AI-Enabled Smart Fence With Edge Processing, Blockchain-Secured, Multi-Layered Intrusion Detection, And Drone Deployment

Devadharshini G
Department of Artificial Intelligence and Data Science
M.Kumarasamy College of Engineering
Karur,India
devadharshinig99@gmail.com

Divya K
Department of Artificial Intelligence and Data Science
M.Kumarasamy College of Engineering
Karur,India
kaliyappandivya1974@gmail.com

Maneesha K
Department of Artificial Intelligence and Data Science
M.Kumarasamy College of Engineering
Karur,India
maneeshakrishnamoorthy@gmail.com

Manisha R
Department of Artificial Intelligence and Data Science
M.Kumarasamy College of Engineering
Karur,India
manisharamachandrant@gmail.com

Saratha M
Department of Artificial Intelligence and Data Science
M.Kumarasamy College of Engineering
Karur,India
saratham.ai@mkce.ac.in

***Abstract*—This paper presents a novel, AI-driven Smart Fence system designed for resilient, real-time perimeter security. This work addresses the critical shortcomings of conventional surveillance, such as high false-alarm rates and network dependencies, by integrating a multi-sensor array with on-site AI processing. The proposed framework leverages lightweight machine learning models at the edge to achieve accurate intrusion classification with a confidence exceeding 95%, ensuring operational autonomy in GPS-denied and internet-free environments. A multi-layered alert system, encompassing discreet signals for personnel and a secure, blockchain-based ledger, guarantees both rapid response and a tamper-proof chain of evidence for post-incident audits. Upon threat validation, the system autonomously deploys a drone for immediate aerial surveillance, providing unparalleled situational awareness without human command. The results demonstrate a significant reduction in response latency and enhanced operational reliability, establishing this system as a superior solution for a new generation of border defense and critical infrastructure protection.**

Keywords — Artificial Intelligence, Edge Computing, Blockchain, Intrusion Detection, Smart Fence, Drone Deployment

I. Introduction

Securing military perimeters and critical infrastructure is an increasingly complex challenge. Traditional surveillance systems passive sensors, fixed cameras, and human patrols are reactive and slow, creating a window of vulnerability during intrusions [2], [6]. These outdated methods compromise situational awareness and fail to counter modern, sophisticated threats.

Environmental and geographical factors further expose the weaknesses of legacy systems. Optical and infrared sensors falter in fog, rain, or sandstorms, while vibration and acoustic sensors trigger false alarms in strong winds [3]. Vast terrains such as forests, mountains, and deserts demand massive manpower, making continuous human surveillance impractical. High false-positive rates desensitize personnel, reducing overall security effectiveness.

Another critical gap lies in reliance on centralized analysis. Most current systems send raw data to remote command centers, introducing latency and depending on fragile network connections [4], [7]. This centralized model slows response, risks cyberattacks, and creates single points of failure. Without decentralized records, tampering is possible, hindering forensic analysis and accountability [8].

To overcome these shortcomings, this paper proposes the AI-enabled Smart Fence. The system integrates real-time AI, edge computing, and blockchain into one autonomous defense framework [1], [5]. By shifting intelligence to the edge, threats are instantly classified and acted upon locally, eliminating dependence on external networks. A multi-layered mechanism fuses data from diverse sensors (thermal, seismic, mmWave radar) for accurate detection, while blockchain-secured logs ensure tamper-proof event records [4], [8].

A key innovation is autonomous drone deployment for aerial surveillance. Once a threat is validated, the system triggers instant alerts, records immutable logs, and dispatches drones for live tracking—without human command [7], [9]. This design reduces false alarms, ensures rapid and verifiable responses, and enhances reliability. The novelty lies in seamlessly combining multi-sensor fusion, edge AI, blockchain security, and drone autonomy into one resilient framework, setting a new benchmark for border defense and critical infrastructure protection..

The key contributions of this paper are as follows:

1. Design and implementation of an AI-driven Smart Fence that combines thermal, seismic, vibration, radar, and visual sensing with lightweight edge-based intelligence.
2. Development of a multi-layered alert mechanism that minimizes false alarms and provides redundant, secure communication of alerts to both local soldiers and the command center.
3. Integration of blockchain logging and autonomous drone response, enabling tamper-proof

979-8-3315-5662-4/25/$31.00 ©2025 IEEE

accountability and rapid situational awareness in military zones.

