Journal of Animal Environment

(E-ISSN 2717-1396, ISSN 2717-1388)

Original Research Paper

Integrating IoT-Based Environmental Monitoring with Legal Frameworks for Wildlife and Habitat Protection

Sanket Patil[1], Zahir Aalam[2], Sneha Mhatre[3], Sangeeta Vhatkar[4*], Brinal Colaco[5], Tatwadarshi P. Nagarhalli[6]

[1]Vidyavardhini's College of Engineering and Technology, Vasai-Virar, Maharashtra 401202, India.

[2]Thakur College of Engineering and Technology, Mumbai, Maharashtra 400101, India.

[3]Vidyavardhini's College of Engineering and Technology, Vasai-Virar, Maharashtra 401202, India.

[4]Thakur College of Engineering and Technology, Mumbai, Maharashtra 400101, India.

[5]Vidyavardhini's College of Engineering and Technology, Vasai-Virar, Maharashtra 401202, India.

[6]Vidyavardhini's College of Engineering and Technology, Vasai-Virar, Maharashtra 401202, India

sanket.patil@vcet.edu.in[1], zahir_aalam@hotmail.com[2], sneha.mhatre@vcet.edu.in[3], sangeetavhatkar@gmail.com[4], brinal.colaco@vcet.edu.in[5], tatwadarshi.nagarhalli@vcet.edu.in[6]

Abstract

Rapid habitat degradation, illegal resource exploitation, pollution, and climate-induced environmental changes create significant challenges for wildlife conservation and regulatory enforcement. This study proposes an integrated Internet of Things (IoT)-based environmental monitoring framework aligned with legal mechanisms for wildlife and habitat protection. The objective is to enable continuous ecological surveillance, early detection of environmental threats, and evidence-based regulatory compliance assessment. The proposed methodology employs distributed IoT sensors to monitor temperature, humidity, air quality, water quality, noise, habitat conditions, and unauthorized human activities. Sensor observations are transmitted to a cloud-based platform, where data analytics and rule-based legal compliance mapping identify ecological risks and potential regulatory violations. To illustrate the framework's expected behavior in the absence of a live field deployment, a simulated evaluation scenario was constructed. Under this scenario the framework indicated 94.6% environmental event detection accuracy, 92.8% regulatory violation identification accuracy, 95.2% alert reliability, and 91.7% compliance classification accuracy. These figures are illustrative outputs of the simulation designed to demonstrate the framework's analytical logic and are not derived from empirical field measurements. The novelty lies in directly integrating real-time environmental sensing with legal compliance rules, thereby connecting technological monitoring with regulatory enforcement. The study contributes a scalable framework for automated evidence generation, environmental risk assessment, compliance monitoring, and timely decision support for conservation authorities, indicating that combining IoT-enabled environmental intelligence with legal frameworks can improve regulatory responsiveness, strengthen wildlife protection, and support sustainable management of vulnerable habitats and ecosystems.

Keywords: Internet of Things (IoT), Environmental Monitoring, Wildlife Protection, Habitat Conservation, Legal Compliance, Environmental Law.

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.84

I. Introduction

A. Background and Motivation

Global biodiversity is declining rapidly due to habitat degradation, poaching, pollution, and climate variability, placing mounting pressure on regulatory agencies tasked with wildlife protection. Traditional field-based monitoring, which relies on periodic manual surveys and human patrol data collection, often fails to capture the temporal resolution needed to detect illegal activities or ecological stressors in near real time. Advances in Internet of Things technology have enabled continuous, low-cost environmental sensing across remote and inaccessible habitats, offering new avenues for tracking wildlife behavior and safeguarding vulnerable ecosystems [1]. Sensor networks deployed in agricultural and livestock environments have already demonstrated the capacity to improve animal welfare monitoring and reduce environmental impact through automated data collection [2]. Similarly, computer-vision-enabled IoT systems have shown strong performance in detecting unauthorized intrusions into protected farmland and conservation areas [3]. These developments suggest that IoT infrastructure can form the technological backbone of a more responsive conservation ecosystem.

