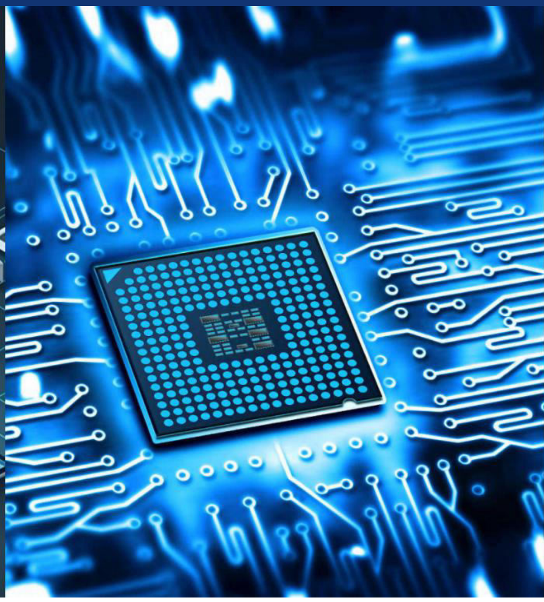
IJIRCCE

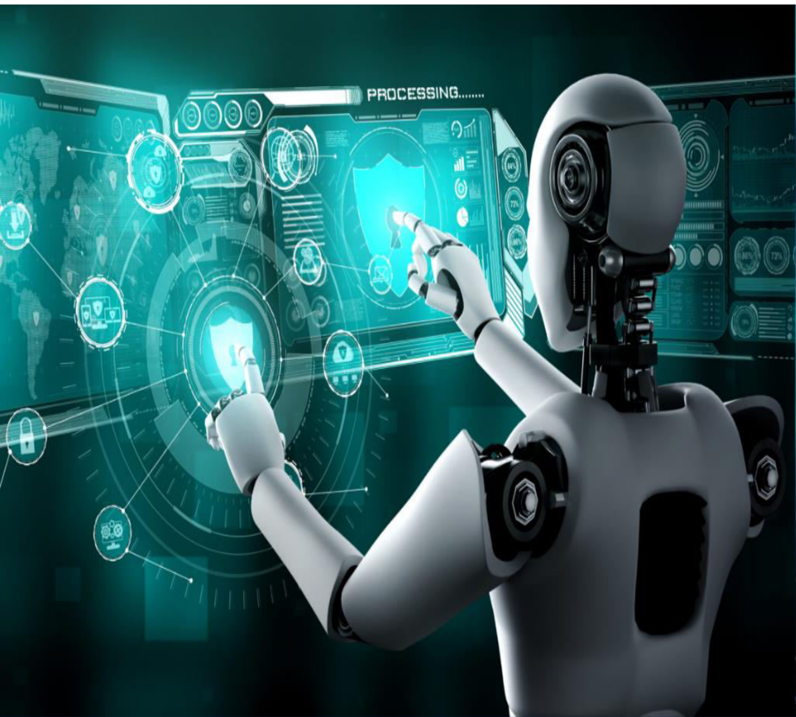
ISSN(O): 2320-9801

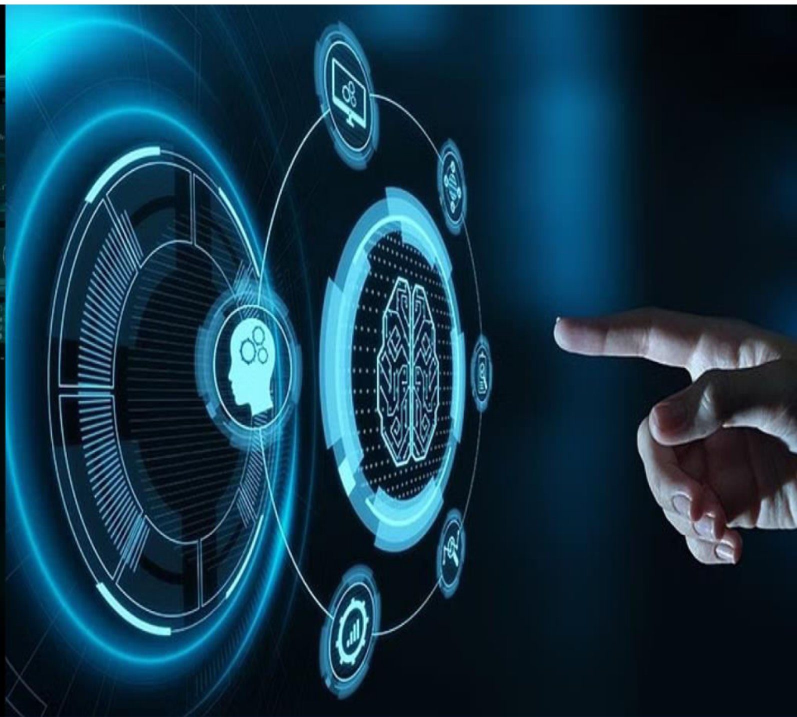
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405014

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI based Wildlife Intrusion Detection & Prevention System

Dr. P. Jamuna Rani*, Abishek V, Bharanedharan R **, Deepak R**, Gowtham S**.**

Associate Professor, Department of Chemistry, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamil Nadu, India*

UG Student, Department of Computer Science and Engineering, Mahendra Institute of Technology, Mallasamudram, Namakkal, Tamil Nadu, India**

ABSTRACT: An AI-based Wildlife Intrusion Detection and Prevention System (WIDPS) represents a sophisticated fusion of computer vision, edge computing, and non-lethal deterrent technology designed to mitigate human-wildlife conflict. At its core, the system utilizes high-resolution thermal or RGB cameras coupled with Passive Infrared (PIR) sensors to monitor boundary zones in real-time. When motion is detected, the raw data is instantly processed by an on-site "Edge AI" unit—such as a Jetson Nano or Raspberry Pi—running deep learning architectures like YOLOv8 or SSD (Single Shot Detector). This localized processing is critical; it allows the system to distinguish between a "false positive" like a domestic dog or swaying branches and a "target threat" like an elephant or a leopard without relying on an unstable cloud connection. Once a specific species is classified, the system executes a tiered response: it simultaneously transmits a low-latency alert via LoRaWAN or GSM to forest rangers and triggers a species-specific deterrent. These deterrents are carefully calibrated to be effective yet harmless, utilizing ultrasonic