Results in Engineering 24 (2024) 103277

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering

AI-powered IoT and UAV systems for real-time detection and prevention of illegal logging

Montaser N.A. Ramadan [a], Mohammed A.H. Ali [a,*], Shin Yee Khoo [a,b], Mohammad Alkhedher [c]

[a] Department of Mechanical Engineering, Faculty of Engineering, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[b] Centre of Research Industry 4.0 (CRI 4.0), Faculty of Engineering, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[c] Mechanical and Industrial Engineering Department, Abu Dhabi University, 59911, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Keywords:
CNN
Illegal logging detection
IoT
Lorawan, Real-time environmental monitoring,
UAV-based monitoring

ABSTRACT

Illegal logging poses a significant threat to environmental conservation, contributing to deforestation, ecosystem disruption, and economic losses. Traditional detection methods, such as ground patrols and satellite imagery, are often ineffective, expensive, and time-consuming. This paper introduces a novel Unmanned Aerial Vehicles (UAV)-based IoT system for chainsaw noise detection and prevention. The system uses low-cost IoT nodes with microphones and microcontrollers to detect chainsaw sounds via a Convolutional Neural Network (CNN) model. These nodes reduce power consumption, allowing the battery to last at least 8 years. Detected chainsaw sounds are transmitted to a LoRaWAN gateway and forwarded to a cloud server. The cloud server processes the data and dispatches a drone equipped with a camera to the site. The drone streams live video to the cloud, where AI algorithms analyze the footage for human presence. If detected, the drone activates sound and light alarms to deter illegal logging. Experimental results show that IoT nodes can detect chainsaw sounds up to 100 m, with the CNN model achieving an accuracy of 99.37 % and a loss of 0.0185. Comparisons with Logistic Regression, Decision Tree, Random Forest, and SVM demonstrated the superior performance of CNN. This UAV-IoT system offers a fast, reliable, scalable, and real-time solution for detecting and preventing illegal logging. Leveraging advanced AI and IoT technologies, this system enhances environmental monitoring and conservation efforts. It represents a significant step forward in the fight against illegal logging, providing a practical, effective, and sustainable solution.

1. Introduction

Illegal logging, defined as the unauthorized harvesting, transportation, purchase, or sale of timber in violation of national laws, is a pervasive global issue with severe environmental, social, and economic repercussions, including deforestation, biodiversity loss, and significant government revenue losses [1,2]. Unlike legal logging, which adheres to strict regulatory frameworks and sustainable practices, illegal logging often involves document forgery, corruption, and exploitation of legal loopholes to meet high timber demands [3,4]. The prevalence of illegal logging is widespread, affecting countries with vast forest resources such as Brazil, Indonesia, and the Democratic Republic of the Congo, as well as regions like West Kalimantan in Indonesia [1,4]. For instance, in Indonesia, illegal logging is regulated under Forestry Law No 19 of 2004 and Law No 18 of 2013, which impose severe sanctions, including up to 15 years of imprisonment and fines up to IDR 100 billion [1]. Despite these regulations, the effectiveness of measures to combat illegal logging is often undermined by inadequate governance, lack of binding policies, and insufficient community awareness [2,3]. Factors such as economic development, rule of law, and control of corruption play crucial roles in the prevalence of illegal logging, indicating that comprehensive and multifaceted approaches are necessary to address this complex issue effectively [3,5]. The interconnectedness of illegal logging with other criminal activities, such as the illegal wildlife trade, further complicates enforcement efforts, as seen in Cameroon where both activities share organized networks and access routes, exacerbating ecological and socio-economic impacts [6]. Technological advancements, such as remote sensing and artificial intelligence, offer promising tools for monitoring forest conditions and detecting illegal logging activities, as demonstrated by the use of Google Earth Engine in Indonesia to identify forest change events [7]. However, the lack of specific forensic-ready tests for timber species and geographic origin remains a significant

* Corresponding author.
E-mail address: hashem@um.edu.my (M.A.H. Ali).

https://doi.org/10.1016/j.rineng.2024.103277
Received 8 August 2024; Received in revised form 22 October 2024; Accepted 29 October 2024
Available online 31 October 2024

challenge, necessitating further research and development in this area [8]. The socio-economic drivers of illegal logging, including poverty and cultural factors, also need to be addressed through community engagement and education to raise legal awareness and promote sustainable practices [5]. International efforts, such as INTERPOL's Project Leaf, which seized over 50,000 m^3 of illegally logged timber valued at $8 million across 12 countries in Central and South America, highlight the scale of the problem and the need for coordinated global action [9]. Strengthening policy regimes, enhancing law enforcement capabilities, and fostering international cooperation are essential steps towards mitigating the impacts of illegal logging and ensuring the protection of forest resources for future generations [4,9].

Illegal logging is a pervasive issue with profound environmental and economic impacts. Environmentally, it is a major driver of deforestation, contributing to approximately 50–90 % of deforestation in key tropical regions, as reported by the United Nations[10] .This rampant deforestation leads to significant biodiversity loss and ecosystem disruption, threatening endangered species such as orangutans in Indonesia and tigers in India by destroying their natural habitats [11,12]. The illegal extraction of timber not only depletes forest resources but also exacerbates climate change by reducing the carbon sequestration capacity of forests [13]. Economically, illegal logging undermines legitimate forestry businesses by flooding the market with cheaper, illegally sourced timber, which depresses timber prices and leads to significant revenue losses for governments [14]. This illegal activity is often linked to corruption and organized crime, further destabilizing local economies and governance structures [15]. For instance, in Mexico, the volume of illegal logging is nearly equivalent to that of the legal harvest, driven by demand from the construction and manufacturing sectors, which perpetuates a productivity trap in the forest sector [14]. In the Brazilian Amazon, illegal logging is a significant threat, with powerful landholders often associated with larger illegal deforestation events, highlighting the need for stringent enforcement of forest regulations and land tenure reforms to curb this practice [16]. The situation is exacerbated by the lack of effective forensic tools to trace the origin of timber, making it difficult to prosecute illegal activities and enforce laws [17]. Moreover, the economic viability of forest enterprises is compromised, as seen in the mixed impacts of forest certification schemes, which aim to promote sustainable forest management but have shown varied success in reducing deforestation and forest degradation [18]. In regions like Pará, Brazil, the legal timber market is highly selective, with a preference for a small group of species, leading to overexploitation and potential extinction of these species [19]. The illegal use of natural resources, including logging, also poses a global threat to biodiversity, as seen in the Brazilian Amazon, where indirect methods of assessing illegal activities reveal higher rates of wildlife consumption and other illegal practices than direct methods [20]. Overall, addressing illegal logging requires a multifaceted approach, including the development of robust forensic tools, stringent enforcement of forest regulations, land tenure reforms, and the promotion of sustainable forest management practices to balance economic growth with conservation efforts.

The detection and prevention of illegal logging face significant challenges due to the limitations of traditional methods such as ground patrols and satellite imagery. Ground patrols, while effective in small areas, are constrained by human resources and accessibility, particularly in vast and remote forest regions, making it difficult to cover large areas efficiently. Satellite imagery, although useful for broad monitoring, presents issues such as high costs, low temporal resolution, and the need for complex, time-consuming analysis. For instance, high-resolution satellite imagery can cost several hundred dollars per square kilometer, making continuous monitoring prohibitively expensive [7,21]. To address these limitations, there is a pressing need for innovative, cost-effective, and efficient methods that provide real-time data and can cover extensive areas.

Unmanned Aerial Vehicles (UAVs) have emerged as powerful tools in environmental monitoring, offering advantages like high spatial resolution, cost-effectiveness, and the ability to operate in remote areas. They have been successfully used for forest fire monitoring, species classification, and ecological mapping, providing real-time data and high-resolution imagery at lower costs than traditional methods [22,23, 24]. However, challenges such as real-time data processing and operational efficiency—particularly regarding battery life and data transmission—remain significant hurdles for widespread adoption [25]. Continued advancements in UAV technology, including modular designs and improved data processing algorithms, are critical to enhancing their effectiveness in environmental applications.

To address these challenges, integrating UAVs with other advanced technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) can significantly enhance their detection and prevention capabilities. For example, the use of Sentinel 1 and 2 data in conjunction with the Google Earth Engine (GEE) platform allows for the monitoring of illegal logging events even in regions with high cloud cover, as radar sensors can penetrate clouds, providing continuous observation of forest conditions [7]. Additionally, the implementation of IoT can aid in the establishment of effective forest management and surveillance by utilizing GPS to identify the location of deforestation activities such as tree-cutting and fires, thereby enabling more responsive and informed decision-making [26]. Furthermore, the use of deep learning models to detect the sound of logging activities, such as chainsaw sounds, has shown promising results, with convolutional neural networks (CNN) achieving high accuracy in sound classification, thus providing a reliable method for real-time monitoring and alert generation [27]. Wireless sensor networks combined with neural networks can also detect chainsaw and human sounds in protected forests, accurately identifying the source of the sounds and communicating alerts to authorities, thereby enhancing the ability to respond to illegal activities promptly [28]. Moreover, the integration of camera modules using TensorFlow and RFID technology can help spot trespassers and notify them about the required permissions to enter restricted forest areas, further aiding in the prevention of illegal logging [29]. These advanced technologies not only offer more precise and timely detection of illegal logging activities but also provide scalable solutions that can be implemented across large and remote forest areas, addressing the limitations of traditional methods and contributing to the protection and conservation of forest ecosystems. Therefore, the adoption of these innovative technologies is crucial for enhancing the effectiveness of illegal logging detection and prevention efforts, ensuring the sustainability of forest resources and the preservation of biodiversity.

In this research work, A novel UAV-based IoT system is proposed for chainsaw noise sensing and detection to prevent illegal logging. The system integrates low-cost IoT nodes equipped with microphones and microcontrollers that utilize a Convolutional Neural Network (CNN) model to detect chainsaw sounds. These IoT nodes communicate with a LoRaWAN gateway, which forwards the alerts to a cloud server. The cloud server processes the data and dispatches a drone equipped with a visual camera to the detection site. The drone streams live video to the cloud, where AI algorithms analyze the footage for human presence. If individuals are detected, the drone activates an onboard sound and light alarm system to deter illegal logging activities.

This integrated system offers a fast, reliable, scalable, and real-time solution for detecting and preventing illegal logging. It leverages advanced AI and IoT technologies to enhance environmental monitoring and conservation efforts. The system's design ensures low power consumption, allowing the IoT nodes to operate for at least 8 years on a single battery. The high accuracy of the CNN model and the real-time response capability of the drone significantly improve the effectiveness of illegal logging detection and prevention.

The evaluation of the proposed system demonstrates its effectiveness in real-time illegal logging detection and prevention. Through rigorous testing, the system achieved a high accuracy in detecting chainsaw sounds using the CNN model, and the UAV's rapid response capability allowed for prompt intervention. The system's low power consumption and long operational lifespan make it suitable for deployment in remote forest areas. Additionally, the integration of AI-based analysis of drone footage provided reliable identification of human presence, further enhancing the system's ability to prevent illegal activities. The results of these evaluations validate the system's potential for large-scale implementation in forest conservation efforts.