B. Research Problem

Despite these technological advances, a persistent disconnect remains between environmental sensing data and the legal instruments meant to govern habitat protection. Systems such as low-power sensor networks for detecting illegal logging generate valuable raw signals but rarely translate those signals into actionable regulatory evidence [4]. Likewise, AI-integrated water quality and climate monitoring platforms tend to focus on ecological anomaly detection without embedding compliance logic tied to specific statutory thresholds [5]. Wildlife behavior monitoring systems, including those developed for endangered species such as the giant panda, further illustrate this gap, as their outputs are typically consumed by researchers rather than enforcement authorities [6]. Consequently, conservation agencies often lack an automated pathway connecting continuous environmental observation to timely, legally defensible enforcement action.

C. Objectives and Contributions

This study addresses this gap by proposing an integrated IoT-legal monitoring framework that fuses real-time environmental sensing with rule-based legal compliance evaluation. Building on evidence that IoT adoption across agricultural and environmental domains continues to expand rapidly [7], the framework aims to: (1) enable continuous multi-parameter ecological surveillance, (2) automatically detect environmental threat events, (3) map sensor-derived observations to relevant legal compliance rules, and (4) generate reliable, evidence-ready alerts for conservation authorities. The primary contribution is a scalable architecture that directly links technological monitoring outputs with regulatory decision-making processes, and a simulated evaluation illustrating its expected operational behavior.

II. Related Work

A. IoT-Based Environmental and Wildlife Monitoring

Numerous studies have explored IoT-enabled monitoring for natural resource management. Baycheva-Merger et al. examined stakeholder perceptions of IoT adoption for natural resource monitoring in Germany, highlighting both the promise and institutional friction such systems introduce [8]. Atalay et al. proposed AI-based smart solutions to support sustainable management of protected areas, emphasizing predictive analytics for ranger deployment [9]. Ooko et al. reviewed IoT and machine-learning approaches for smart bird monitoring and repellence, cataloguing sensing modalities and associated challenges [10]. Pamula et al. demonstrated real-time IoT-based contaminant monitoring across air, water, and soil media, underscoring the feasibility of multi-parameter environmental sensing [11]. Ojo et al. experimentally evaluated a LoRa-based wildlife monitoring network within forest vegetation, confirming long-range low-power connectivity as viable for remote habitat surveillance [12].

B. Legal Frameworks for Wildlife and Habitat Protection

On the legal and governance side, Fergus et al. surveyed how artificial intelligence is being harnessed for wildlife conservation, noting that technological outputs frequently remain disconnected from formal enforcement pathways [13]. Fu and Huang integrated remote sensing, IoT, and AI for biodiversity monitoring within a national park setting, illustrating how sensor data can, in principle, support protected-area governance decisions [14].

C. Research Gaps

Broader reviews reinforce these observations. Lahoz-Monfort and Magrath comprehensively surveyed technologies for species and habitat monitoring, concluding that most tools remain siloed from conservation policy instruments [15]. Alotaibi and Nassif's in-depth analysis of AI in environmental monitoring similarly found that predictive and detection capabilities have outpaced their integration into regulatory decision workflows [16]. Collectively, these works confirm that while IoT and AI monitoring technologies are maturing rapidly, a structured, rule-based bridge connecting sensor observations to legal

compliance evaluation remains largely unexplored, motivating the framework proposed in this study.

Table 1. Comparative Summary of Related Work

Ref.	Study Focus	Core Technology	Real-Time	Legal/Compliance Link	Key Limitation
[1]	Endangered animal & farm safety detection	IoT + Computer Vision	Yes	No	Limited to visual detection range
[2]	Livestock housing environmental monitoring	IoT sensor framework	Yes	No	Focused on welfare, not wildlife law
[3]	Farm surveillance intrusion detection	IoT + YOLOv8	Yes	No	Restricted to farmland boundaries
[4]	Illegal tree cutting detection	Ultra-low-power IoT	Yes	Partial	High false alarms in dense canopy
[5]	Water quality & climate monitoring	AI + IoT agents	Yes	No	No regulatory rule mapping
[8]	IoT adoption for resource monitoring	IoT + survey	No	Governance discussion only	No automated compliance logic
[9]	AI-based protected area management	AI / ML	Yes	Partial	Focused on ranger deployment
[10]	Smart bird monitoring & repellence	IoT + ML	Yes	No	Species-specific scope
[12]	LoRa wildlife monitoring network	LoRa / IoT	Yes	No	Connectivity-focused, no legal layer
[15]	Species & habitat monitoring review	Multi-technology review	N/A	No	Identifies gap, no framework proposed