frequency arrays, high-intensity LED strobes, or acoustic mimicry (such as the sound of bees to deter elephants) to steer the animal back into the forest. By logging every encounter, the system creates a granular heat map of animal movement patterns, allowing for data-driven conservation strategies and ensuring that the prevention methods remain dynamic and effective over time.

KEYWORDS: Artificial Intelligence, Wildlife Detection, Animal Intrusion, Smart Farming, Human-Wildlife Conflict, Prevention System.

I. INTRODUCTION

1.1. The core of an AI-based wildlife intrusion system lies in its ability to process visual data at the "edge," meaning the intelligence is located directly on the device rather than a distant server. By utilizing compact microcontrollers or single-board computers equipped with deep learning models like YOLOv8, the system can instantaneously identify species with high precision. This localized processing is vital for remote regions where internet connectivity is sparse, ensuring that the system can distinguish between a harmless domestic animal and a potential threat, such as a wild boar or elephant, in under a second.

1.2. Once an intruder is confirmed, the system initiates a tiered, non-lethal prevention strategy designed to minimize habituation. Instead of a single repetitive alarm, the AI triggers specific deterrents based on the identified species—such as ultrasonic frequency arrays for primates or acoustic mimicry of natural predators for larger mammals. These hardware responses are often paired with high-intensity LED strobes to disorient the animal safely. This targeted approach ensures that the deterrent remains effective over time, steering the wildlife back into their natural habitat without causing physical injury or environmental stress.