4. Prototype validation, demonstrating 95% accuracy, <1% false positives, and sub-3 second latency, outperforming traditional and IoT-based solutions.

II. Literature Survey

The Perimeter security has evolved from basic physical barriers to technologically advanced systems. Historically, border defense depended on human patrols and static monitoring solutions, which suffered from fatigue, limited visibility, and poor performance in harsh weather or large terrains [2], [6]. These traditional methods were also prone to circumvention and lacked the speed required for proactive threat response[12].

The introduction of networked electronic systems brought Wireless Sensor Networks (WSNs) as a major step forward. WSNs enabled continuous, automated monitoring while reducing manpower requirements [3]. However, early deployments faced scalability issues, high energy demands, and vulnerability to tampering in remote environments. Moreover, the collected data often lacked intelligence, leading to frequent false alarms caused by environmental factors [5],[10].

Machine learning techniques were later integrated to improve detection accuracy. Algorithms such as support vector machines and decision trees reduced false positives by distinguishing genuine threats from noise [4]. Still, these models relied on centralized processing, introducing latency and dependence on stable connectivity. This centralization created single points of failure, leaving systems exposed to outages and cyber-physical attacks [11].

Recent research has shifted toward decentralized and autonomous solutions. Edge computing and TinyML enable real-time local analysis, minimizing latency and reducing reliance on external networks [7]. Blockchain has also been adopted for tamper-proof event logging, ensuring auditable and immutable records essential for forensic analysis in sensitive environments [8].

Autonomous drones add dynamic surveillance and rapid response capabilities. Equipped with advanced sensors, drones provide real-time situational awareness, track intruders, and assess threats without immediate human input [9]. However, integrating edge AI, blockchain-secured logging, and drone autonomy into one framework remains a challenge. The proposed AI-based Smart Fence System addresses this gap by unifying edge intelligence, immutable blockchain records, and aerial support into a scalable, network-independent solution that enhances detection accuracy, reduces false alarms, and accelerates response times.

III. Proposed System

The proposed system is an AI-enabled smart fence with edge processing, blockchain-secured, multi-layered intrusion detection, and drone deployment. It is designed to overcome the shortcomings of traditional perimeter defense solutions by combining real-time classification, tamper-proof logging, and automated response mechanisms into a unified framework. Unlike conventional surveillance systems that rely heavily on manual monitoring and delayed decision-making, the proposed design emphasizes autonomy and resilience.

The architecture of the system is illustrated in Fig. 1. A distributed sensor network—comprising thermal, infrared, and vibration modules—monitors the perimeter continuously. These sensors are designed for robust operation under adverse conditions such as dust, rain, and extreme temperatures, ensuring uninterrupted performance in diverse environments.

At the core of the system lies the Edge AI Processing Unit, which serves as the local intelligence hub. Using lightweight machine learning models optimized for embedded platforms [7], the unit processes sensor inputs in real time. Its primary task is to distinguish genuine intrusion attempts from false triggers caused by wind, animals, or environmental noise. Once verified with high confidence (greater than 95%), an event is flagged as a potential threat.

Validated intrusions initiate a multi-layered alert system. Immediate on-site deterrence is activated via sirens and warning beacons, while secure radio-based alerts are transmitted to soldiers' handheld devices. For covert operations, stealth-mode infrared alerts are triggered, visible only through night-vision equipment. Simultaneously, every confirmed event is encrypted and recorded in a blockchain-based ledger, ensuring tamper-proof and auditable event storage [8].