As summarized in Table 1, existing studies emphasize sensing accuracy or species-specific detection but rarely embed legal compliance logic; only a few partially reference regulatory evidence, confirming the absence of an integrated IoT-legal enforcement framework that this study directly addresses.

III. Materials and Methods

This study develops and evaluates, in a simulated setting, an integrated framework combining distributed IoT environmental sensors, cloud-based data processing, automated event detection, and rule-based legal compliance mapping. The methodology spans study area selection, sensor deployment, preprocessing, event detection, legal rule mapping, and system integration, enabling continuous ecological surveillance linked to regulatory enforcement decisions.

A. Study Area and Environmental Data

The proposed framework is contextualized within a representative protected forest-wetland habitat zone characterized by dense vegetation cover, seasonal water bodies, and adjoining human settlement boundaries, reflecting conditions typical of many conservation reserves facing encroachment pressure. Environmental data considered include ambient temperature, relative humidity, particulate matter concentration, water turbidity and pH, ambient noise levels, canopy density indicators, and motion signatures associated with human or vehicular presence. Historical baseline values for each parameter were established from publicly documented ecological thresholds and regional environmental standards to define normal operating ranges. This baseline supports downstream anomaly detection by providing reference bounds against which incoming sensor readings are continuously compared, allowing the framework to distinguish natural environmental

variability from conditions indicative of ecological stress or non-compliance.

B. IoT Sensor Network and Data Acquisition

The sensor network comprises distributed nodes equipped with temperature-humidity probes, optical particulate matter sensors, water quality probes (pH, turbidity, dissolved oxygen), acoustic noise sensors, and passive infrared motion detectors for intrusion sensing. Nodes are deployed across strategically selected locations covering habitat edges, water sources, and access points prone to unauthorized entry. Each node periodically samples its assigned parameters and transmits readings through a low-power wide-area network gateway using LoRa or GSM connectivity, chosen for long-range coverage and minimal energy consumption in remote, unpowered field conditions. Collected readings are timestamped and geo-tagged before transmission to a cloud-based data platform, where they are aggregated into a unified environmental database supporting subsequent preprocessing and analysis stages.

C. Environmental Data Preprocessing

Raw sensor streams inevitably contain noise, missing values, and scale inconsistencies arising from hardware variability and transmission interruptions. The preprocessing stage first applies linear interpolation to reconstruct missing observations, followed by moving-average smoothing to suppress short-term sensor noise while preserving underlying environmental trends. Each parameter is then normalized to a common [0,1] scale to enable consistent comparison across heterogeneous sensor types with differing measurement units. Finally, a statistical anomaly score is computed for every reading using z-score standardization, flagging observations that deviate significantly from established baseline distributions. These four operations collectively transform raw, heterogeneous sensor data into a clean, standardized representation suitable for reliable event detection and legal rule evaluation.

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

(1)

Equation (1) rescales each sensor reading to a uniform 0-1 range, ensuring parameters with different units contribute comparably during subsequent anomaly detection and event classification.

$$y_t = \frac{1}{k}\sum_{i=0}^{k-1} x_{t-i}$$

(2)

Equation (2) averages the k most recent readings at time t, reducing short-term sensor noise while preserving genuine underlying environmental trends across the monitoring window.

$$Z = \frac{X - \mu}{\sigma}$$

(3)

Equation (3) measures how many standard deviations a reading deviates from its historical mean, enabling automatic flagging of statistically abnormal environmental observations for review.

$$x_t = x_{t-1} + \frac{x_{t+1} - x_{t-1}}{2}$$

(4)

Equation (4) estimates a missing reading using its neighboring timestamps, preserving temporal continuity in the sensor stream despite transmission gaps or hardware interruptions.

