding 95% with a false positive rate below 5%. The Random Forest approach demonstrates strong scalability, adaptive learning capability, and energy efficiency that is appropriate for the resource-constrained nodes typical of deployed WSN environments. The system provides a valuable defensive layer for the network infrastructure that supports surveillance data collection and transmission.

The scope of this work is confined to network-layer anomaly detection through traffic analysis. It does not interpret visual events, classify physical objects, or contribute directly to intrusion detection in the physical environment. The system also faces challenges in handling continuously evolving attack patterns without model retraining, and its performance is sensitive to the quality and representativeness of the training dataset. It is therefore best understood as a complementary network security layer rather than a complete border surveillance solution.

VI. DRONE-BASED BORDER MONITORING WITH IOT

Overview Siddique et al. [6] present a mobile, drone-assisted border surveillance system that addresses a key limitation of fixed camera approaches: the inability to cover large, geographically irregular, or rapidly changing border areas. Their platform integrates cameras, GPS modules, IoT communication devices, and a CNN based image classifier to provide real-time aerial monitoring with automatic identity classification and location tagged alerting.

The system captures aerial images using drone-mounted cameras and processes them through a custom-trained CNN model to classify detected individuals as either border guards or unauthorized civilians, primarily based on clothing and uniform patterns. GPS coordinates are linked to each detection event, and IoT integration enables real-time transmission of images, classification results, and location data to central monitoring authorities through server and cloud platforms.
The CNN classifier achieves approximately 98% classification accuracy on the custom dataset. Drone-based deployment provides significant advantages in coverage flexibility, enabling rapid surveillance of areas that are difficult or dangerous for ground patrols. IoT integration supports real-time data relay and alert generation, making the system suitable for fast-response security applications in remote or expansive border regions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155207

The system's performance is notably sensitive to environmental conditions, with image quality degrading significantly under rain, fog, dust, or low-light scenarios. Drone endurance is constrained by battery capacity, limiting continuous coverage duration. The classification logic relies heavily on clothing-based visual cues, which may be insufficient or unreliable in diverse operational settings where individuals may not present clear distinguishing attire. Privacy and ethical concerns related to aerial surveillance are also noted.

VII. COMPARATIVE ANALYSIS

Table I. Comparative Summary of Reviewed Papers

Aspect	Paper 1 [2]	Paper 2 [3]	Paper 3 [4]	Paper 4 [5]	Paper 5 [6]
Primary Focus	Object detection& tracking	Secure image transmission	Integrated surveillance pipeline	WSN network security	Dronebased monitoring
AI/ML Used	Yes (YOLO, ,DeepSORT)	No	Yes (CNN, ViT, RNN)	Yes (Rando m Forest, SVM)	Yes (CNN)
IoT Integration	No	No	Partial	Yes (WSN)	Yes
Data Security	No	Yes (AES + RSA)	Partial (anonymization)	No	No
Weather Robustness	Partial	N/A	Partial	N/A	Limited
Edge Suitability	Limited (GPU-heavy)	Good	Partial	Good	Partial
Privacy Consideration	No	Yes	Yes	No	Limited

A cross-cutting pattern emerges from the comparison: performance improvements in one dimension are frequently accompanied by trade-offs in another. Deep learning models achieve high detection accuracy but demand substantial computational resources. Encryption secures data in transit but adds processing overhead and contributes nothing to physical threat detection. Drone platforms expand spatial coverage but remain limited by battery life, environmental sensitivity, and narrow classification logic. Network-layer machine learning strengthens communication infrastructure but lacks any capacity to interpret physical events. This suggests that future border surveillance architectures should be designed as integrated, layered systems rather than isolated functional modules.

VIII. RESEARCH GAPS AND CHALLENGES

Reviewing the five studies collectively reveals several persistent research gaps that motivate continued work in this area.