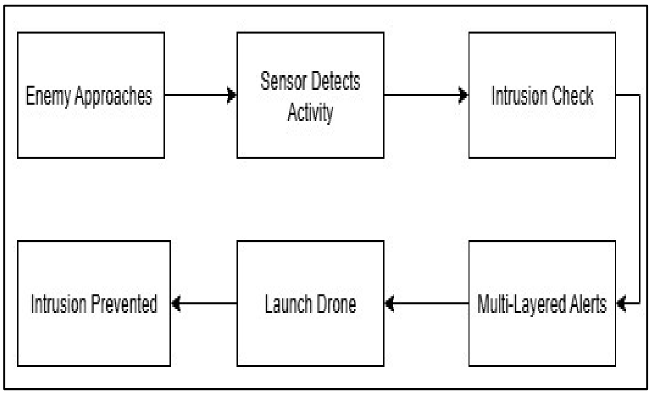

Fig 1. Workflow

The response phase involves coordinated autonomous actions. Drones are deployed to provide aerial surveillance, track intruders, and relay live situational data back to the command center [9]. Automated deterrence measures, such as high-intensity lighting or sonic barriers, can also be activated. Ground troops are notified as the final layer of defense, ensuring rapid human intervention if required. All activities are logged in real time, providing commanders with complete situational awareness.

The integration of edge AI, blockchain, and drone technology results in a system that offers faster response, operational independence, and high resilience against environmental and cyber challenges. Its modular design allows for scalability and adaptation across diverse applications, from border defense to critical infrastructure protection.

A. *System Architecture*

The architecture of the proposed Smart Fence system is a modular and multi-layered framework designed to be both resilient and scalable. The system begins with an enemy approaching the perimeter fence. A network of diverse sensors, including thermal, infrared, and vibration sensors, is positioned along the boundary to continuously monitor for unusual activity. These sensors are specifically designed to withstand harsh environmental conditions such as dust, rain, fog, and extreme temperatures, ensuring reliable performance in any climate.

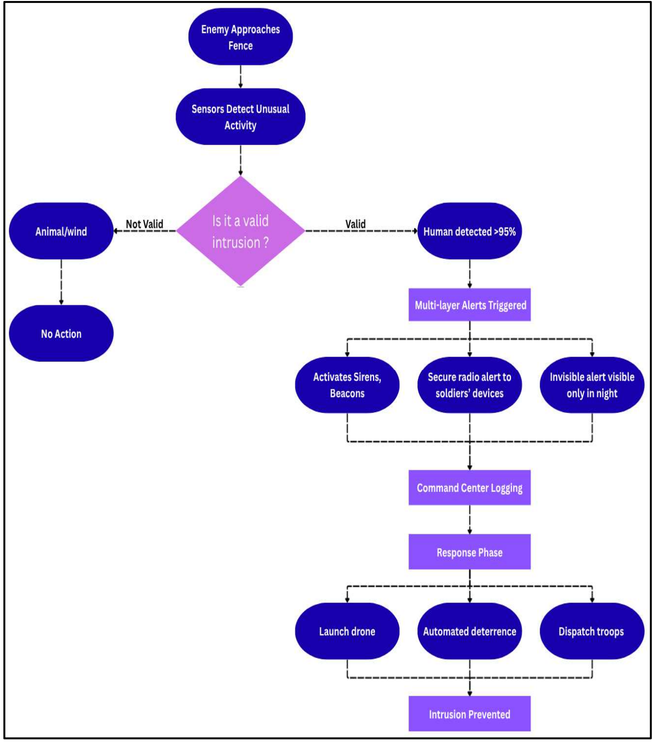
Enemy Approaches Fence
Sensors Detect Unusual Activity
Is it a valid intrusion ?
Not Valid
Valid
Animal/wind
No Action
Human detected >95%
Multi-layer Alerts Triggered
Activates Sirens, Beacons
Secure radio alert to soldiers' devices
Invisible alert visible only in night
Command Center Logging
Response Phase
Launch drone
Automated deterrence
Dispatch troops
Intrusion Prevented

Fig 2. System Architecture

The Edge AI processing unit acts as the central intelligence hub. It collects real-time sensor data and analyzes it locally using lightweight machine learning models to distinguish valid human intrusions from false triggers such as animal movement or environmental disturbances, applying a confidence threshold of over 95 percent. Once a valid intrusion is confirmed, the system immediately initiates a multi-layered logging and alert process. Event data, including the fence sector ID and time of detection, is securely recorded in a blockchain-based ledger for tamper-proof accountability and forensic analysis as illustrated in Fig. 2.