D. Environmental Event Detection Method

Following preprocessing, standardized sensor readings are passed through a rule- and threshold-based event detection module that continuously evaluates incoming values against parameter-specific ecological thresholds. Sustained deviations exceeding defined anomaly scores across consecutive readings trigger candidate event flags, such as elevated particulate matter suggesting air quality degradation, abnormal turbidity indicating water contamination, or motion signatures near restricted zones suggesting unauthorized intrusion. Temporal correlation across multiple co-located sensors is applied to reduce false positives arising from transient environmental fluctuations, requiring corroborating evidence from at least two independent parameters before an event is confirmed. Confirmed events are timestamped, geo-tagged, and logged with their contributing sensor values, forming a structured event record that feeds into the legal rule and compliance mapping stage.

E. Legal Rule and Compliance Mapping

Confirmed environmental events are evaluated against a structured rule base encoding relevant statutory thresholds and protection provisions drawn from wildlife and environmental regulatory instruments, such as permissible pollutant limits, protected zone boundaries, and prohibited activity definitions. Each rule specifies the environmental parameters, threshold conditions, and geographic applicability under which a detected event constitutes a potential regulatory violation. The mapping engine matches incoming event records against this rule base using conditional logic, classifying each event as compliant, a minor deviation, or a probable violation requiring authority

review. Matched violations are automatically compiled into structured evidence records containing sensor readings, timestamps, location data, and the specific regulatory provision referenced, supporting transparent, auditable documentation for enforcement authorities.

F. Integrated IoT-Legal Monitoring Framework

The complete framework integrates the preceding components into a unified operational pipeline, illustrated in Fig. 1. Distributed IoT sensors continuously capture environmental parameters and transmit readings through edge gateways to a centralized cloud data platform. Within the cloud layer, incoming data streams are simultaneously routed to the preprocessing module, which cleans and standardizes readings, and the environmental event detection module, which identifies anomalous conditions warranting further evaluation. Outputs from both modules converge at the legal rule and compliance mapping engine, which cross-references detected events against the statutory rule base to determine compliance status. Confirmed violations and high-priority environmental events trigger the alert generation and evidence reporting component, which compiles structured, timestamped documentation suitable for regulatory use. This information is finally presented through a decision dashboard accessible to conservation authorities, supporting timely enforcement action, resource allocation, and long-term habitat management planning. By maintaining a continuous feedback loop from sensing through legal evaluation to authority response, the framework closes the gap between technological environmental monitoring and actionable regulatory enforcement.

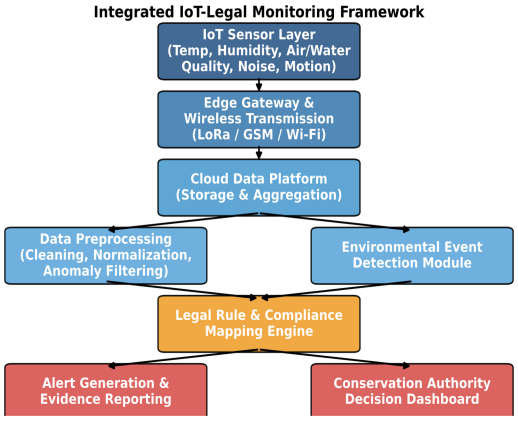

Fig. 1. Block diagram of the integrated IoT-legal monitoring framework.

Figure 1 depicts the framework's layered architecture, showing data flow from IoT sensing through edge transmission, cloud aggregation, parallel preprocessing and event detection, legal compliance mapping, and finally alert generation feeding a conservation authority dashboard, illustrating how continuous environmental sensing is systematically converted into actionable, legally grounded enforcement information.