Multi-Modal Sensing: Most reviewed systems rely predominantly on visual sensing through standard cameras. This creates a fundamental vulnerability to poor lighting, fog, rain, and other visibility-degrading conditions. Only the drone-based system partially addresses this by its aerial vantage, but it remains camera-dependent. Integration of passive infrared (PIR) sensors, thermal cameras, LiDAR, acoustic detectors, and radar would provide more resilient, all-weather detection capability.

Incomplete Security Coverage: Despite surveillance data being highly sensitive, only one of the five papers explicitly addresses secure transmission. The remaining four systems transmit data without discussion of encryption, authentication, or protection against interception and tampering, leaving significant security gaps in proposed deployments.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155207

Computational Constraints: Several high-accuracy systems are practically limited by their reliance on powerful GPU infrastructure. For deployment in remote border regions, on drone platforms, or in distributed IoT nodes, lightweight model architectures using techniques such as pruning, quantization, and knowledge distillation are essential but insufficiently explored in the reviewed work.

False Alarm Management: Systems generating excessive false positives risk eroding operator trust and may result in genuine threats being ignored. None of the reviewed papers propose robust multi-evidence confidence fusion mechanisms specifically designed to suppress false alarms under challenging real-world conditions.

Privacy and Ethics: Only one paper explicitly incorporates data anonymization. As surveillance systems inevitably capture individuals who pose no threat, the absence of privacy-preserving design raises serious ethical and regulatory concerns that the research community has not yet adequately addressed.

IX. PROPOSED CONCEPTUAL FRAMEWORK

Based on the analysis of the reviewed literature and the identified gaps, a conceptual framework for a more comprehensive border intrusion detection system is proposed. This framework is intended to guide the development of the proposed project and is presented here at a high level without implementation details.

The sensing layer should integrate RGB cameras, passive infrared sensors, and acoustic detectors to provide robust, multimodal detection capability across varying environmental and lighting conditions. This multi-sensor approach reduces the single-point-of-failure risk inherent in camera-only systems. The processing layer should employ a lightweight YOLO-based object detector optimized through pruning and quantization for edge deployment, combined with DeepSORT for consistent identity tracking across frames.

Machine learning classifiers such as Random Forest can provide supplementary behavioural analysis and sensor fusion. The communication and security layer should implement a hybrid AES-RSA encryption scheme for all outgoing surveillance data, alert messages, and authentication traffic, ensuring that sensitive information is protected against interception and manipulation throughout the transmission pipeline.

The alerting layer should incorporate a confidence-based fusion mechanism that aggregates evidence from multiple sensors before triggering alerts, reducing false positives while maintaining high sensitivity to genuine intrusion events. Finally, a privacy protection module should anonymize non-suspect individuals prior to data storage or external sharing, ensuring compliance with ethical and regulatory requirements for surveillance system deployment.

The proposed AI-Based Secure Border Surveillance System is designed to monitor border areas using Artificial Intelligence, IoT devices, and encrypted communication. The system collects real-time data from surveillance cameras, motion sensors, and acoustic sensors. These sensors detect movement, capture video footage, and identify environmental sounds such as footsteps or vehicles. The collected data is combined using a sensor data aggregator and sent as a live data stream for processing. In the AI Processing and Analysis stage, the data undergoes preprocessing techniques such as image enhancement and noise reduction to improve quality.

The YOLOv8 algorithm is used for object detection to identify humans, animals, and vehicles with high accuracy and faster processing speed. After detection, the DeepSORT algorithm tracks the movement of objects across video frames. The classification module further categorizes detected objects, including distinguishing between friendly soldiers and intruders. Behaviour analysis is then performed to identify suspicious activities such as line crossing or unusual movement.