1.1. Study contribution and novelty

The primary objective of this study is to develop an integrated UAV-based IoT system for the detection and prevention of illegal logging activities. The system leverages advanced AI algorithms, IoT technology, and UAV capabilities to create a scalable, real-time monitoring solution that enhances the efficiency and effectiveness of forest conservation efforts. The contribution and novelty of this paper can be summarize as following:

1. Innovative Integration of Technologies: This study uniquely combines IoT, UAVs, and AI to form a comprehensive monitoring system. The integration of acoustic detection of chainsaw sounds with visual monitoring through drone cameras provides a robust approach to identifying and deterring illegal logging activities.
2. Extended Battery Life for IoT Nodes: The IoT nodes are designed with a power-saving mechanism, allowing them to operate for at least 8 years on a single battery. This innovation significantly reduces maintenance costs and ensures long-term deployment in remote forest areas.
3. High Detection Accuracy with CNN: The use of a Convolutional Neural Network (CNN) model for chainsaw sound detection achieves high accuracy, with results showing 99.37 % accuracy and a low loss of 0.0185. This outperforms traditional machine learning models, demonstrating the effectiveness of the CNN approach.
4. Real-Time Response and Active Intervention: The system's real-time response capability allows for immediate intervention by activating a drone equipped with sound and light alarms. This novel use of UAVs for active intervention effectively deters illegal logging activities.
5. Scalability and Reliable Communication: The system is designed to be scalable, allowing for large-scale deployment across extensive forested areas. The use of LoRaWAN for communication ensures reliable data transmission over long distances, enhancing the system's applicability in various environmental monitoring scenarios.

The structure of this paper is organized as follows: The Introduction provides the context and background of the study, outlining the challenges of illegal logging and the need for advanced detection systems. The Literature Review surveys existing solutions and highlights the technological advancements relevant to this research. The Material and Method section details the design, implementation, and operational mechanisms of the proposed system. The Results and Validation section presents the experimental findings and evaluates the performance of the system. Finally, the Conclusion summarizes the key contributions of the study and discusses potential future directions for research.

2. Literature review

Illegal logging poses a significant threat to environmental conservation, contributing to deforestation, ecosystem disruption, and substantial economic losses, with the World Bank estimating annual losses of up to $15 billion [10]. Effective detection and prevention strategies are crucial to combat this pervasive issue. AI technologies offer transformative potential in addressing illegal logging by processing and analyzing large datasets quickly, identifying patterns, and providing real-time insights, thereby significantly improving upon traditional methods. Integrating AI with other technologies like UAVs and IoT can create a comprehensive monitoring system. The literature review covers several key sections: the current state of research, technological approaches and methodologies, effectiveness and limitations, future directions, and recommendations. Current research highlights the use of AI in wildlife acoustic monitoring, which has shown significant progress but still faces gaps in understanding and application [30]. Technological approaches include the use of deep learning algorithms like U-Net 3D with multispectral and synthetic aperture radar images to detect deforestation with high accuracy [31], and satellite-based alert systems to track selective logging in tropical forests, demonstrating strong linear relationships between alerts and visually identified tree cover loss [21]. Machine learning techniques combined with robotic platforms and artificial vision systems have been used for remote monitoring of forest health, including moisture content and forest degradation [32]. The development of unmanned forest machines for real-time detection and positioning of harvested logs using AI algorithms like YOLOv3 further exemplifies the technological advancements in this field [33]. The effectiveness of these AI solutions is evident in their ability to provide accurate and timely data, although challenges remain, such as the difficulty in obtaining cloud-free satellite imagery in tropical regions and the need for better alignment of vessel tracking with fishing regulations in marine conservation areas [7,34]. Future directions include improving the accuracy and usefulness of AI algorithms, developing new methodologies for remote sensing-based verification of logging activities, and enhancing the integration of AI with other technologies for a more robust monitoring system [7,21,30]. The conclusion emphasizes the need for continued research and development to fully realize the potential of AI in combating illegal logging and promoting sustainable forest management. This comprehensive approach, leveraging AI and other advanced technologies, can significantly enhance the effectiveness of conservation efforts and mitigate the adverse impacts of illegal logging on the environment and economy.

Illegal logging is a significant global issue, prompting the development of various solutions leveraging advanced technologies and traditional methods. Satellite imagery has become a cornerstone in forest monitoring due to its broad area coverage and ability to provide historical data. Programs like Landsat and Sentinel are instrumental in tracking deforestation, offering high-resolution optical and radar data that can detect even small-scale disturbances in near-real time [21,35]. These satellites enable the use of sophisticated algorithms, such as the random forest classification on Google Earth Engine (GEE) and the Cumulative Sum (CuSum) approach, to monitor forest conditions and detect illegal logging events with high accuracy [7,36]. However, these technologies come with limitations, including high costs, the need for specialized analysis, and delays in data processing, which can hinder timely interventions [37]. Additionally, the effectiveness of satellite data can be compromised by atmospheric conditions, such as cloud cover, which is particularly challenging in tropical regions [7,35]. Ground patrols are another method used to combat illegal logging, but they face practical challenges such as limited coverage, high resource intensiveness, and the difficulty of accessing remote forest areas [38]. Camera traps offer a targeted approach by monitoring specific areas and detecting human activities, but they are limited by their fixed locations and lack of real-time capabilities, making them less effective for large-scale monitoring [39]. To enhance the effectiveness of these methods, multi-source data fusion, combining satellite imagery with Unmanned Aerial Vehicle (UAV) data, has been proposed. This approach provides a more comprehensive understanding of forest ecosystems by integrating different types of data, thus overcoming the limitations of single-sensor systems [40]. Remote sensing technologies, such as video surveillance and wireless systems [41,42,43], also play a crucial role in real-time monitoring and early detection of illegal activities, although they require significant investment and technical expertise to implement effectively [44]. International efforts to combat illegal logging include legislation in destination countries, such as the Australian Illegal Logging Prohibition Act, which mandates due diligence by companies importing timber products. However, these laws often rely on the legal

Table 1
Comparative analysis of scalability, accuracy, real-time capabilities, and drawbacks of technologies for preventing illegal logging.

Paper	Technology Type	Key Insights	Accuracy	Real-Time	Scalability	Integration Technologies	Drawbacks
[57]	IoT-based Smart System	Effective for real-time detection; uses solar power to maintain operations in remote areas.	High precision in detecting illegal logging and forest fires; real-time monitoring and alerts.	Yes	Moderate	AI, IoT	Initial setup and maintenance costs can be high.
[21]	Satellite-based Forest Disturbance Alerts	Effective for near-real-time detection; strong linear relationship between alerts and tree cover loss.	High accuracy in detecting tree cover loss and disturbances at a 10 m resolution.	Yes	High	AI, Satellite	Limited reliability in areas with few disturbances; cannot directly observe logging volumes.
[58]	UAV-Lidar	Provides detailed insights into forest structure, diversity, and microclimate changes due to edge effects.	High precision in capturing detailed canopy structure and edge effects.	NO	Moderate	UAV, Lidar	Limited by flight range, weather, and regulatory restrictions; high initial and maintenance costs.
[59]	Spatial Data and Satellite Information	Effective for monitoring legal compliance and planning; accurate slope and terrain analysis.	High accuracy with high-resolution data (e.g., LiDAR); variability with lower resolution data.	NO	High	AI, Satellite	Data resolution variability affects accuracy; high costs for high-resolution data and infrastructure.
[60]	Machine Learning-Based Electronic Tree Surveillance System	Effective for real-time detection of illegal logging; integrates sensor technology with ML techniques.	High accuracy (97.5 %) using SVM classifier.	Yes	Moderate	AI, IoT	High initial costs and maintenance; affected by environmental factors.
[61]	IoT-based Sound Acquisition and Acoustic Signal Analysis System	Enhances existing camera-based surveillance with sound detection; effective for monitoring large areas.	High accuracy in detecting chainsaw activities using Mel-frequency cepstral coefficients.	NO	High	AI, IoT	Resource-intensive deployment; dependent on network connectivity and power supply.
[62]	Vibration Sensor and NRF Technology	Effective for near-real-time detection of illegal logging; uses vibration sensors and NRF transmitters for accurate detection.	High accuracy using vibration sensors for logging detection.	Yes	Moderate		High initial costs and maintenance; affected by environmental factors.
[63]	Acoustic Surveillance System	Effective for near-real-time detection of illegal logging; uses audio recordings and SVM for accurate monitoring.	High accuracy using SVM algorithm for logging detection; 94.42 % accuracy at 20 dB SNR.	Yes	Modertate	AI	High initial costs and maintenance; affected by environmental factors.

frameworks of source countries, which can be undermined by corruption and inadequate enforcement, highlighting the need for a more robust transnational framework [38]. Overall, while satellite imagery and advanced remote sensing technologies offer powerful tools for monitoring and combating illegal logging, their effectiveness is often limited by high costs, the need for specialized skills, and environmental factors. Ground patrols and camera traps provide valuable support but are constrained by their operational limitations. A multi-faceted approach, integrating various technologies and international cooperation, is essential for addressing the complex issue of illegal logging effectively.

Recent research on preventing illegal logging has highlighted several major findings and trends, particularly the shift from traditional methods to advanced technological solutions. One significant trend is the increasing use of remote sensing technologies, such as the Google Earth Engine (GEE) platform, which employs artificial intelligence and machine learning algorithms to monitor forest conditions and detect illegal logging activities in near-real time. For instance, the random forest classification algorithm on the GEE platform has been used to analyze Sentinel 1 and 2 data, revealing extensive forest changes and illegal logging spots in Indonesia [7]. Similarly, the RAdar for Detecting Deforestation (RADD) alerts, derived from dense time series satellite data, have proven effective in tracking selective logging activities in the Congo Basin, demonstrating a strong correlation between satellite alerts and visually identified tree cover loss [21]. Unmanned aerial vehicles (UAVs) are also gaining traction, with recent studies focusing on tree classification and segmentation using data from UAVs equipped with RGB or multispectral cameras and LiDAR scanners. These methods, often combined with machine learning techniques, have shown improved accuracy and interpretability in forest monitoring [45]. Additionally, the development of unmanned forest machines for automated operations, such as log detection and positioning using the YOLOv3 algorithm, represents another technological advancement aimed at enhancing forest management and reducing illegal logging [33]. Deep learning (DL) methods, particularly convolutional neural networks (CNNs), have been widely applied in forestry for tasks such as surface quality evaluation of sawn timber, forest resource surveys, and tree species identification, further supporting the shift towards AI-driven solutions [46]. The use of high-throughput sequencing technologies and bioinformatics tools to obtain complete chloroplast genomes of commercial timber species has also been identified as a promising method for developing genetic markers to combat illegal logging, supporting international regulations like CITES and the EU Timber Regulation [47]. Despite these technological advancements, challenges remain, such as the need for better governance and law enforcement to effectively curb illegal logging. Studies have shown that factors like economic growth, rule of law, and control of corruption significantly impact the prevalence of illegal logging, underscoring the importance of robust institutional frameworks [15,48]. Moreover, the socio-economic dynamics, such as the demand from construction and manufacturing sectors, continue to drive illegal logging, indicating the need for comprehensive strategies that address both technological and socio-economic aspects [14]. Overall, the integration of advanced technologies like AI, UAVs, and DL methods with improved governance and international cooperation represents a holistic approach to preventing illegal logging and promoting sustainable forest management.