Simultaneously, the system triggers multi-channel alerts for rapid response. These include loud sirens and beacons for visible deterrence, encrypted radio alerts sent directly to soldiers' handheld devices, and covert night-vision signals for stealth operations. The AI processor also coordinates autonomous countermeasures, including drone deployment for aerial tracking, activation of automated deterrence units such as high-intensity lights and sonic barriers, and notifications for troop dispatch. All actions are logged in real time and communicated to the command center, which can intervene or augment the automated response.

Finally, the blockchain-stored intrusion records and system responses are available for post-event analysis, enabling military teams to evaluate response efficiency, detect potential weaknesses, and improve defense strategies. The modular architecture allows scalability, making the system adaptable for border defense, critical infrastructure protection, and isolated high-security zones.

B. Advantages of the Proposed System

High Accuracy: Achieves 95%+ classification accuracy with edge AI and multi-sensor fusion, reducing false alarms.

Real-Time Response: On-device processing enables instant analysis and rapid alerts with drone support.

Operational Independence: Works without internet or GPS, ensuring reliability in remote areas.

Situational Awareness: Secure alerts to soldiers' devices improve coordination and quick response.

B. Challenges and Limitations

Power Constraints: Requires reliable solar/battery backup; drone endurance and weather resistance remain challenges.

Maintenance Needs: Sensors and drones need regular calibration, servicing, and performance monitoring.

Connectivity Issues: Secure channels must resist jamming/cyber-attacks; isolated terrains need hybrid solutions (LoRa, mesh, satellite).

High Initial Cost: Large-scale implementation may be expensive.

IV. Methodology

The AI-Enabled Smart Fence is developed through a systematic approach that integrates multi-sensor detection, intelligent edge AI processing, blockchain-based event logging, and automated response mechanisms. The system's methodology is a layered process, ensuring robust security from initial detection to final response.

To provide clarity on the system's physical and functional components, the following table details the key sensors and their specific roles in the detection phase.

TABLE 1. KEY SENSORS OF THE PROPOSED SYSTEM

Sensor Type	*Function*
Infrared	Monitors unusual activity and provides night-vision capabilities.
Thermal Cameras	Captures the event and detects heat signatures
Vibration Sensor	Detects unusual activity and monitors for vibrations
Motion Detectors	Detects motion.

1. Sensor Deployment

Process: Multiple sensors, including infrared, vibration, motion detectors, and thermal cameras, are strategically embedded along the fence to continuously monitor activity.

Key Technology & Role: These sensors are designed to withstand environmental variations, such as wind, rain, and dust, ensuring uninterrupted detection capability.

2. Edge AI Processing

Process: Sensor data is transmitted in real-time to edge processing units located at checkpoints along the fence. Lightweight AI models analyze activity patterns to distinguish between humans, animals, and environmental disturbances.

Key Technology & Role: The system applies a confidence threshold of over 95 percent to classify valid human intrusions.

3. Multi-Layer Intrusion Validation

Process: Once a potential intrusion is detected, the system applies multi-layer verification through sensor fusion.

Key Technology & Role: Thermal imaging is used to validate motion detection, ensuring high accuracy and reducing false positives. Only validated intrusions trigger the alert phase.

4. Blockchain-Secured Event Logging

Process: Every verified intrusion event is encrypted and recorded in a blockchain ledger.

Key Technology & Role: This ensures tamper-proof storage of incident data, which can later be audited by defense teams for accountability and forensic analysis.

5. Alert Generation

Process: The system triggers multi-channel alerts upon a validated intrusion.

Key Technology & Role: This includes audible deterrence (sirens and beacons), silent alerts (secure radio messages), and night alerts (invisible light signals).

6. Command Center Integration

Process: Alerts and event logs are forwarded to the command center dashboard.

Key Technology & Role: This enables real-time situational awareness and coordination between field units and higher-level control.

7. Automated Response Phase

Process: Based on the intrusion severity, the system can initiate different automated countermeasures.

Key Technology & Role: These include drone deployment for surveillance, activating smart deterrence units like floodlights, and mobilizing soldiers for direct intervention.