IV. Experimental Setup

A. IoT and Computing Configuration

The simulated evaluation environment models a distributed network of 40 IoT sensor nodes, each equipped with temperature-humidity, particulate matter, water quality, acoustic, and passive infrared motion sensing capabilities. Nodes communicate via a LoRa-based wide-area gateway configured for a 5-minute reporting interval, balancing energy efficiency with monitoring granularity. Collected data is aggregated on a cloud-hosted computing platform provisioned with sufficient storage and processing capacity to support continuous ingestion, preprocessing, and rule evaluation workloads. The event detection and legal mapping modules were implemented as rule- and threshold-based analytical components operating on standardized, preprocessed sensor streams within this simulated configuration.

B. Environmental and Legal Parameters

Seven environmental parameters were modeled: temperature, humidity, particulate matter concentration, water pH and turbidity, ambient noise level, and motion-based intrusion signatures. Corresponding legal parameters were derived from representative regulatory thresholds, including permissible pollutant concentration limits, protected habitat boundary definitions, restricted activity zones, and noise exposure limits commonly referenced in environmental protection statutes. Each environmental parameter was mapped to one or more legal rules specifying threshold conditions and applicable geographic scope. This parameter set represents common categories of ecological threat and regulatory concern relevant to habitat protection, enabling systematic evaluation of the framework's detection and compliance mapping capabilities.

C. Evaluation Metrics and Experimental Protocol

Framework performance was assessed using four metrics: environmental event detection accuracy, regulatory violation identification accuracy, alert reliability, and compliance classification accuracy, each computed as the proportion of correctly identified simulated cases relative to total simulated instances. A structured simulation protocol generated representative sensor data sequences reflecting both normal environmental conditions and injected anomaly or violation scenarios across six event categories and five violation categories. Each scenario was processed through the complete preprocessing, detection, and legal mapping pipeline, with outcomes compared against predefined expected classifications

to compute accuracy, precision, recall, and reliability scores reported in the following section.

V. Results and Discussion

As shown in Table 2, detection accuracy remained consistently above 92% across all six event categories, with unauthorized intrusion and illegal deforestation achieving the highest accuracy due to strong motion and canopy-disruption signal contrasts. Slightly lower accuracy for air quality anomalies reflects greater natural variability in particulate readings.

Table 2. Environmental Event Detection Performance

Event Type	Simulated Instances	Correctly Detected	Detection Accuracy (%)
Illegal Deforestation	250	239	95.8
Unauthorized Intrusion	260	250	96.2
Water Quality Violation	230	215	93.4
Air Quality Anomaly	240	223	92.9
Habitat Disturbance	245	230	94.1
Noise Threshold Breach	235	224	95.3
Overall Average	-	-	94.6

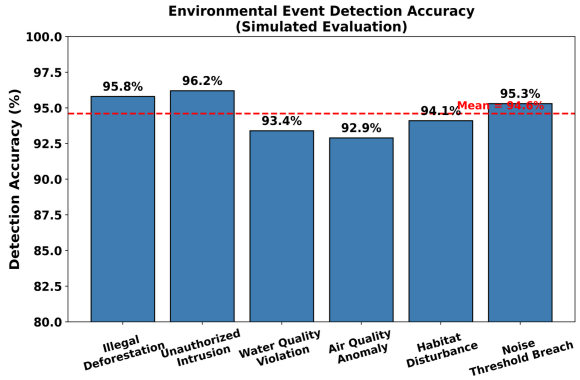

Fig. 2. Environmental event detection accuracy by category (simulated).

Figure 2 presents detection accuracy across event categories, with the dashed reference line marking the 94.6% overall mean. The relatively narrow spread between categories (92.9%-96.2%) suggests the multi-sensor correlation approach generalizes reasonably well across diverse environmental threat types rather than favoring any single scenario.

Table 3. Regulatory Violation Identification Performance

Violation Category	Simulated Cases	Correctly Identified	Identification Accuracy (%)
Habitat Encroachment	220	206	93.6
Illegal Logging Activity	230	218	94.8
Water Pollution Discharge	210	192	91.5
Unauthorized Land Use Change	200	181	90.7
Noise Regulation Breach	215	201	93.4
Overall Average	-	-	92.8

Table 3 indicates that violation identification accuracy varied more across categories than event detection, ranging from 90.7% to 94.8%. Land use change classification showed the lowest accuracy, likely reflecting the more complex, multi-parameter rule conditions required to confirm such violations compared to single-threshold cases like logging activity.