Artificial Intelligence (AI) techniques have become pivotal in detecting illegal logging, leveraging machine learning, deep learning, neural networks, and computer vision to enhance monitoring and enforcement efforts. Machine learning algorithms, such as random forest and support vector machines, are employed to analyze satellite images and aerial photos from UAVs, identifying changes in forest cover indicative of illegal logging activities [7,49]. For instance, the random forest classification algorithm on the Google Earth Engine (GEE) platform has been used to monitor forest conditions and detect illegal logging events in Indonesia, utilizing Sentinel 1 and 2 data to overcome challenges posed by cloud cover in tropical regions [7]. Deep learning

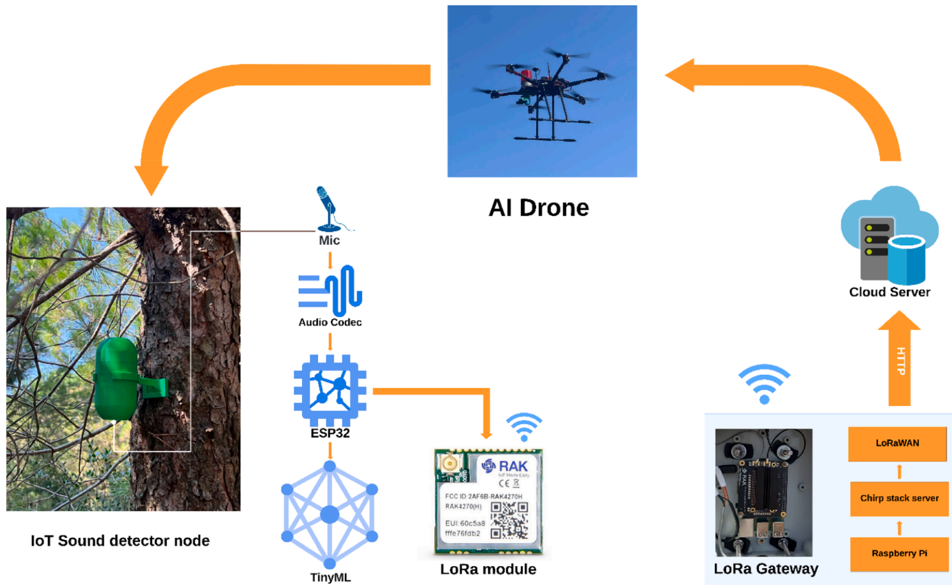


Fig. 1. Block diagram of the UAV-IoT system for illegal logging detection and prevention.

models, particularly Convolutional Neural Networks (CNNs), are adept at image recognition tasks, making them suitable for analyzing high-resolution aerial imagery to detect deforestation patterns and classify tree health [50,51]. Faster R-CNN, for example, has been used to automatically detect and classify unhealthy and dead trees from RGB imagery captured by drones, facilitating rapid response to forest threats [50]. In addition to visual data, acoustic monitoring systems employing neural networks can detect the sound of chainsaws, a common indicator of illegal logging. These systems use sensors to capture acoustic data, which is then processed using AI models to identify specific noise patterns associated with logging activities. Environmental data from IoT devices, such as temperature, humidity, and wind speed, also play a crucial role in predicting and analyzing illegal logging activities, as these factors can influence the likelihood of forest fires and other related events [52,53]. Data preprocessing techniques are essential to enhance the quality and reliability of the data used in AI models. Noise reduction methods are applied to filter out irrelevant information from satellite images and acoustic data, ensuring that the models focus on significant features. Data augmentation techniques, such as rotating, flipping, and scaling images, are used to increase the diversity of the training dataset, improving the robustness of the models. Feature extraction methods, including principal component analysis (PCA), are employed to reduce the dimensionality of the data and highlight the most relevant features for model training [49]. Moreover, AI-enabled systems like TimberSleuth integrate human feedback to refine their anomaly detection capabilities, using visual analytics to help analysts identify and confirm illegal logging activities in trade records [54]. The combination of these advanced AI techniques and diverse data sources significantly enhances the ability to monitor, detect, and respond to illegal logging, contributing to more effective forest conservation and management efforts.

The performance outcomes across various studies on illegal logging detection demonstrate significant advancements through the application of AI and deep learning techniques. For instance, a study by Anđelić et al. utilized deep learning models to detect chainsaw sounds, comparing multilayer perception (MLP) and convolutional neural network (CNN) approaches. The CNN-based model achieved a sound classification accuracy of 94.96 % on a YouTube dataset and 88.87 % on a real environment dataset, outperforming the MLP-based model [27]. Similarly, Bandaranayake et al. proposed a system using wireless sensor networks and neural networks to detect chainsaw and human sounds in protected forests. Their machine learning model demonstrated an accuracy of over 93 %, with the system capable of distinguishing noises from a range of 30 m and detecting sound positions within 180°, effectively communicating alerts to authorities through a wireless transmission protocol [55]. Additionally, Singh et al. highlighted the efficacy of deep learning models in high-resolution imagery and remote sensing for object detection, including trees, underscoring the superior performance of deep learning over traditional computer vision algorithms in surveillance applications [56]. These studies collectively illustrate how AI, particularly deep learning, has significantly enhanced the detection and prevention of illegal logging by improving accuracy, range, and real-time communication capabilities, thereby contributing to more effective forest conservation efforts.

Table 1

In conclusion, the integration of advanced technologies such as AI, UAVs, and IoT has significantly enhanced the detection and prevention of illegal logging. AI techniques, particularly deep learning algorithms, have proven effective in processing and analyzing large datasets to identify illegal activities in near-real time. While traditional methods like satellite imagery and ground patrols provide valuable data, their limitations highlight the need for innovative solutions that leverage multiple data sources. Despite the progress, challenges remain, including data quality, computational requirements, and environmental factors like cloud cover. Future research should address these issues by improving data preprocessing, developing more robust AI models, and enhancing multisource data integration. Additionally, robust governance and international cooperation are crucial for effective enforcement and combating illegal logging.

Ongoing research and development are essential to fully realize the potential of these technologies. Future directions include refining AI algorithms for better accuracy, developing new remote sensing methodologies, and creating integrated monitoring systems. By combining technological advancements with effective governance, Conservation efforts can be significantly improved, mitigating the impacts of illegal logging on the environment and economy, while promoting sustainable forest management and preservation.

3. Material and methods

3.1. System overall description

This paper presents a novel solution for detecting and preventing illegal logging by integrating IoT sensors, Unmanned Aerial Vehicles (UAVs), and Artificial Intelligence (AI) technologies. The core of the

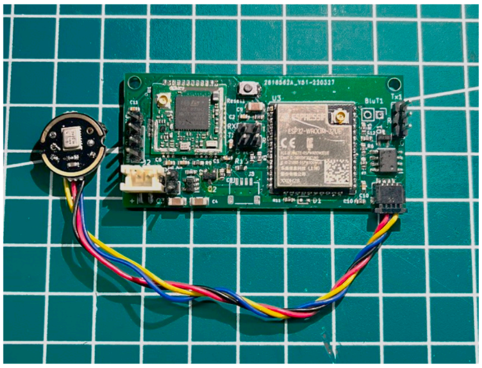


Fig. 2. Main PCB Board Control of the IoT Sound Detection Node.

system consists of IoT nodes equipped with acoustic sensors, which detect the sound of chainsaws using a CNN model. When a chainsaw sound is detected, the IoT node sends an alarm signal through a LoRaWAN network to a central gateway. The gateway then forwards this alarm to a cloud-based server, which serves as the central hub for data processing and command distribution.

Upon receiving the alarm, the cloud server issues an automated command to a ground station to deploy a drone to the specific location where the activity was detected. The drone, equipped with high-resolution cameras and AI-powered image recognition capabilities, autonomously flies to the detection site to verify the presence of illegal logging. If the drone's AI camera confirms that individuals are cutting trees, it activates an onboard sound alarm system to warn and force them to stop their activities as shown in Fig. 1.

This multi-layered approach ensures a rapid and efficient response to illegal logging activities. By integrating IoT sensors for real-time acoustic detection, a LoRaWAN network for reliable signal transmission, a cloud server for centralized processing, and UAVs for on-site verification and intervention, this system provides a comprehensive monitoring and enforcement solution. It enhances detection accuracy and response times while minimizing the need for extensive ground patrols, making it a scalable and cost-effective solution for large-scale deployment in forest conservation efforts.

3.2. Design and functionality of IoT nodes

The IoT node used in this system is designed for efficient and long-term monitoring of illegal logging activities in forested areas. Each node is integrated with a microcontroller board and a microphone, and it operates on a lithium battery. This design ensures both functionality and durability, allowing the node to operate in the field for extended periods with minimal maintenance.

The IoT node operates in two distinct modes: deep sleep mode and running mode. This dual-mode functionality is crucial for reducing power consumption and extending the battery life. In deep sleep mode, which lasts for 10 min, the node conserves energy by shutting down most of its operations, drawing only 5 μA of current. This low-power state significantly reduces the energy draw, contributing to the node's ability to run on a battery for at least 10 years. For every 10 min, the IoT node transitions to running mode for 10 s. During this brief period, the node activates its microphone, sampling the audio at a rate of 16 kHz to detect chainsaw sounds. The captured sound is then processed using a CNN TinyML model for accurate sound identification. This sophisticated AI model ensures high accuracy in detecting the specific noise patterns associated with illegal logging activities.

Once a chainsaw sound is detected, the node immediately sends an alarm signal to the LoRaWAN gateway, specifically the RAK7244. The RAK7244 is a high-performance LoRaWAN gateway equipped with a Raspberry Pi 4 and a built-in GPS module, supporting multiple channels and offering robust long-range communication. This gateway is designed for scalability and flexibility, making it an ideal choice for IoT applications in remote and large-scale environments. The gateway then forwards this signal to the cloud server for further processing and response coordination. This seamless communication chain enables real-time detection and rapid response to illegal logging activities.

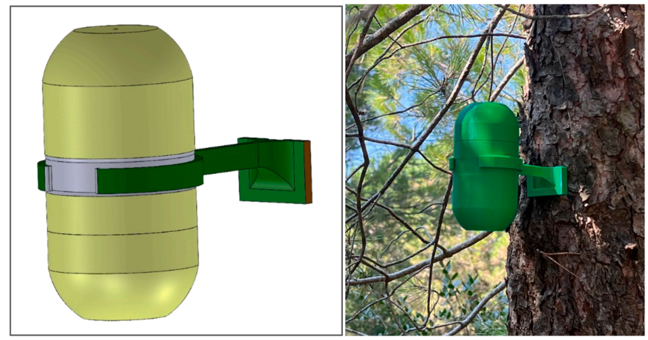


Fig. 3. Left, the 3D enclosure design; Right, the 3D printed prototype.