1.3. For long-term reliability in harsh outdoor environments, these systems are built as autonomous, solar-powered units that utilize low-power communication protocols like LoRaWAN. To conserve energy, the high-power AI camera remains in a standby state until a Passive Infrared **(**PIR**)** sensor detects a heat signature, at which point the system "wakes up" to analyse the scene. This energy-efficient cycle allows the device to operate indefinitely in dense forests or farmlands, providing farmers and forest officials with real-time alerts and data logs that help map animal movement patterns and prevent future conflicts.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. DEVELOPING AN AI-BASED WILDLIFE INTRUSION

2.1. Primary Open-Source Repositories

➢ The foundation of the system's intelligence relies on massive, community-verified libraries like LILA BC and Snapshot Serengeti.
➢ These sources provide millions of labeled images across thousands of species, allowing the AI to learn distinct physical features and movement patterns.
➢ By utilizing these global databases, the model gains the robust capability to identify animals in various terrains and complex backgrounds.

2.2. Thermal and Infrared Datasets

➢ For effective night-time monitoring, the system utilizes specialized thermal imagery datasets to recognize heat signatures.
➢ Since many wildlife intrusions occur under the cover of darkness, training the AI on infrared data is crucial for maintaining high detection accuracy 24/7.
➢ These sources help the system distinguish between the heat profile of a large mammal and environmental heat radiation from rocks or soil.

2.3. Site-Specific Custom Data

➢ To minimize "false positives" caused by local vegetation or specific farm layouts, custom data is collected directly from the deployment site.
➢ By feeding the AI images of the actual environment—including empty frames with swaying trees or moving shadows—the system learns to ignore localized noise.
➢ This "negative sampling" significantly improves the reliability of alerts for the end-user.

2.4. Transfer Learning and Fine-Tuning

➢ Rather than training a model from scratch, the system employs Transfer Learning by using pre-trained architectures like YOLOv8.
➢ Developers take a model already familiar with general objects and fine-tune it with a smaller, targeted dataset of local wildlife.
➢ This method drastically reduces the required computational power while achieving high precision for specific regional intruders.

2.5. Real-Time Data Feedback Loops

➢ To ensure the system remains effective over time, a continuous feedback loop is established where new, misclassified images are used to retrain the model.
➢ Every "false alarm" or missed detection is logged and tagged, serving as a new data source for future updates.
➢ This iterative process allows the AI to adapt to changing seasons, animal habituation, and shifting migration paths.

III. AI TECHNIQUES IN WILDLIFE INTRUSION DETECTION & PREVENTION SYSTEM

3.1. Primary Open-Source Repositories

➢ The foundation of the system's intelligence relies on massive, community-verified libraries like LILA BC and Snapshot Serengeti.
➢ These sources provide millions of labeled images across thousands of species, allowing the AI to learn distinct physical features and movement patterns.
➢ By utilizing these global databases, the model gains the robust capability to identify animals in various terrains and complex backgrounds.

3.2. Thermal and Infrared Datasets

➢ For effective night-time monitoring, the system utilizes specialized thermal imagery datasets to recognize heat signatures.
➢ Since many wildlife intrusions occur under the cover of darkness, training the AI on infrared data is crucial for maintaining high detection accuracy 24/7.

➢ These sources help the system distinguish between the heat profile of a large mammal and environmental heat radiation from rocks or soil.

3.3. Site-Specific Custom Data

➢ To minimize "false positives" caused by local vegetation or specific farm layouts, custom data is collected directly from the deployment site.
➢ By feeding the AI images of the actual environment—including empty frames with swaying trees or moving shadows—the system learns to ignore localized noise.
➢ This "negative sampling" significantly improves the reliability of alerts for the end-user.