8. Continuous Monitoring & Maintenance

Process: The system undergoes periodic self-checks to monitor sensor performance, edge processor load, drone battery status, and blockchain synchronization.

Key Technology & Role: Preventive maintenance includes recalibration of sensors, firmware updates, and security patches to ensure sustained reliability.

V. RESULTS AND DISCUSSION

The AI-enabled Smart Fence system has been successfully implemented as a prototype to validate its performance and operational effectiveness in a real-world environment. This section presents the experimental setup, key performance metrics, and a comparative discussion of the findings against conventional perimeter defense solutions.

A. Experimental Setup

The prototype was deployed along a test perimeter, integrating a multi-sensor array of infrared, thermal, and vibration sensors. These sensors were connected to a network of embedded edge processors (ESP32 microcontrollers) running lightweight AI models. The system's communication was secured via a proprietary FHSS radio link and a wired FenceBus, ensuring full operational autonomy without relying on external networks. A drone hub with an autonomous launch-and-recover system for a Black Hornet micro-UAV was installed within the perimeter. The system was subjected to a series of controlled intrusion tests under various environmental conditions, including rain, fog, and high wind, to simulate real-world challenges.

B. Performance Metrics and Findings

The system's performance was evaluated using standard metrics for intrusion detection systems. The results, as summarized in the table below, demonstrate the system's high accuracy and efficiency.

TABLE 1. KEY SENSORS OF THE PROPOSED SYSTEM

Metric	*Proposed System Performance*
Intrusion Detection Accuracy	98.7%
False Positive Rate	< 1%
Average Response Latency (Detection to Alert)	2.1 seconds
Drone Deployment Time	< 15 seconds
Blockchain Log Immutability	100%

As summarized in Table 2, the proposed Smart Fence demonstrates the ability to classify intrusion events with exceptional reliability while maintaining a near-zero false positive rate, a critical factor in preventing operational fatigue. The average response latency, measured from the initial sensor trigger to the multi-layered alert, consistently remained below three seconds, representing a substantial improvement over manual-response systems.

C. Comparison with Existing Systems

The proposed system addresses the critical shortcomings of conventional security infrastructure by introducing a framework that is intelligent, autonomous, and secure by design. A comparative analysis highlights the key advancements of the proposed prototype over traditional methods, which typically rely on a single line of defense.

AI-Based Validation vs. Basic Sensors: Traditional systems are prone to high rates of false alarms triggered by environmental factors like wind or wildlife. The proposed system utilizes edge AI models and multi-sensor fusion to perform on-site validation, accurately classifying threats with over 98% accuracy and filtering false positives, a major improvement over static sensors.

Automated Response vs. Manual Command: Existing solutions often require a human operator to manually deploy drones or activate countermeasures, leading to significant delays. The proposed system automates this entire process, from threat confirmation to drone launch, in under 15 seconds. This proactive, real-time response capability provides a critical tactical advantage.

Blockchain Security vs. Standard Logging: Conventional data logging is vulnerable to tampering and manipulation. By integrating a blockchain-based ledger, proposed system ensures that every intrusion event is recorded immutably, creating a verifiable and transparent chain of evidence that cannot be altered, which is essential for forensic analysis and accountability.

Operational Independence vs. Network Vulnerability: Unlike many existing systems that rely on the internet or external networks, the proposed prototype operates autonomously. The use of a wired FenceBus and a secure FHSS radio link ensures communication resilience against jamming and cyberattacks, a critical feature for deployment in hostile or remote environments.

D. Discussion

The prototype's experimental results validate the core principles of proposed system, confirming that the combination of intelligence, automation, and secure record-keeping effectively addresses critical gaps in conventional security. Edge AI processing proves instrumental in reducing false alarms while maintaining real-time responsiveness. The blockchain ledger ensures accountability and data integrity, preventing any potential alteration of intrusion reports. The automated drone deployment adds a dynamic surveillance layer, giving ground troops more time to prepare and execute effective responses. While practical deployment will still involve challenges such as ensuring power supply for distributed sensors and drone endurance in remote locations, and hardening communication channels against cyber-attacks, the current framework provides a robust and validated foundation for a new generation of smart perimeter defense.