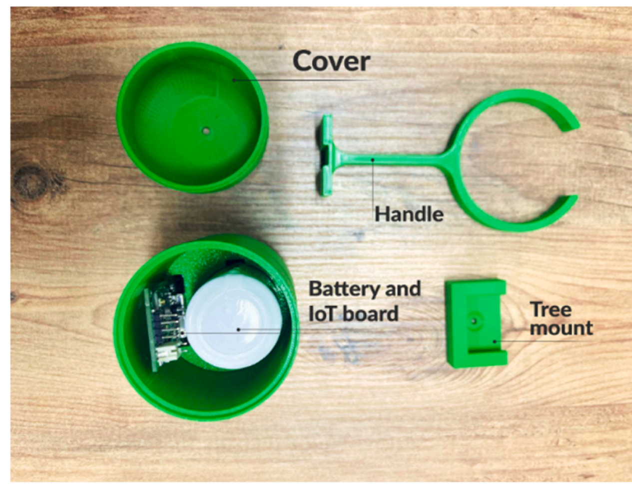


Fig. 4. Components of the IoT sound detection node.

The hardware configuration of the IoT node, including the microcontroller board, microphone, and power management system, is illustrated in Fig. 2. The IoT node is powered by an ESP32 microcontroller, known for its low power consumption, built-in Wi-Fi, and Bluetooth capabilities, making it ideal for IoT applications. The SPH8878LR5H-1 microphone from Knowles is used for sound detection, offering high performance with a flat frequency response and low phase distortion. It features a 67 dB(A) Signal-to-Noise Ratio (SNR) and a 134 dB SPL AOP, ensuring a large, distortion-free dynamic range for detecting chainsaw sounds. The power management system includes an 18Ah lithium battery, and an optimized circuit design that switches between active and sleep modes to extend battery life to at least 8 years. This robust and efficient design ensures that the IoT nodes are well-suited for deployment in remote and challenging environments, providing a reliable solution for continuous forest monitoring and illegal logging prevention.

3.3. Enclosure design for IoT node

A lightweight and durable enclosure has been designed and printed using a 3D printer to house the IoT node's components. The design is compact, accommodating the main board, microphone sensor, and battery within a single unit. This compact form factor ensures that all hardware elements fit securely inside the enclosure.

The enclosure is specifically designed to be mounted on trees as shown in Fig. 3. It features a small handle part that can be easily fixed to

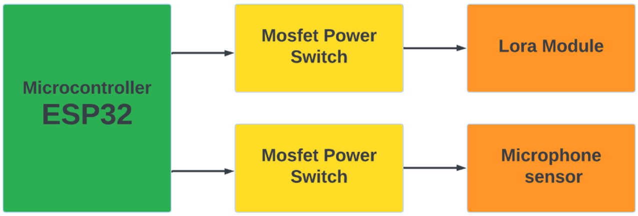


Fig. 5. Power Management Connection Diagram for IoT Node.

the tree, providing a stable attachment point. The main enclosure unit can then be fitted onto this handle, allowing for straightforward installation and removal.

One of the key functions of the enclosure is to protect the electronic components from environmental factors such as sun, rain, and varying weather conditions. The material used for printing the enclosure is ABS (Acrylonitrile Butadiene Styrene), known for its strength, durability, and resistance to weathering. This thoughtful design ensures that the IoT node remains functional and protected in outdoor settings, maintaining its performance and longevity.

Fig. 4 illustrates the various parts of the IoT node, including the Cover, which protects the internal components, the Handle for mounting or handling the node, the Battery and IoT board which powers the device and processes the sound detection, and the Tree Mount for securely attaching the node to a tree in the forest.

3.4. Power distribution system of the IoT node

To minimize the power consumption of the IoT node, an advanced power management technique utilizing MOSFET power transistors has been implemented. These transistors are connected and controlled by the microcontroller, allowing precise management of power distribution to the node's components.

In deep sleep mode, the microcontroller instructs the MOSFET transistors to completely cut off power to the LoRa module and the microphone sensor. This action is taken just before the microcontroller enters its low-power sleep state, ensuring that no unnecessary power is consumed by these components during this period. When the microcontroller wakes up, it signals the MOSFET transistors to restore power to both the LoRa module and the microphone sensor, allowing the node to perform its monitoring functions.

This technique significantly reduces overall power consumption, enabling the IoT node to operate on a lithium battery for at least 10 years without the need for battery replacement. This extended battery life greatly reduces maintenance costs and ensures reliable long-term operation of the IoT nodes in remote forest environments.

Fig. 5 shows the power management connection diagram, illustrating how the MOSFET transistors are integrated into the system to control power distribution effectively.

3.5. Chain sound detection using CNN model

3.5.1. Data collection for TinyML model

The data used to train the TinyML model was meticulously gathered from various sources to ensure robustness and accuracy in detecting chainsaw sounds. Primary data collection involved recording sound directly from the IoT nodes. In a controlled environment, field tests were conducted to record the sound of a real chainsaw using the IoT nodes. These recordings captured continuous chainsaw noise over a period of at least 10 min. To build a comprehensive dataset, the recorded audio was meticulously segmented into 1-second clips. Each of these clips represents a single sample, resulting in a total of 600 samples, where 1 sample equals exactly 1 s of chainsaw sound. Additionally, to expand the dataset, chainsaw recordings were sourced from YouTube. Several chainsaw recordings were downloaded and similarly split into 1-second clips, providing another 600 samples. This diverse collection of chainsaw sounds from different environments and sources enhanced the model's ability to generalize and accurately detect chainsaw noises in various conditions.

Table 2
Sources of the dataset.

Data Source	Description	Number of Samples
IoT Node Recordings Obtained in This Study	Chainsaw sounds recorded in controlled environment	600
YouTube Recordings (https://www.youtube.com/watch?v=c7FIeVUWRMU)	Chainsaw sounds from various recordings	600
Background Noise 1. https://www.kaggle.com/datasets/ouaraskhelilrafik/tp-02-audio 2. https://www.kaggle.com/datasets/rasmushaugland/initcarsound 3. https://www.kaggle.com/datasets/luisblanche/birdcall-background 4. https://www.kaggle.com/datasets/dejolilandry/asvpesdspeech-nonspeech-emotional-utterances	Bird calls, animal sounds, human voices, and vehicle noises	6000

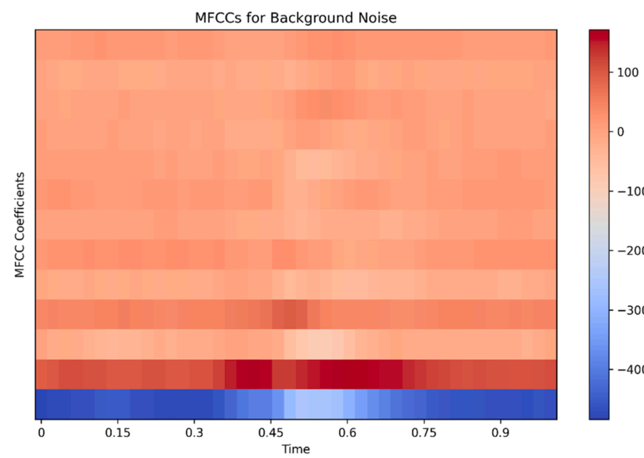


Fig. 6. MFCCs for background noise.

To further refine the TinyML model, extensive background noise data was collected directly through field recordings and sourced from online repositories. This included recording of bird calls, animal sounds, human voices, and vehicle noises. Over 6000 samples of these background sounds were integrated into the dataset. Incorporating these noise samples was crucial for training the AI model to distinguish between chainsaw sounds and other ambient noises accurately. By including these diverse audio samples, the TinyML model was optimized to operate effectively in real-world forest environments, reducing the likelihood of false positives and enhancing overall performance. Table 2 shows the sources and distribution of the dataset used for training the TinyML model.

3.5.2. Analysis of the dataset

The collected dataset was analyzed to ensure a balanced representation of chainsaw sounds and background noises, which is crucial for training an effective TinyML model. The analysis and feature extraction were conducted using Python, with the Librosa library employed to extract Mel Frequency Cepstral Coefficients (MFCCs) from the audio data. Fig. 6 shows the MFCCs for a sample of background noise. The Y-axis represents the MFCC coefficients, which capture the power spectrum of the sound, and the X-axis represents time. MFCCs are a common feature used in audio processing to represent the short-term power

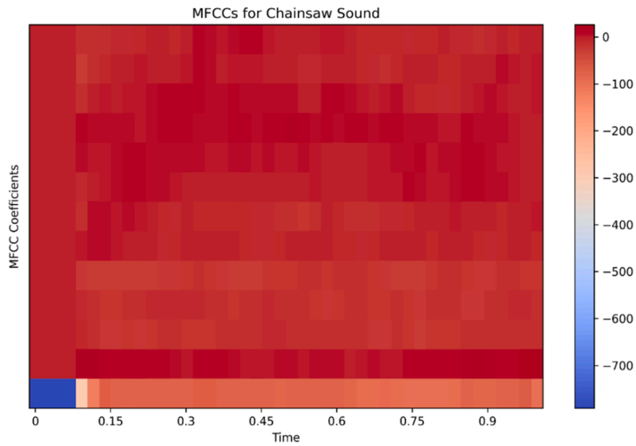


Fig. 7. MFCCs for chainsaw sound.

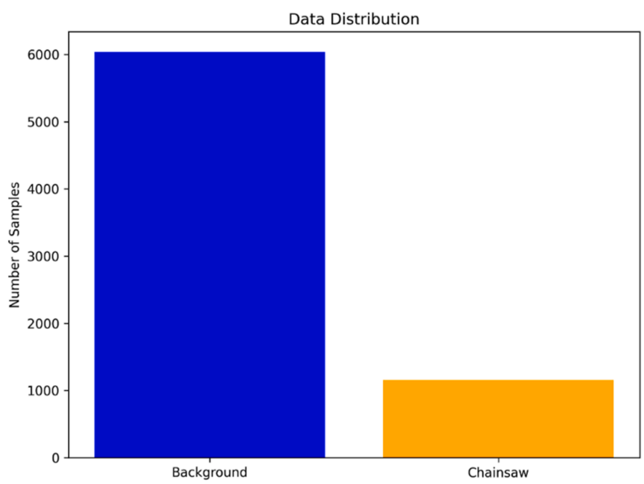


Fig. 8. Data distribution.

spectrum of a sound signal, helping to distinguish different types of sounds.

For the machine learning modeling, TensorFlow and Keras were utilized to develop the TinyML model. These tools enabled the creation of a CNN-based model optimized for accurate and efficient sound detection, essential for real-time environmental monitoring.

Fig. 7 displays the Mel Frequency Cepstral Coefficients (MFCCs) for a sample of chainsaw sound. Similar to the background noise figure, the Y-axis represents the MFCC coefficients, and the X-axis represents time. The distinct pattern in the MFCCs for the chainsaw sound helps the TinyML model differentiate it from other background noises.

The AI algorithm employed in the TinyML model is designed to detect chainsaw sounds even in the presence of background noises such as bird calls, human voices, or vehicle sounds. While the model was trained on distinct datasets, the characteristic sound of a chainsaw typically has a much higher amplitude compared to other environmental sounds. During testing, it was observed that the microphone can effectively capture the dominant chainsaw noise, even when other background sounds are present. The high energy and distinct frequency patterns of the chainsaw sound allow the model to identify it accurately, minimizing the impact of background noise on detection performance.