3.4. Transfer Learning and Fine-Tuning

➢ Rather than training a model from scratch, the system employs Transfer Learning by using pre-trained architectures like YOLOv8.
➢ Developers take a model already familiar with general objects and fine-tune it with a smaller, targeted dataset of local wildlife.
➢ This method drastically reduces the required computational power while achieving high precision for specific regional intruders.

3.5. Real-Time Data Feedback Loops

➢ To ensure the system remains effective over time, a continuous feedback loop is established where new, misclassified images are used to retrain the model.
➢ Every "false alarm" or missed detection is logged and tagged, serving as a new data source for future updates.
➢ This iterative process allows the AI to adapt to changing seasons, animal habituation, and shifting migration paths.

IV. AI TECHNIQUES IN WILDLIFE INTRUSION DETECTION & PREVENTION SYSTEM

The effectiveness of a modern Wildlife Intrusion Detection and Prevention System (WIDPS) relies on a hierarchy of AI techniques. These techniques transform raw sensor data into immediate, life-saving actions for both humans and animals.

4.1. Computer Vision & Object Detection

This is the primary technique used to "see" and identify intruders. Rather than just detecting motion, AI analyzes visual patterns to confirm if the intruder is a specific animal.
➢ YOLO (You Only Look Once): The industry standard for real-time detection. It is favored for its speed, allowing a camera to identify an animal (e.g., a wild boar or elephant) in milliseconds. This is critical for activating deterrents before the animal enters a danger zone.
➢ Convolutional Neural Networks (CNNs): The architecture behind most visual AI. CNNs excel at "Feature Extraction," meaning they can recognize an animal even if it is partially hidden by bushes or moving in low-light conditions.
➢ Thermal Image Processing**:** AI is trained specifically on infrared data to detect heat signatures. This technique is vital for nocturnal wildlife that cannot be seen by standard RGB cameras.

4.2. Multi-Sensor Data Fusion

To reduce "false positives" (like a blowing leaf or a domestic dog triggering the alarm), AI uses Data Fusion to cross-verify information from different sources.
➢ Acoustic Pattern Recognition**:** AI algorithms analyze sound frequencies. For example, the system can distinguish the low-frequency rumble of an elephant from the sound of wind or a passing vehicle.
➢ Seismic Analysis**:** Vibration sensors in the ground detect the "footfall signature" of heavy mammals. AI compares this seismic data with visual data to confirm a high-threat intrusion.
➢ PIR & Radar Integration**:** Low-power sensors trigger the "high-power" AI camera to wake up, saving battery life while maintaining 24/7 vigilance.

4.3. Behavioral Analysis & Anomaly Detection

Advanced systems don't just detect *what* the animal is; they predict *what it will do*.
➢ Trajectory Prediction**:** AI tracks the movement path of the animal. If the trajectory intersects with a farm or a road, the system escalates the alert.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405014

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

➢ Recurrent Neural Networks (RNN/LSTM): These models analyze "temporal" data (sequences of movement). They can differentiate between an animal that is calmly grazing and one that is exhibiting aggressive or "intrusive" behaviour.
➢ Anomaly Detection**:** AI learns the "normal" background of a forest. Any deviation—such as the sound of a chainsaw, a gunshot, or a vehicle—is flagged as a potential poaching or illegal logging threat.

4.4. Adaptive & Edge AI
Because these systems are often deployed in remote areas with no internet, the AI must be "Edge-based" and "Adaptive."
➢ Edge Computing**:** Using lightweight models (like Mobile Net or Tiny-YOLO) that run directly on small devices like a Raspberry Pi or Jetson Nano. This removes the need for a cloud connection and ensures zero-latency response.
➢ Reinforcement Learning**:** Some advanced systems use "Active Learning" to improve. If a deterrent (like a specific sound) fails to scare an animal away, the system tries a different frequency or sound and "learns" which method is most effective for that specific species.