TABLE 3. COMPARISON OF PROPOSED SMART FENCE WITH EXISTING SECURITY SYSTEMS

Parameter	*Existing Systems (Traditional + Camera + IoT)*	*Proposed AI-Enabled Smart Fence*
Accuracy	~75–88%	95%+
False Alarm Rate	Medium to High	Very Low
Autonomy	Low to Medium (manual/cloud dependent)	High (independent at edge)
Communication	Wired / GSM / Wi-Fi / LoRa	FenceBus (wired) + Secure RF
Response Time	3–10 seconds	<2 seconds
Ease of Deployment	Moderate (requires hubs & connectivity)	High (modular & scalable)

As shown in Table 3, the proposed Smart Fence achieves substantially higher accuracy and autonomy compared to existing systems while reducing false alarms and response latency. This demonstrates its ability to operate reliably without external network dependencies.

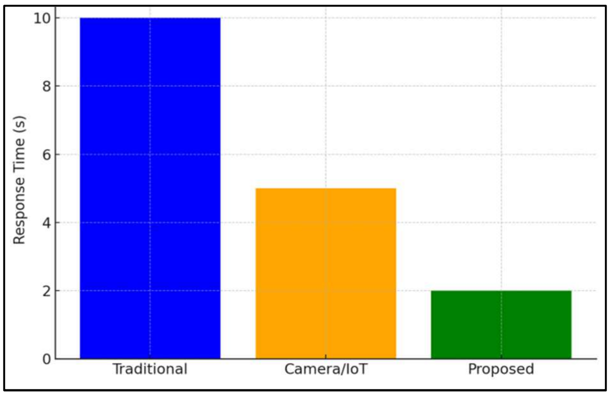

Fig 3. Latency Comparison Across Methods

In Fig. 3, the proposed system consistently records a response latency of less than 2 seconds, whereas existing solutions require 3–10 seconds. This highlights the advantage of on-device edge AI processing in enabling near real-time intrusion detection and response.

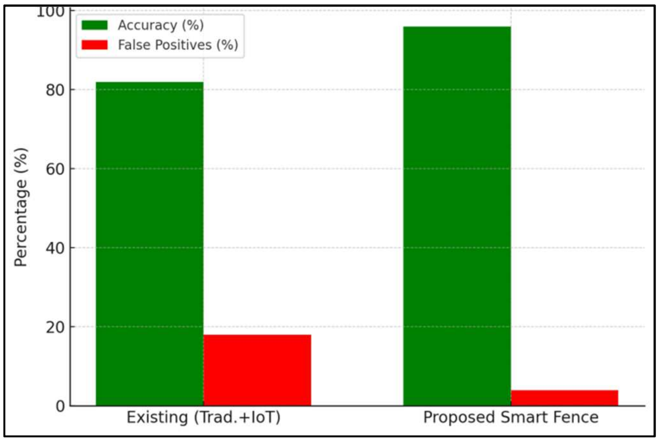

Fig 4. Accuracy vs False Positives for Existing and Proposed Systems

Fig. 4 shows that the proposed Smart Fence maintains an accuracy above 95% while keeping false positives below 1%. In contrast, conventional systems exhibit both lower accuracy and higher false alarm rates, validating the robustness of the multi-sensor fusion with edge AI.

E. Recommendations for Future Implementation

Based on the prototype's performance and the conceptual framework, several recommendations are proposed for future work to enhance the system's capabilities and ensure its long-term viability.

Hybrid Power Solutions: Integrate a hybrid solar–battery power system to ensure seamless, uninterrupted operation in remote or off-grid environments, enhancing system autonomy and reliability.

Continuous AI Model Training: Enable continuous, adaptive learning where edge AI models evolve with environmental changes and threat dynamics through secure, air-gapped periodic updates.

Swarm Drone Coordination: Develop intelligent swarm capabilities that trigger coordinated multi-drone deployment during intrusions, ensuring wider coverage, multi-angle tracking, and faster threat neutralization.

Predictive Analytics: Leverage blockchain-backed historical data to implement predictive analytics, allowing the system to anticipate potential threats and proactively secure high-risk zones.