The distribution of samples in the dataset is shown in Fig. 8, highlighting the number of samples for background noise and chainsaw sounds. The Y-axis represents the number of samples, and the X-axis represents the categories. This distribution indicates that the dataset is imbalanced, with a larger number of background noise samples compared to chainsaw sounds. Despite this imbalance, the TinyML model is trained to accurately distinguish between chainsaw sounds and other ambient noises. The model's training process includes techniques to handle this imbalance, ensuring that it can effectively learn the characteristics of chainsaw sounds despite the disparity in sample numbers. These visualizations and explanations help in understanding the data characteristics and the model's robustness in detecting chainsaw sounds.

Table 3
Description of the CNN-based Chainsaw Sound Detector.

Layer Name	Input Size	Output Size	Specifications (Kernel Size, No of Kernels, Stride)
Input	(40, 1, 1)	(40, 1, 1)	N/A
Conv2D	(40, 1, 1)	(38, 1, 32)	Kernel Size: (3, 1), No of Kernels: 32, Stride: 1
MaxPooling2D	(38, 1, 32)	(19, 1, 32)	Pool Size: (2, 1), Stride: 2
Flatten	(19, 1, 32)	(608)	N/A
Dense	(608)	(64)	No. of Neurons: 64, Activation: ReLU
Dense (Output)	(64)	(2)	No. of Neurons: 2, Activation: Softmax

3.6. Designing the CNN for chainsaw sound detection using TinyML

3.6.1. Model architecture

The architecture of the CNN for detecting chainsaw sounds is designed to be efficient enough to run on TinyML devices while maintaining high accuracy. Table 3 provides a detailed description of each layer in the CNN model, including the input and output sizes and the specifications for each layer.

- Input Layer:

The input layer receives MFCC features extracted from audio files, which are reshaped to a size of (40, 1, 1). This represents 40 MFCC coefficients for a single time step, with a single channel.

- First Convolutional Layer:

This layer (Conv2D) applies 32 convolutional filters, each of size (3, 1), to the input data. The convolution operation helps to capture low-level features from the MFCC input. The activation function used is ReLU (Rectified Linear Unit), which introduces non-linearity into the model. The output size after this layer is (38, 1, 32), as the convolution reduces the spatial dimensions of the input.

- Pooling Layer:

Following the convolutional layer, a max pooling layer (MaxPooling2D) is used to reduce the spatial dimensions further. The pooling layer uses a pool size of (2, 1), which halves the size of the input in one dimension while keeping the other dimension unchanged. This layer helps to reduce the computational load and prevent overfitting. The output size after pooling is (19, 1, 32).

- Flatten Layer:

The flatten layer converts the 2D feature maps into a 1D vector. This transformation is necessary for connecting the convolutional layers to the dense (fully connected) layers. The output size after flattening is 608.

- First Dense Layer:

This dense layer has 64 neurons and uses the ReLU activation function. It processes the flattened vector and helps the model learn higher-

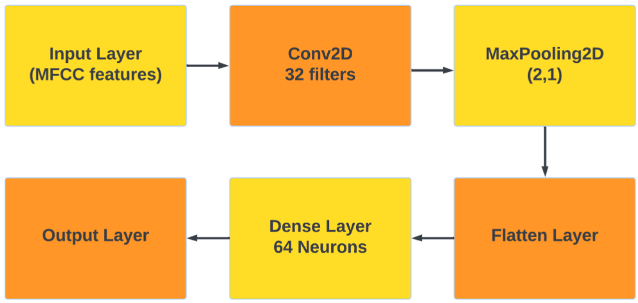


Fig. 9. Block Diagram of the CNN Architecture for Chainsaw Sound Detection.

level features from the data. The output size of this layer is 64.

- Output Layer:

The final layer is a dense layer with 2 neurons, corresponding to the two classes (chainsaw sound and background noise). It uses the softmax activation function to output probabilities for each class, ensuring the sum of the outputs equals 1. The output size of this layer is 2.

Table 3 provides a comprehensive overview of the CNN architecture used for chainsaw sound detection. Each layer is described in terms of its input and output sizes, along with specific configurations like kernel size, number of kernels, and stride for convolutional layers. This structured format helps in understanding the flow of data through the network and the transformations applied at each step.

The architecture ensures that the model is capable of detecting chainsaw sounds with high accuracy while being efficient enough to run on low-power TinyML devices. The use of convolutional layers helps in extracting meaningful features from the audio data, while the pooling and dense layers contribute to reducing dimensionality and learning complex patterns, respectively. The final output layer classifies the input into one of the two categories, enabling effective detection of illegal logging activities.

3.6.2. Block diagram of the CNN architecture

The block diagram (Fig. 9) below illustrates the architecture of the proposed CNN model for detecting chainsaw sounds. It provides a visual representation of the data flow through each layer, from the input of MFCC features, progressing through convolutional and pooling layers, and culminating in the final classification output. This diagram highlights how the model processes audio data step-by-step, enhancing the understanding of its structure and operational flow within the detection system.

3.6.3. Equations for CNN models

Convolution Operation

The convolution operation involves applying a filter to the input data to produce a feature map. The output of a convolutional layer can be computed as:

$$Output(i,j,k) = ReLU\left(\sum_{m=1}^{M}\sum_{n=1}^{N} \times \sum_{c=1}^{C} Input\ (i+m-1,\ j+n-1,\ c).Filter(m,n,c,k)\right) \tag{1}$$

Where:

- Output(i,j,k) is the output value at position (i,j) for the k -th filter.
- Input($i + m - 1$,$j+n-1$, c) is the input value at position ($i + m - 1$, $j+n-1$) for the c-th channel.
- Filter(m,n,c,k) is the filter value at position (m,n) for the c -th channel and k -th filter.
- Bias(k) is the bias term for the k -th filter.
- ReLU is the Rectified Linear Unit activation function.

Max Pooling Operation

Max pooling reduces the spatial dimensions of the input by taking the maximum value over a defined window. The output of a max pooling layer can be computed as:

$$Output\ (i,j,k) = max_{m=1}^{P} max_{n=1}^{Q} Input(i+m-1,j+n-1,k) \tag{2}$$

Where:

- Output(i,j,k) is the output value at position (i,j) for the k-th channel.
- Input($i + m - 1$, $j+n-1$, k) is the input value at position ($i + m - 1$, $j+n-1$) for the k -th channel.
- P and Q are the height and width of the pooling window.

Fully Connected Layer

The fully connected (dense) layer computes the output as a weighted sum of the input values, followed by an activation function. The output of a dense layer can be computed as:

$$Output(k) = ReLU\left(\sum_{i=1}^{I} Input(i).Weight(i,k) + Bias(k)\right) \tag{3}$$

Where:

- Output(k) is the output value for the k -th neuron.
- Input(i) is the input value for the i -th input.
- Weight(i, k) is the weight connecting the i -th input to the k -th neuron.
- Bias(k) is the bias term for the k -th neuron.
- ReLU is the Rectified Linear Unit activation function.

Softmax Activation

The softmax function is used in the output layer to convert the raw output scores into probabilities. The softmax function can be computed as:

$$Softmax(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{J} e^{z_i}} \tag{4}$$

Where:

- z_i is the raw output score for the i th class.
- J is the total number of classes.
- Softmax(z_i) is the probability for the i th class.

3.6.4. Dataset division: training and testing

After extracting MFCC features from the audio files and preparing the dataset, the next crucial step involves dividing the dataset into training, validation, and testing sets. This ensures the model is trained on a portion of the data, validated on another portion to tune hyperparameters, and evaluated on a separate, unseen portion to gauge its generalization performance.

The dataset was divided using the "train_test_split" function from the "sklearn.model_selection" module. Initially, 25 % of the data was allocated for testing, while 75 % was reserved for training. To further refine the model, 20 % of the training data was used for validation. This approach ensures that the model can learn from a broad set of training samples while being fine-tuned with validation data and evaluated on the test set for unbiased performance metrics.

Given the dataset's imbalance between chainsaw sounds and background noise, we ensured that both classes were well-represented across the training, validation, and testing sets to avoid biased learning. Additionally, techniques such as data augmentation were employed to artificially expand the training set and improve the model's ability to generalize to new data.

3.7. Autonomous deployment of intervention drone

3.7.1. Optimal deployment of IoT nodes for forest monitoring

The deployment of IoT nodes in forested areas is crucial for effective monitoring and prevention of illegal logging activities. To maximize the coverage area and ensure efficient use of resources, the nodes are strategically placed in a hexagonal grid pattern. This section explains the deployment process, the rationale behind the chosen method, and the mathematical calculations involved. Additionally, the acoustic coverage of the microphones integrated with each node is considered to ensure accurate detection of chainsaw sounds.

3.7.2. Deployment strategy

The goal of deploying IoT nodes is to cover the largest possible area with minimal overlap, ensuring comprehensive monitoring. A hexagonal grid pattern is chosen because it provides optimal coverage with the least amount of overlap between adjacent nodes.

3.7.3. Hexagonal grid pattern

In a hexagonal grid pattern, each node is positioned at the vertices of adjacent hexagons. This arrangement is efficient for covering large areas because it minimizes gaps and overlaps. The distance between the centers of two adjacent nodes in a hexagonal pattern is $\sqrt{3} \times r$, where r is the radius of the coverage area of a single node.

3.7.4. Acoustic coverage and microphone sensitivity

Each IoT node is equipped with a microphone that must effectively capture the sound of a chainsaw. The sensitivity of the microphone and its ability to detect chainsaw sounds depend on the sound pressure level (SPL) measured in decibels (dB). Chainsaw sounds typically range from 110 to 120 dB at the source. For the microphone to detect the chainsaw sound clearly, it must be sensitive enough to pick up the sound from a distance, accounting for the attenuation of sound over distance. The effective range of the microphone can be determined based on its sensitivity and the expected SPL of the chainsaw sounds.

3.7.5. Area calculations

To understand the efficiency of the deployment strategy, the area covered by each node and the total area covered by all nodes are calculated.

Area Covered by One Node:

Hexagon Area: The area of a hexagon is typically calculated using the formula:

$$A_{hexagon} = \frac{3\sqrt{3}}{2} r^2 \tag{5}$$

Where r is the radius (or distance from the center to any vertex) of the hexagon.

Hexagon Area Calculation:

If $r = 100$ *meters* :

$$A_{hexagon} = \frac{3\sqrt{3}}{2} \times (100)^2 \approx 25980.76 \text{ square meters}$$

Non-Overlap Area Calculation:

The non-overlap area per hexagon might be approximated by:

$$\text{Non} - \text{overlapping area per hexagon} = \left(\pi(100)^2 - \frac{3\sqrt{3}}{2} \times (100)^2\right) \div 6 \approx 905.86 \text{ square meters}$$

Non-overlapping Area: The calculation accounts for the non-overlapping area by subtracting the overlapping segments between the adjacent hexagons. The non-overlap area for each hexagon is calculated as 905.86 square meters

Total Area Calculation:

The total area covered by the five hexagons includes the sum of the areas of the hexagons plus the 16 non-overlapping sections:

$$\text{Total Area} = 5 \times A_{hexagon} + 16 \times 905.86 \approx 144397.58 \text{ square meters}$$

Table 4
Locations and distances of IoT Nodes to gateway.