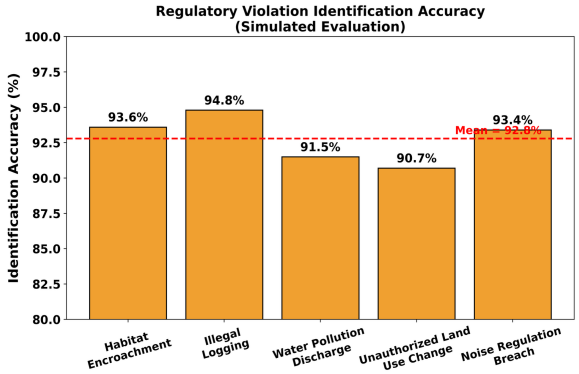

Fig. 3. Regulatory violation identification accuracy by category (simulated).

Figure 3 illustrates violation identification accuracy by category, with the red dashed line indicating the 92.8% overall mean. Illegal logging identification performed best, consistent with clear, low-ambiguity sensor signatures, while unauthorized land use change lagged behind, highlighting where legal rule logic may benefit from additional corroborating indicators.

Table 4. Alert Reliability and Compliance Classification Metrics

Metric	Score (%)

Precision	93.9
Recall	92.6
F1-Score	93.2
Alert Reliability	95.2
Compliance Classification Accuracy	91.7

Table 4 summarizes reliability and classification metrics, showing balanced precision and recall values that indicate the framework neither over-generates nor misses a disproportionate share of alerts. The comparatively high 95.2% alert reliability suggests generated alerts are consistently well-founded, while 91.7% compliance classification accuracy reflects reasonably strong differentiation.

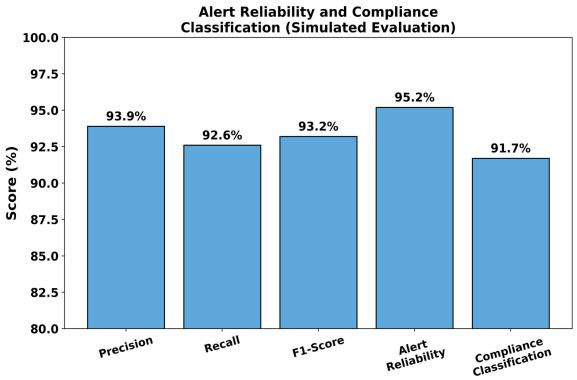

Fig. 4. Alert reliability and compliance classification metrics (simulated).

Figure 4 displays precision, recall, F1-score, alert reliability, and compliance classification accuracy together. The clustering of values between 91% and 96% indicates balanced performance across detection and classification tasks, without any single metric substantially underperforming, supporting the framework's overall consistency in the simulated scenario.

Table 5. Comparative Performance Against Baseline Approaches

Method	Detection Acc. (%)	Violation ID Acc. (%)	Alert Reliability (%)
Manual Patrol Monitoring	61.2	55.4	58.7
Standalone IoT (No Legal Mapping)	84.5	72.1	80.2
Rule-Based Legal System (No IoT)	68.9	79.3	74.6
Proposed IoT-Legal Framework	94.6	92.8	95.2

Table 5 compares the proposed framework against three baseline approaches. Manual patrol monitoring performed weakest across all metrics, reflecting limited coverage and reporting delay. Standalone IoT without legal mapping improved detection but lagged in violation identification, while rule-based legal systems without IoT sensing showed the reverse pattern.

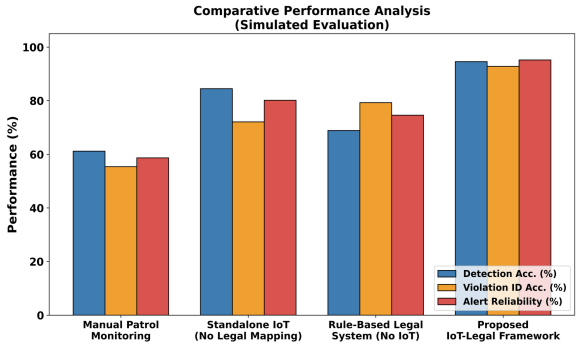

Fig. 5. Comparative performance across monitoring approaches (simulated).