V. APPLICATIONS OF AI BASED WILDLIFE INTRUSION

5.1. Agricultural & Crop Protection
➢ These systems act as a 24/7 digital guard for farms, preventing the economic devastation caused by crop-raiding animals.
➢ Real-Time Crop Guarding**:** AI cameras identify herbivores like elephants or wild boars as they approach field boundaries, triggering deterrents before damage occurs.
➢ Reduced Economic Loss**:** By preventing intrusions, farmers can save high-value harvests (such as sugarcane or maize), which are often targeted by wildlife.

5.2. Infrastructure & Road Safety
➢ Smart systems help prevent "roadkill" and vehicle accidents on highways or railways that cut through forest corridors.
➢ Dynamic Road Signs**:** When an animal is detected near a highway, AI triggers digital warning signs to alert drivers to slow down immediately.
➢ Railway Safety Zones**:** Acoustic and visual sensors detect wildlife on tracks, sending instant alerts to train operators to prevent collisions with large mammals.

5.3. Human Settlement & Village Security
➢ In regions where villages border forest reserves, these systems prevent predators and large mammals from entering residential areas.
➢ Early Warning Systems**:** Villages receive instant SMS or loudspeaker alerts when a predator (like a leopard or tiger) is detected in the vicinity.
➢ Livestock Protection**:** Monitors cattle sheds and pens, activating deterrents to scare away predators looking for easy prey.

5.4. Conservation & Anti-Poaching
➢ Beyond prevention, these systems serve as critical tools for forest departments to monitor biodiversity and stop illegal activities.
➢ Illegal Activity Detection**:** AI is trained to recognize "human" signatures, chainsaws, or gunshots, alerting rangers to poaching or illegal logging in real-time.
➢ Biodiversity Mapping**:** Automatically logs the frequency and health of different species, helping conservationists track migration and population trends.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

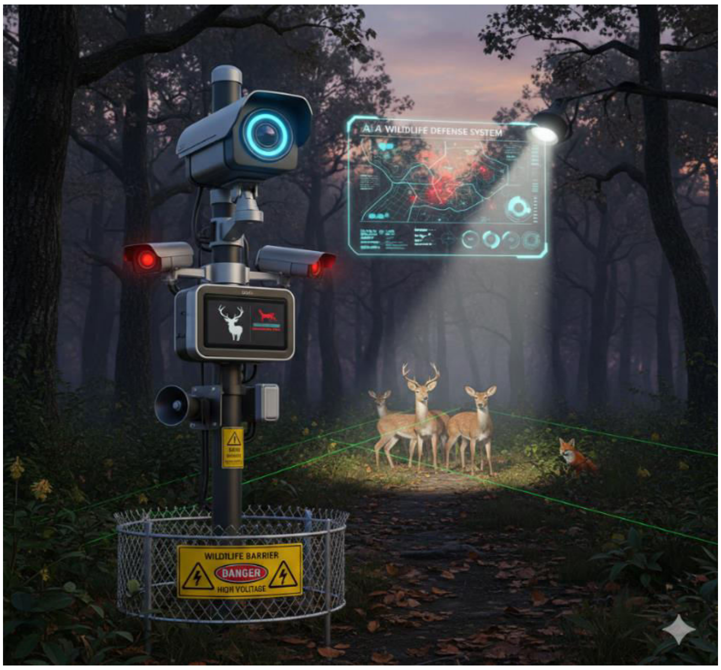


Fig.1 AI BASED WILDLIFE INTRUSION DETECTION & PREVENTION SYSTEM

VI. CHALLENGES IN AI BASED WILDLIFE INTRUSION DETECTION & PREVENTION SYSTEM

Implementing an AI-based system in rugged, outdoor environments comes with significant hurdles. Below are the primary challenges categorized by their technical and environmental impact.

6.1. Environmental & Hardware Durability

The physical deployment of sensors in the wild exposes the system to extreme conditions that can lead to hardware failure.