Node	Latitude	Longitude	Distance to Gateway (meters)
Node 1	41.144333	28.727532	840.12
Node 2	41.145112	28.728881	928.63
Node 3	41.143554	28.728881	975.32
Node 4	41.144333	28.730230	1057.50
Node 5	41.142775	28.730230	1112.31

3.7.8. Deployment process

- Node Placement:

Since the IoT nodes do not have built-in GPS, each node was manually installed in a hexagonal pattern, with its precise location recorded using a GPS navigator as shown in Table 4. These recorded coordinates were then inserted into the cloud server to map the exact positions of the nodes. This process ensures that the system can accurately monitor and respond to activities at each node's location, enhancing the effectiveness of the detection and prevention mechanism.

- Visualization:

The hexagonal deployment of the IoT nodes is illustrated in Fig. 10, where each hexagon represents the coverage area of a node. Different colors indicate distinct coverage areas, with red dots marking the center of each hexagon and a blue dot marking the geometric center of the overall hexagonal pattern. The calculations and the hexagonal deployment strategy demonstrate the efficiency of this method in covering a large area with minimal overlap.

The total area covered by the five nodes is approximately 144,397.58 m^2s. This strategic arrangement ensures that the IoT nodes are optimally placed to maximize coverage, enhancing the monitoring system's effectiveness in detecting illegal logging activities.

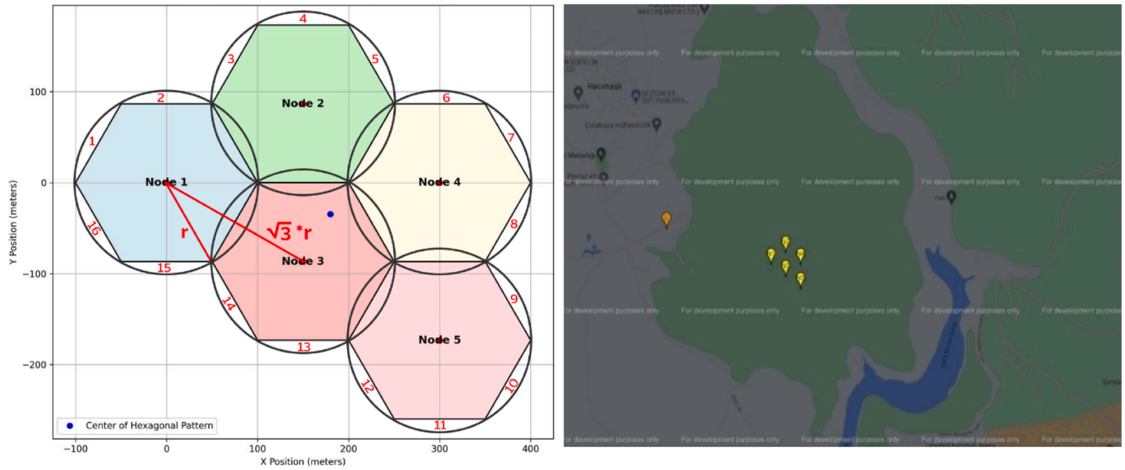
The provided map visualization represents the strategic deployment of IoT nodes and a Gateway for forest monitoring in a hexagonal grid pattern. Each marker on the map corresponds to a specific IoT node, and the map is displayed in satellite view to provide a realistic representation of the terrain as shown in Fig. 10. b.

3.7.9. Acoustic considerations

To ensure the microphones capture chainsaw sounds effectively, the SPL and the effective range of the microphones must be considered. If a chainsaw generates a sound of 120 dB at the source, and considering a standard attenuation rate, the microphones should be sensitive enough to detect this sound from a distance. The placement of nodes is optimized not only for spatial coverage but also for acoustic detection, ensuring that any chainsaw activity within the coverage area is detected promptly.

3.8. Autonomous drone for illegal logging detection and response

In the proposed project, a hexacopter drone equipped with a Pixhawk flight controller was integrated to enhance the response capabilities of the monitoring system as shown in Fig. 11. The drone is powered by a 6S 16,000 mAh battery, allowing it to fly for up to 40 min on a single charge, covering a maximum distance of approximately 26 kms. Connectivity is established through a 4 G GSM modem, specifically the SIM COM A7670 G model, which enables the drone to communicate directly with the cloud server in real-time. The integration is managed using Mission Planner software, which allows for seamless coordination between the drone and the cloud server.



(a) (b)

Fig. 10. IoT nodes deployment and coverage areas: (a): Hexagonal deployment of the IoT nodes of optimal coverage, (b): node and gateway positions.

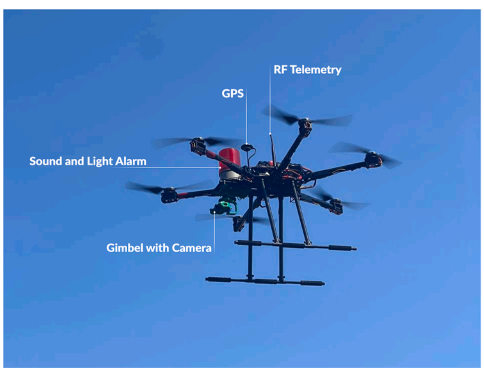


Fig. 11. Autonomous AI-powered UAV.

When an IoT sound detection node identifies and confirms the sound of a chainsaw, it sends an alert to the cloud server with the precise GPS coordinates of the detected sound. The cloud server then processes this information and sends the location details to the drone via the GSM modem. Upon receiving the coordinates, the drone autonomously takes off and navigates to the specified location. The Pixhawk flight controller ensures that the drone's flight is stable and precise, enabling it to perform effective aerial surveillance. The entire process is managed using Mission Planner software, a powerful ground control station application that facilitates the seamless integration between the cloud server and the drone. Mission Planner allows for real-time monitoring, mission planning, and autonomous flight control, ensuring that the drone can efficiently respond to alerts and perform surveillance tasks with accuracy.

Once at the location, the drone conducts a detailed survey, capturing high-resolution images or streaming live video footage to verify the presence of illegal logging activities. The live video feed is transmitted back to the cloud server in real time, where it is processed for immediate analysis and decision-making. For this purpose, an Amazon Web Services (AWS) server is utilized, providing robust and scalable cloud computing resources. At the server side, ready-made AI tools from AWS are employed to detect the presence of persons or suspicious activities within the footage, leveraging advanced machine learning models optimized for real-time video analysis. If any illegal activity is detected, the drone is equipped with a light and sound alarm system that activates to warn the perpetrators and deter further illegal actions. The use of Mission Planner software ensures that the flight paths, waypoints, and specific actions of the drone are meticulously planned and executed,

Table 5
Bill of Materials (BoM) for the UAV-Based IoT System.

Component	Specification	Quantity	Cost (per unit)	Total Cost
ESP32 Microcontroller	Low-power, Wi-Fi, and Bluetooth-enabled	5	$10	$50
Microphone (SPH8878LR5H-1)	Sensitivity: −38 dBV/Pa, 120 dB SPL	5	$5	$25
Battery (18Ah Lithium)	Long-life, 8 years of power	5	$20	$100
LoRaWAN Gateway	Custom-built (no cost for gateway)	1	N/A	N/A
Drone (Hexacopter)	Pixhawk controller, 4 G GSM modem, camera, alarm	1	$900	$900
3D Printed Enclosure	ABS, weather-resistant	5	$3	$15
Total Cost				$1090

enhancing the efficiency and effectiveness of the monitoring operation. This integration of AWS cloud services, AI tools, and Mission Planner software creates a highly responsive and automated system capable of real-time monitoring and intervention.

3.9. Cost analysis and comparison with existing methods

In this section, we present a cost analysis of the proposed UAV-based IoT system for chainsaw sound detection and compare it with existing methods used in forest monitoring, such as satellite imagery and traditional ground patrols.

- Hardware Costs: Each IoT node, comprising a high-performance microphone (SPH8878LR5H-1), an ESP32 microcontroller, an 18Ah lithium battery, and a 3D-printed ABS enclosure, costs approximately $50 per unit as shown in Table 5. The total cost of the IoT nodes, including five units, amounts to $250. The UAV used in this system, equipped with a high-resolution camera, a Pixhawk flight controller, a 6S 16,000 mAh battery, a sound and light alarm unit, a 4 G GSM modem, and a gimbal for camera stabilization, costs $900. Depending on additional specifications, the cost of the UAV may range between $1000 and $1500.
- Operational Costs: The IoT nodes are designed for extremely low power consumption, with a battery life of up to 8 years, significantly reducing maintenance costs. The operational cost for cloud-based

data processing on Amazon Web Services (AWS) is approximately $30 per month, covering data storage, real-time processing, and server management. Since we utilize our own LoRaWAN gateway, there are no additional costs for data transmission between nodes and the cloud server.

- Deployment Costs: The estimated cost to deploy the system across a 10 km^2 forest area is approximately $5000, which includes the hardware for the IoT nodes and UAVs, as well as installation costs for optimizing node placement and coverage. On a per-square-kilometer basis, this amounts to $500 per km^2, offering significant cost savings over alternative monitoring methods like satellite imagery or ground patrols.

Comparison with Existing Methods:

- Satellite Monitoring: Satellite imagery costs can reach up to $500 per square kilometer per month for high-resolution imagery. In comparison, the proposed system can cover the same area with much lower monthly operational costs, and it provides real-time data with higher accuracy.
- Ground Patrols: Traditional ground patrols incur significant labor costs, with an estimated annual cost of $10,000–$20,000 for a similar coverage area, depending on personnel and logistical requirements. The UAV-based system offers continuous monitoring at a fraction of this cost.

3.10. *Efficient multi-drone deployment for IoT-triggered alerts*

At the ground stations, a fleet of drones is continuously connected to the cloud server, ready to respond to any alerts triggered by the IoT nodes. When multiple IoT nodes send an alarm, the system is designed to handle several scenarios efficiently:

Simultaneous Alerts from Nearby Nodes:

If both IoT nodes send alarms at the same time and the distance between them is <500 m, a single drone is capable of covering both areas. The drone will be deployed to a central position between the two nodes, flying at an altitude of 100 m. This height, combined with the high-resolution camera onboard, allows the drone to effectively monitor both areas simultaneously, ensuring no illegal activities go undetected.

Sequential Alerts from Nearby Nodes:

In cases where the alarms do not occur simultaneously but are still within close proximity, the same drone will first investigate the area corresponding to the first alarm. After verifying that region, it will then proceed to the second location, ensuring comprehensive coverage of both areas.

Alerts from Distant Nodes:

If the IoT nodes that send alarms are located in different regions or areas that are >500 m apart, the system will automatically deploy multiple drones. Each drone will be dispatched to the specific area corresponding to its respective alarm. This ensures that all regions are monitored effectively without delay.

The system's ability to deploy multiple drones simultaneously, combined with the use of high-resolution cameras and optimized flight paths, ensures that our monitoring network remains robust and responsive. By managing these scenarios efficiently, our approach minimizes the risk of overlooking any illegal logging activities, regardless of where or when they occur.

4. Validation and results

This section presents the validation process, and the results obtained from the deployment of the system. The effectiveness of the IoT sound detection nodes, the autonomous drone response, and the integration with the cloud server were rigorously tested. The methodologies used to validate each component are detailed, along with an analysis of the performance metrics and outcomes. The results demonstrate the system's reliability and efficiency in detecting and responding to illegal logging activities.