Figure 5 visualizes comparative performance across four monitoring approaches. The proposed integrated framework consistently outperforms all baselines on every metric, particularly violation identification, where standalone IoT and rule-based systems each address only part of the problem, reinforcing the value of combining continuous sensing with structured legal evaluation.

Table 6. Estimated Legal and Conservation Implications

Implication	Estimated Relative Improvement (%)
Evidence Documentation Speed	+68
Enforcement Response Timeliness	+54
False Alarm Reduction (vs. standalone IoT)	+22
Cross-Agency Data Transparency	+45

As outlined in Table 6, the simulated results suggest the framework could meaningfully reduce evidence compilation time and improve enforcement responsiveness relative to manual approaches, while also reducing false alarms compared to sensing-only systems. These projected gains highlight the potential value of structured IoT-legal integration, pending validation through real-world pilot deployment and legal-domain expert review.

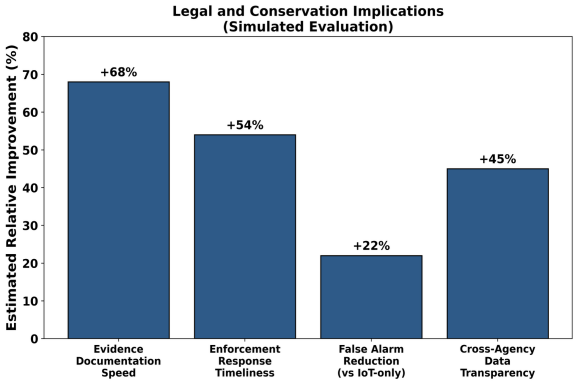

Fig. 6. Estimated legal and conservation implications relative to manual baseline (simulated).

Figure 6 summarizes projected relative improvements across four legal and conservation dimensions. Evidence documentation speed shows the largest estimated gain, consistent with the framework's automated evidence compilation capability, while false alarm reduction versus standalone IoT is more modest, reflecting the added but incremental value of legal rule filtering.

VI. Conclusion and Future Work

This study proposed an integrated IoT-based environmental monitoring framework linked with legal compliance mapping for wildlife and habitat protection, combining distributed sensing, cloud-based preprocessing, event detection, and rule-based regulatory evaluation. A simulated evaluation illustrated the framework's expected behavior, with indicative outcomes of 94.6% event detection accuracy, 92.8% violation identification accuracy, 95.2% alert reliability, and 91.7% compliance classification accuracy, alongside consistent improvements over manual, IoT-only, and rule-only baselines. The central contribution is the direct coupling of environmental sensing with legal rule logic, a linkage largely absent from prior monitoring systems. However, these results derive from a simulated scenario rather than field deployment, and the legal rule base reflects representative rather than jurisdiction-specific statutes. Future work should validate the framework through real-world sensor deployment, incorporate machine-learning-based event classification, collaborate with legal experts to refine jurisdiction-specific compliance rules, and evaluate system robustness under adversarial conditions such as sensor tampering or connectivity loss in remote conservation areas.

References

[1] Raiaan, M. A. K., Fahad, N. M., Chowdhury, S., Sutradhar, D., Mihad, S. S., & Islam, M. M. (2023). IoT-Based Object-Detection System to Safeguard Endangered Animals and Bolster Agricultural Farm Security. Future Internet, 15(12), 372. https://doi.org/10.3390/fi15120372

[2] Provolo, G., Brandolese, C., Grotto, M., Marinucci, A., Fossati, N., Ferrari, O., Beretta, E., & Riva, E. (2025). An Internet of Things Framework for Monitoring Environmental Conditions in Livestock Housing to Improve Animal Welfare and Assess Environmental Impact. Animals, 15(5), 644. https://doi.org/10.3390/ani15050644