➢ Extreme Weather Resistance**:** Devices must withstand high humidity, monsoon rains, and intense heat, which can damage sensitive electronics and camera lenses.

➢ Power Supply Instability**:** Maintaining a 24/7 power source in remote forests is difficult, often requiring large solar arrays that may be blocked by dense tree canopies.

➢ Physical Vandalism by Wildlife**:** Curious or aggressive animals, such as monkeys or elephants, may physically attack or dislodge the cameras and sensors.

6.2. Technical & Computational Limitations

Processing complex AI models in real-time requires significant power, which is often at odds with the limited resources of "edge" devices.

➢ Processing Power vs. Latency**:** Compact devices like a Raspberry Pi may struggle to run high-accuracy models quickly enough to trigger a deterrent before an animal moves out of range.

➢ False Positives**:** Environmental "noise," such as swaying branches, moving shadows, or heavy rain, can trick the AI into triggering unnecessary alarms.

➢ Connectivity Gaps**:** Many wildlife zones lack 4G/5G coverage, forcing reliance on LoRaWAN or satellite links, which have very limited data bandwidth for sending images.

6.3. Data & AI Model Accuracy

AI is only as good as the data it is trained on, and wildlife presents unique challenges that standard datasets often miss.

➢ Night-time Detection Quality**:** Most animals are nocturnal, but training AI on grainy or low-contrast thermal/IR footage often leads to lower accuracy compared to daylight.

➢ Species Mimicry & Camouflage**:** Animals evolved to blend into their surroundings; an AI may fail to "see" a camouflaged leopard or tiger against a complex forest floor.

➢ Habituation to Deterrents**:** Over time, intelligent animals (like elephants) may realize that the AI-triggered sounds or lights carry no real threat, rendering the prevention system ineffective.

6.4. Socio-Economic & Ethical Constraints

Even a perfect technical system faces challenges regarding cost, local acceptance, and legal regulations.

➢ High Initial Cost**:** The cost of specialized thermal cameras, solar power kits, and AI hardware can be prohibitive for small-scale farmers or underfunded forest departments.

➢ Maintenance Requirements**:** These systems are not "set and forget"; they require skilled technicians to troubleshoot software bugs and repair physical damage in remote areas.

➢ Privacy Concerns**:** Cameras deployed near villages or public roads may raise legal and ethical concerns regarding the surveillance of local human populations.

VII. FUTURE PROSPECTS AI BASED WILDLIFE INTRUSION

7.1. Advancements in Edge Intelligence

The next generation of wildlife systems will move beyond simple detection toward autonomous, "smart" decision-making directly at the sensor level.

➢ On-Device Model Compression**:** Future systems will use ultra-lightweight architectures like **YOLOv11-Tiny** or specialized neural engines, allowing complex AI to run on low-power chips for years on a single battery.

➢ Self-Learning Algorithms**:** Systems will utilize "Online Learning," where the AI adapts to new animals or changing environments in real-time without needing a manual software update.

➢ Behavioural Prediction**:** Beyond mere identification, AI will analyse gait and posture to predict animal intent, distinguishing a curious animal from an aggressive one.

7.2. Satellite-Linked Global Networks

The integration of satellite technology will allow for the protection of vast, remote wilderness areas where cellular signals are non-existent.

➢ Direct-to-Satellite Connectivity**:** Integration with low-earth orbit (LEO) constellations like **Starlink** will enable real-time alerts from the deepest parts of the Amazon or African savannas.

➢ Swarm Intelligence**:** Multiple AI nodes will communicate with each other to track an animal's path across an entire landscape, creating a "moving digital corridor" of protection.

➢ Global Conservation Dashboards**:** Data from thousands of remote sensors will feed into a worldwide AI map, allowing scientists to track migration shifts due to climate change.

7.3. Sophisticated Bio-Mimetic Deterrents

Future prevention methods will move away from simple lights and sirens toward "smart" deterrents that mimic nature with high precision.