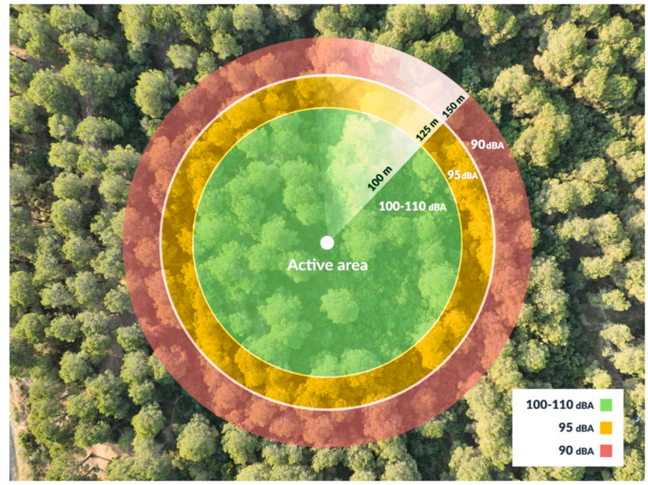


Fig. 12. Active area of the sound detector IoT node.

Table 6
Detection performance at various distances.

Distance (r)	Measured dBA	Detection Accuracy	Stability
50 m	110 dBA	High (95 %–100 %)	Stable
75 m	105 dBA	High (95 %–100 %)	Stable
100 m	100 dBA	High (95 %–100 %)	Stable
125 m	95 dBA	Medium (70 %–85 %)	Unstable
150 m	90 dBA	Low (50 %–70 %)	Unstable

4.1. *Testing the sound detection system*

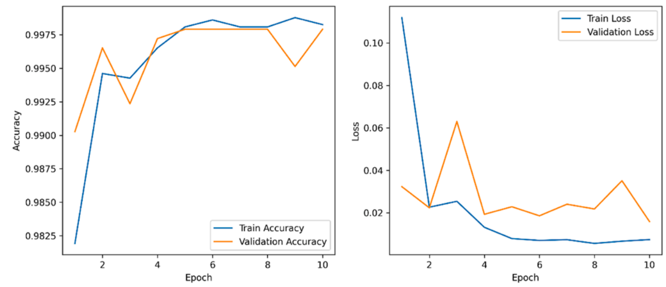
To validate the effectiveness of the sound detection system, real-world tests were conducted to determine the optimal coverage area of the microphone for accurately detecting chainsaw sounds. The primary objective was to identify the maximum radius (r) within which the microphone can reliably detect chainsaw sounds.

A series of tests were set up at varying distances from the microphone, incrementally increasing the radius to observe the detection performance. A digital sound level meter measured the sound pressure levels in decibels (dBA) at each distance. The microphone was positioned at a fixed location, and the chainsaw was operated at distances of 50 m, 75 m, 100 m, 125 m, and 150 m respectively, as shown in Fig. 12. At each distance, the chainsaw was operated while the digital sound level meter recorded the dBA levels, and the sound detection system monitored the microphone input to detect the chainsaw sound.

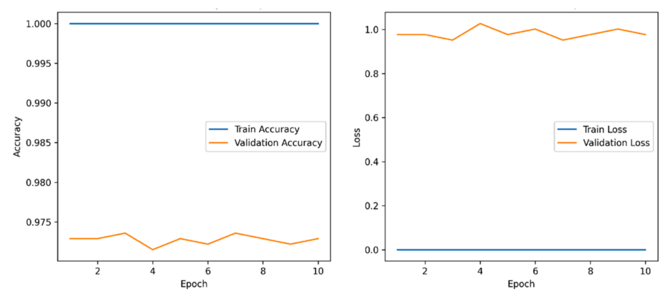
The tests revealed that the microphone could reliably detect the chainsaw sound up to a radius of 100 m. Beyond this distance, the detection accuracy decreased, and the system's performance became unstable. The dBA readings provided a clear indication of the sound pressure level, correlating well with the detection results.

A series of tests were set up at varying distances from the microphone, incrementally increasing the radius to observe the detection performance. The dBA readings provided a clear indication of the sound pressure level, and the detection accuracy was assessed at each distance. In Table 6, the "Detection Accuracy" column has been categorized into High, Medium, and Low levels, with corresponding ranges of accuracy percentages provided for each.

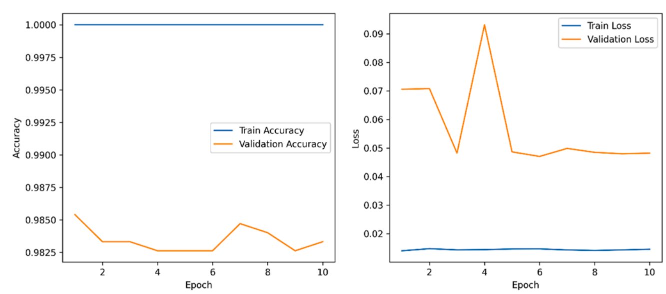
- High Accuracy (95 %–100 %) indicates that the detection system correctly identifies the chainsaw sound nearly all the time.



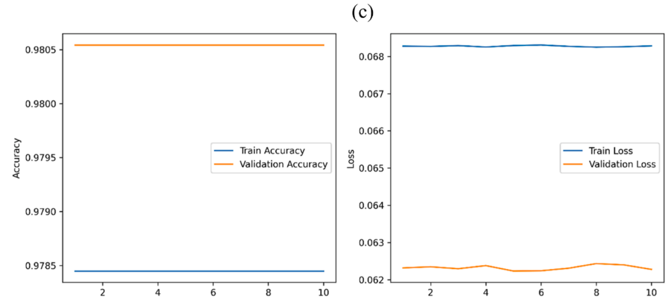
(a)



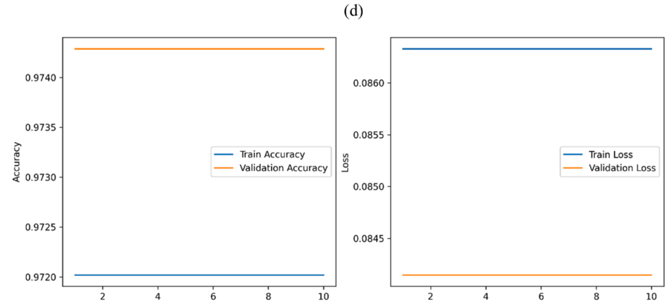
(b)



(c)



(d)



(e)

Fig. 13. Epoch vs. accuracy and loss for all models: (a) CNN, (b) decision tree, (c) random forest, (d) SVM, and (e) logistic regression.

- Medium Accuracy (70 %−85 %) suggests a moderate success rate, with the system correctly identifying the chainsaw sound most of the time, but with some errors.
- Low Accuracy (50 %−70 %) reflects a lower success rate, where the system's ability to correctly identify the chainsaw sound is significantly reduced, likely due to increased distance or interference.

This table clearly defines what each level of detection accuracy means, providing a more detailed understanding of the system's performance at various distances. The testing confirmed that the microphone's optimal coverage area is within a 100-meter radius for accurate and stable detection of chainsaw sounds. These findings ensure that the sound detection nodes can effectively monitor illegal logging activities within this range, providing a robust solution for the integrated monitoring system.

4.2. TinyML sound detection results

The performance of various machine learning models—Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and CNN—was evaluated for the task of chainsaw sound detection. The models were compared based on their accuracy and loss metrics, as summarized in Fig. 13.

The results indicate that the CNN model outperforms all other models in both accuracy and loss. This superior performance can be attributed to several factors inherent to CNNs and the nature of the dataset.

CNNs excel at automatically learning and extracting features from raw data. In the context of audio data, such as the chainsaw sound recordings used in this study, CNNs can effectively capture temporal and spectral patterns. This capability allows CNNs to identify complex features that are critical for accurate sound classification. The automatic feature extraction process reduces the need for extensive manual feature engineering, which is required for traditional machine learning models.

The accuracy and loss metrics highlight CNN's advantages. The CNN achieved a significantly higher accuracy than the other models, with a value of 0.9975. In comparison, Random Forest and SVM, which are also powerful classifiers, achieved accuracies of 0.9835 and 0.9809, respectively. Logistic Regression and Decision Tree lagged slightly behind, with accuracies of 0.9745 and 0.9740, respectively. The loss metric further emphasizes CNN's superiority. With a loss of 0.0185, the CNN model demonstrates excellent generalization to unseen data. In contrast, Decision Tree exhibited a notably high loss of 0.9520, indicating overfitting and poor generalization. Random Forest and SVM showed more competitive loss values of 0.0536 and 0.0570, respectively, but still fell short of CNN's performance. Logistic Regression's loss of 0.0840, while relatively low, suggests that it cannot capture the intricate patterns as effectively as CNN.

The CNN model outperformed all other models, achieving the highest accuracy and the lowest loss. Its ability to automatically learn hierarchical features from raw audio data gives it a significant edge in this application. CNN's architecture, tailored for grid-like data such as audio spectrograms, makes it the most suitable model for the task of chainsaw sound detection. The comprehensive evaluation highlights the CNN model as the most effective for detecting chainsaw sounds in audio recordings. Its superior performance in both accuracy and loss metrics underscores its capability to handle complex patterns in the data. While other models like Random Forest and SVM showed competitive performance, they were ultimately outmatched by CNN's advanced feature extraction and generalization abilities. This study validates the use of CNNs for sound detection tasks and supports their application in real-world environmental monitoring systems.

4.3. Power consumption test of the IoT node

The power consumption test of the sound detection IoT node was conducted to evaluate its battery efficiency and longevity. The node operates for 10 s to detect chainsaw sounds and then sends the results across the LoRaWAN network before entering a 10-minute sleep mode to conserve battery power. This cycle is continuously repeated to optimize battery usage and extend the node's operational lifespan.

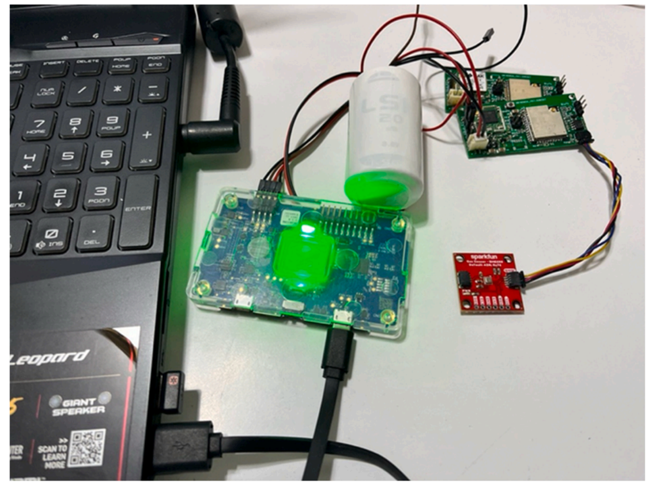


Fig. 14. Testing the power consumption of the IoT sound detection node.

To accurately measure the power consumption, the IoT node was connected to the Power Profiler Kit II for a duration of 24 h, as shown in Fig. 14. This setup allowed for precise monitoring of power consumption during both the operational and deep sleep modes. The Power Profiler Kit II is equipped to measure and record power usage, providing detailed data for analysis. The recorded data was stored on a laptop for further examination.