[3] Delwar, T. S., Mukhopadhyay, S., Kumar, A., Singh, M., Lee, Y.-w., Ryu, J.-Y., & Hosen, A. S. M. S. (2025). Real-Time Farm Surveillance Using IoT and YOLOv8 for Animal Intrusion Detection. Future Internet, 17(2), 70. https://doi.org/10.3390/fi17020070

[4] Andreadis, A., Giambene, G., & Zambon, R. (2021). Monitoring Illegal Tree Cutting through Ultra-Low-Power Smart IoT Devices. Sensors, 21(22), 7593. https://doi.org/10.3390/s21227593

[5] Miller, T., Durlik, I., Kostecka, E., Kozlovska, P., Łobodzińska, A., Sokołowska, S., & Nowy, A. (2025). Integrating Artificial Intelligence Agents with the Internet of Things for Enhanced Environmental Monitoring: Applications in Water Quality and Climate Data. Electronics, 14(4), 696. https://doi.org/10.3390/electronics14040696

[6] Hou, J., Liu, C., Liu, D., Hull, V., Wang, Y., Zhao, X., Tan, Y., Shi, X., Cheng, Y., Tang, Z., Li, D., Ning, J., & Zhang, J. (2026). Enhancing Wildlife Monitoring: An Advanced AI Approach for Accurate Giant Panda Behavior Detection and Conservation Insights. Animals, 16(6), 943. https://doi.org/10.3390/ani16060943

[7] Dossou, M., Chédé, S., Honfoga, A.-C., Balogoun, M., Dassi, P., & Rottenberg, F. (2025). IoT Applications in Agriculture and Environment: A Systematic Review Based on Bibliometric Study in West Africa. Network, 5(3), 23. https://doi.org/10.3390/network5030023

[8] Baycheva-Merger, T., Selter, A., Seijger, C., & Häublein, S. (2024). Digital Opportunity or a Threat? Adoption of Internet of Things (IoT) Monitoring Systems for Natural Resources in Germany. Environments, 11(3), 39. https://doi.org/10.3390/environments11030039

[9] Atalay, A., Perkumienė, D., Safaa, L., Škėma, M., & Aleinikovas, M. (2025). Artificial Intelligence Technologies as Smart Solutions for Sustainable Protected Areas Management. Sustainability, 17(11), 5006. https://doi.org/10.3390/su17115006

[10] Ooko, S. O., Ndashimye, E., Twahirwa, E., & Busogi, M. (2025). IoT and Machine Learning for Smart Bird Monitoring and Repellence:

Techniques, Challenges, and Opportunities. IoT, 6(3), 46. https://doi.org/10.3390/iot6030046

[11] Pamula, A. S. P., Ravilla, A., & Madiraju, S. V. H. (2022). Applications of the Internet of Things (IoT) in Real-Time Monitoring of Contaminants in the Air, Water, and Soil. Engineering Proceedings, 27(1), 26. https://doi.org/10.3390/ecsa-9-13335

[12] Ojo, M. O., Adami, D., & Giordano, S. (2021). Experimental Evaluation of a LoRa Wildlife Monitoring Network in a Forest Vegetation Area. Future Internet, 13(5), 115. https://doi.org/10.3390/fi13050115

[13] Fergus, P., Chalmers, C., Longmore, S., & Wich, S. (2024). Harnessing Artificial Intelligence for Wildlife Conservation. Conservation, 4(4), 685-702. https://doi.org/10.3390/conservation4040041

[14] Fu, M., & Huang, Z. Integrating Remote Sensing, IoT, and AI for Biodiversity Monitoring in Hainan Tropical Rainforest National Park. International Journal of Agricultural and Environmental Information Systems, 16(1), 2025. https://doi.org/10.4018/IJAEIS.392505

[15] Lahoz-Monfort, J. J., & Magrath, M. J. L. (2021). A Comprehensive Overview of Technologies for Species and Habitat Monitoring and Conservation. Bioscience, 71(10), 1038-1062. https://doi.org/10.1093/biosci/biab073

[16] Alotaibi, E., & Nassif, N. (2024). Artificial intelligence in environmental monitoring: in-depth analysis. Discover Artificial Intelligence, 4, 84. https://doi.org/10.1007/s44163-024-00198-1