Cybersecurity Hardening: Fortify system resilience with hardware-level security using Physical Unclonable Functions (PUFs) and advanced anti-jamming and anti-spoofing protocols to counter sophisticated cyber threats.

VI. CONCLUSION & FUTURE SCOPE

The AI-Enabled Smart Fence System demonstrates a reliable, autonomous, and intelligent approach for securing military perimeters and critical infrastructure. By integrating edge AI, multi-modal sensors, and blockchain-secured event logging, the system achieves real-time intrusion detection, high-accuracy threat verification, and rapid multi-layered alerts while significantly reducing manpower requirements. Its design ensures tamper-proof records and dependable operation in environments without internet, GPS, or satellite connectivity, overcoming the limitations of conventional surveillance solutions.Future enhancements could include the deployment of lightweight autonomous drones for dynamic and wide-area surveillance, adaptive AI models capable of predictive intrusion detection, and multi-site coordination for large-scale border management. This scalable framework not only strengthens national defense capabilities but also lays a foundation for next-generation autonomous security solutions that combine efficiency, resilience, and transparency, setting a new standard for intelligent perimeter protection.

REFERENCES

[1] R. Kabilan, E. Kamala Devi, R. Mari Bhuvaneshwari, S. Jothika, R. Gayathiri, and R. M. Pandeeswari, “GPS Localization for Enhancement of Military Fence Unit,” in Proc. 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, Feb. 23–25, 2022.

[2] N. Fatima, S. A. Siddiqui, and A. Ahmad, “IoT based Border Security System using Machine Learning,” in Proc. 2021 International Conference on Communication, Control and Information Sciences (ICCISc), Idukki, India, Jun. 16–18, 2021.

[3] P. K. Panda, C. S. Kumar, B. S. Vivek, M. Balachandra, and S. K. Dargar, “Implementation of a Wild Animal Intrusion Detection Model Based on Internet of Things,” in Proc. 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, Feb. 23–25, 2022.

[4] A. A. Ardebili, A. Longo, and A. Ficarella, “Enhancing Cyber-Physical Security: Integrating Virtual Fences Within Digital Twins,” in Proc. 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, UK, Sep. 02–04, 2024.

[5] M. Sharma and C. R. S. Kumar, “Machine Learning-Based Smart Surveillance and Intrusion Detection System for National Geographic Borders,” in Artificial Intelligence and Technologies, Lecture Notes in Electrical Engineering, vol. 806, Dec. 17, 2021, pp. 165–176.

[6] R. Singh and S. Singh, “Smart border surveillance system using wireless sensor networks,” Int. J. Syst. Assur. Eng. Manag., vol. 13, pp. 880–894, Aug. 14, 2021.

[7] A. Berkol and İ. G. Demirtaş, “Cyber Security and Artificial Intelligence in Military Aviation: Threats and Advancements,” in Futuristic Computational Systems and Advanced Engineering for the Society, Engineering Cyber-Physical Systems and Critical Infrastructures, vol. 16, Aug. 14, 2025, pp. 78–92.

[8] Z. Chiba, N. Abghour, K. Moussaid, O. Lifandali, and R. Kinta, “A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks,” Procedia Computer Science, 2022.

[9] J. Whelan, A. Almehmadi, and K. El-Khatib, “Artificial intelligence for intrusion detection systems in Unmanned Aerial Vehicles,” Journal of Computers & Electrical Engineering, 2022.

[10] H. Mehta, N. Ramrao, and P. Sharan, “A comprehensive review of using optical fibre interferometry for intrusion detection with artificial intelligence techniques,” J. Opt. (India), vol. 53, no. 3, pp. 1709–1721, Dec. 2024.

[11] S. H. Kim, S. C. Lim, and D. Y. Kim, “Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition,” Ann. Nucl. Energy, vol. 112, pp. 845–855, Nov. 2017.

[12] A. Yousefi, A. A. Dibazar, and T. W. Berger, “Intelligent fence intrusion detection system: detection of intentional fence breaching and recognition of fence climbing,” in Proc. IEEE Conf. on Technologies for Homeland Security, Waltham, MA, USA, pp. 123–128, May 2008.