➢ Dynamic Acoustic Mimicry**:** AI will generate highly realistic, non-repetitive predator calls or distress signals that are virtually indistinguishable from real animals to prevent habituation.

➢ Pheromone & Olfactory Triggers**:** Automated dispensers will release species-specific chemical repellents or pheromones only when the AI confirms an intrusion.

➢ Laser-Based Virtual Fences**:** Use of low-power, AI-guided laser patterns that create a visual barrier only visible to animals, steering them away without physical obstructions.

7.4. Drone-Integrated Response Systems

Autonomous drones will become the "rapid response" arm of detection systems, moving from stationary guarding to active intervention.

➢ Automated Aerial Interception**:** When a ground sensor detects a high-threat intrusion (like a tiger near a village), a docked drone will automatically launch to guide the animal away.

➢ Thermal Tracking Drones**:** Drones equipped with AI will maintain a "birds-eye" view of a moving herd, providing real-time coordinates to forest rangers or farmers.

➢ Aerial Deterrent Deployment**:** Drones will carry specialized acoustic or light-based deterrents directly to the animal's location, providing a 360-degree prevention strategy.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VIII. CONCLUSION

The implementation of an AI-Based Wildlife Intrusion Detection and Prevention System marks a significant evolution in conservation technology, offering a sophisticated, non-lethal solution to the persistent challenge of human-wildlife conflict. By integrating high-performance edge computing with real-time computer vision models like YOLO, the system provides a proactive "digital fence" that can distinguish between harmless movement and genuine threats in under a second. Despite the hurdles of hardware durability in rugged terrains and the logistical demands of solar power, the convergence of Satellite IoT, thermal imaging, and species-specific deterrents creates a scalable framework for protecting both agricultural livelihoods and global biodiversity. Ultimately, this technology moves beyond simple surveillance to foster a data-driven coexistence, ensuring that as human settlements expand, we possess the intelligent tools necessary to preserve the natural world without compromising human safety or economic stability.

REFERENCES

1. Abed, N., et al., "IoT and AI-driven solutions for human-wildlife conflict: Advancing sustainable agriculture and biodiversity conservation," *Smart Agricultural Technology*, vol. 11, p. 100829, 2025.
2. Chinapureddy, L. R., et al., "Real Time AI-Based Wildlife Detection and Deterrent System for Farmland Protection," *ResearchGate*, 2024. [Focuses on YOLOv8 and species-specific deterrents].
3. Ronoh, E. K., et al., "Early warning system for human-wildlife conflict using deep learning, IoT and SMS," *NM-AIST Repository*, 2023. [Details Raspberry Pi and YOLO implementation].
4. Patil, M., et al., "Harmful Animal Identification and Detection in Forests Using AI & ML," *Zenodo*, 2025. [Covers CNN-based classification for threat detection].
5. König, H. J., et al., "Human–wildlife coexistence in a changing world," *Conservation Biology*, vol. 34, no. 4, pp. 786–794, 2020.
6. Sree, S., et al., "Beast Sentinel: Smart IoT-Based Wildlife Tracking and Intrusion System," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 2025.
7. Kumar, M. S., et al., "IoT Based Warning System from the Threat of Wild Animals," *6th International Conference on Communication and Electronics Systems (ICCES)*, pp. 550–553, 2021.
8. Sharma, P., et al., "AI-Based Animal Detection and Classification in Forest Areas," *International Journal of Computer Vision and Image Processing*, vol. 10, no. 2, 2020. [Focuses on thermal imaging].
9. Nuchhi, S., et al., "Raspberry Pi-based animal detection system using YOLO-based deep learning algorithms," *Journal of Embedded Systems*, 2020.
10. Abed, N., et al., "Artificial intelligence-driven solutions for mitigating human–wildlife conflict in biodiversity hotspots," *PMC (PubMed Central)*, vol. 12, 2025.