The Decision Engine analyses the processed information and determines whether a threat is present. If suspicious activity is detected, the system generates an alert containing object details, location, timestamp, and captured image or video clip. Finally, the Communication and Response stage securely transmits alerts using AES and RSA encryption through IoT networks such as Wi-Fi, 4G, 5G, or LoRa. The control centre receives the information and enables security personnel to take immediate action. The proposed system improves border security by providing real-time monitoring, intelligent threat detection, secure communication, and rapid response capabilities.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155207

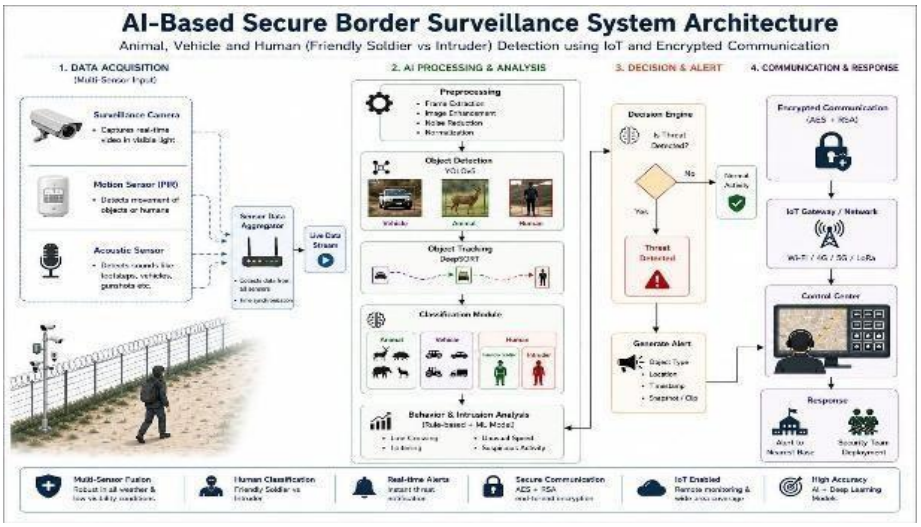

Fig.1 AI-Based Secure Border Surveillance System Architecture

X. CONCLUSION

This survey has reviewed five recent studies addressing AI-driven border intrusion detection from complementary perspectives: real-time object tracking, secure data transmission, integrated surveillance pipelines, wireless sensor network security, and drone-based monitoring. Each study represents a meaningful advancement over conventional manual surveillance, but each also reveals important limitations in robustness, computational efficiency, security coverage, and privacy consideration.

The key finding of this survey is that effective border surveillance cannot be achieved through any single technological approach. Rather, it requires an integrated architecture that unifies visual and non-visual sensing, lightweight deep learning, encrypted communication, and privacy aware design into a coherent system. The proposed conceptual framework reflects these requirements and forms the basis for the development of an AI-Based Secure Border Intrusion Detection and Prevention System with IoT and Encrypted Communication.

REFERENCES

[1]. A. S. Gaadhe, P. K. Lendale, B. P. Kumar, B. R. Darshan, R. Baram, and P. Singh, "A Deep Learning Approach to Track RealTime Objects Using YOLO and DeepSORT for Next-Gen Security and Surveillance," IEEE ICDICI, 2025.

[2]. R. Raman, Y. Farooqui, K. Nisha, and M. Paliwal, "Efficient Encryption Techniques for Secure Transmission of Dynamic Image," IEEE ICKECS, 2025.

[3]. I. Sudha, P. S. Ramesh, S. Narang, Senthilvadivu S., and A. Ponmalar, "Deep Learning for Image and Video Processing in Surveillance Systems: Advancing Security with AI-Driven Insights," IEEE ICCSAI, 2025.

[4]. M. Saranya, S. Srevarshine, V. Sujitha, and T. Sobiya, "Securing Wireless Sensor Networks from Intrusions Using Machine Learning-Based Detection and Response," IEEE ICMSCI, 2025.

[5]. M. A. I. Siddique, M. S. H. Shojol, M. M. Islam, S. Alam, and O. Jyoti, "Smart Border Surveillance: Real-time CNN on Drones with IoT Integration," IEEE ICCIT, 2023.