The Power Profiler Kit II program was configured to record 100 samples per second over the 24-hour period, resulting in nearly 8 million samples stored in a CSV file. This extensive dataset provided a comprehensive view of the IoT node's power consumption patterns.

Fig. 15 displays the power consumption data for the IoT node over various time intervals: 10 s, and 24 h. The spike around 45 mA, as seen in Fig. 14(b), occurs during the initial startup phase of the IoT node's running mode. This brief surge in current is typical when the microcontroller initializes and begins processing tasks, such as activating the microphone and running the CNN model for sound detection. Although this spike is significantly higher than the node's average running current of 15.67 mA, and 7.51 μA during the sleep mode, it is very short in duration and does not significantly affect the overall power consumption. Consequently, it has a negligible impact on the average power consumption, which remains approximately 276.5 μA over the 24-hour period. This transient spike is normal behavior in many IoT devices during the transition from sleep to active mode, particularly when initiating high-power tasks.

4.3.1. Battery life calculation

To further analyze the battery life, the operational duration with an 18 Ah battery was calculated. Here are the detailed calculations:

Convert Time to Hours:

Sleep Mode: 10 min is equal to $\frac{10}{60} = \frac{1}{6}\,hours$

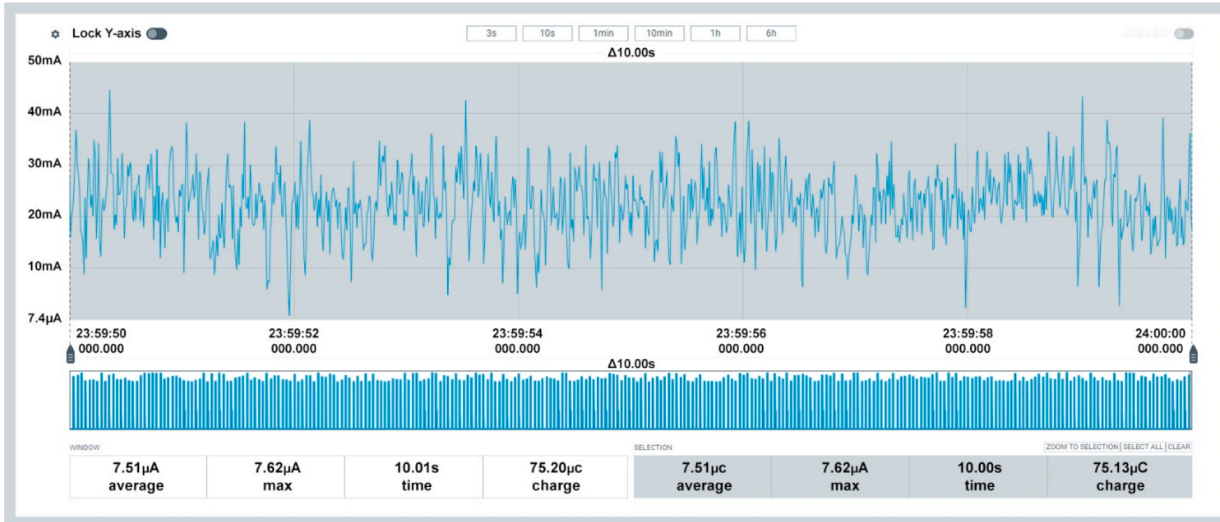
Running Mode: 10 s is equal to $\frac{10}{3600} = \frac{1}{360}\,hours$

Calculate Energy Consumption:

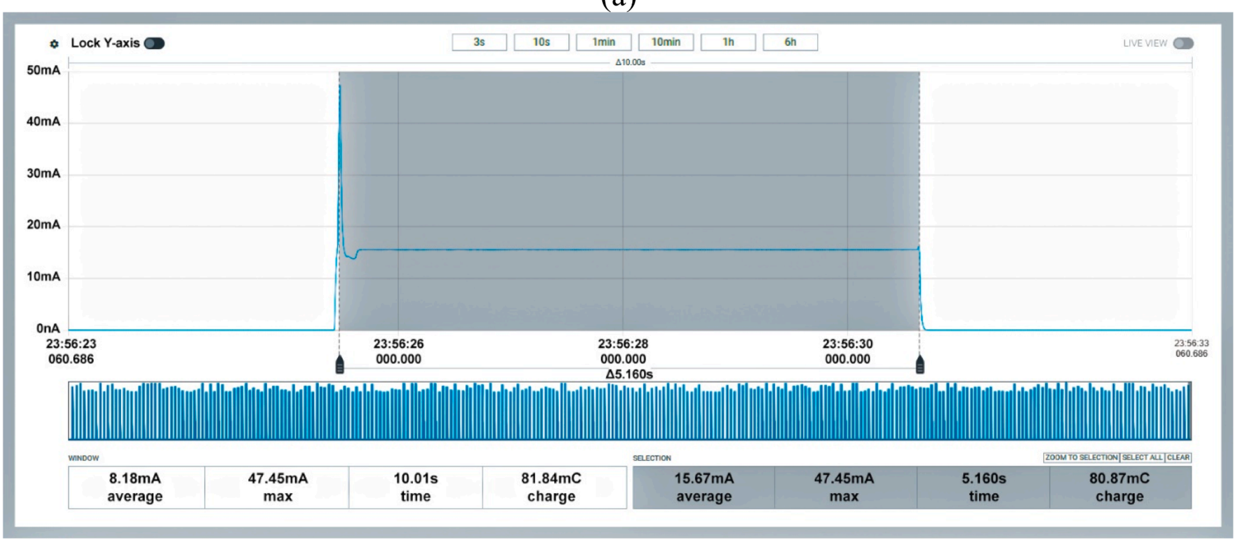
Sleep Mode Energy Consumption:

$$\text{Energy (Sleep Mode)} = 7.51\mu A \times \frac{1}{6}\,hours = 1.25\mu Ah$$

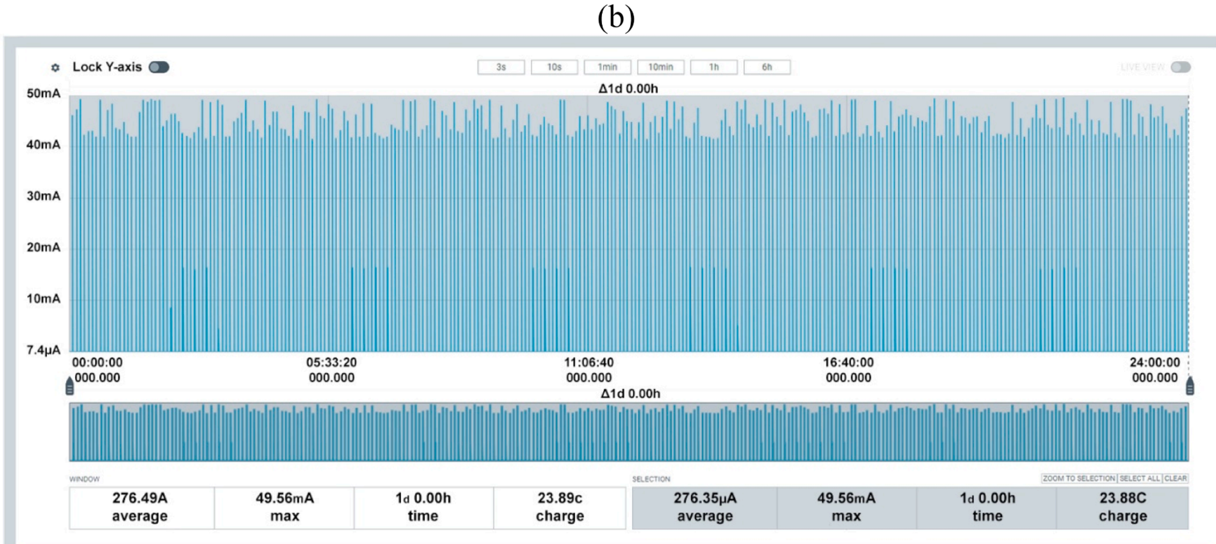
Running Mode Energy Consumption:



(a)



(b)



(c)

Fig. 15. Analysis of Power Consumption in IoT Nodes: (a) Zoom In View for Average Current Measurement during Sleeping Mode, (b) Zoom In View for Average Current Measurement during Running Mode, and (c) Average Current Measurement for a Period of 24 h.

Table 7
Response time and drone flight time for iot sound detection system.

Experiment #	IoT Node Response Time (minutes)	Drone Flight Time (minutes)
1	6:25	4:45
2	2:15	4:56
3	7:13	5:00
4	4:45	4:41
5	5:50	4:49
6	1:19	4:47
7	9:30	5:05
8	6:20	4:43
9	3:45	4:49
10	7:44	4:57

$$\text{Energy (Running Mode)} = 15.67\ mA \times \frac{1}{360} hours$$
$$= 15 \times 1000\mu A \times \frac{1}{360} hours = 43.52\mu Ah$$

Calculate Average Power Consumption:
Total Energy Consumption per Cycle:

$$\text{Total Energy per Cycle} = 1.25\mu Ah + 43.52\mu Ah = 44.77\mu Ah$$

Total Time per Cycle:

$$\text{Total Time per Cycle} = \frac{1}{6} + \frac{1}{360} \approx 0.168\ hours$$

Average Power Consumption:
Calculate Battery Life:

$$\text{Battery Capacity} : 18Ah = 18 \times 10^6 \mu Ah = 18,000,000\mu Ah$$

Battery Life in Hours:

$$\text{Battery Life} = \frac{18,000,000\mu Ah}{276.49\mu A} \approx 65,101\ hours$$

Battery Life in Days:

$$\text{Battery Life in Days} = \frac{65,101\ hours}{24 hours/day} \approx 2,712,57\ days$$

Battery Life in Years:

$$\text{Battery Life in Years} = \frac{2,712,57\ days}{365.25\ days/year} \approx 7.5\ years$$

4.3. *Response time analysis*

To evaluate the response time of the IoT sound detection node, multiple tests were conducted to determine the duration from the moment a sound is detected to the time the IoT node sends an alarm response to the LoRaWAN Gateway, which then forwards it to the cloud server. The variability in response time is attributed to the IoT node's operational cycle, which involves 10 s in active mode and 10 min in deep sleep mode. During sleep mode, the node is unable to detect sound, which explains the fluctuations in response time observed during testing.

4.3.1. *Testing procedure*

A series of 10 tests were performed to measure the response time of the IoT sound detection node. Table 7 displays the results of these experiments, illustrating the variability in response time due to the node's operational cycle. Additionally, the time taken for the drone to reach the fire spot from its location 6 km away from the IoT sensing node was measured. All tests were conducted on the same day under consistent wind conditions, with a wind speed of 11 km/h.

The IoT node response times varied significantly across the experiments, ranging from 1:19 min to 9:30 min. This variability is primarily due to the node's operational cycle, as it can only detect sounds during its 10-second active mode and remains inactive during the 10-minute sleep mode. Any sound occurring during the sleep mode goes undetected until the node wakes up and enters the active mode.

The drone's flight time to reach the fire spot was relatively consistent, ranging from 4:41 min to 5:05 min. This consistent response indicates the reliability of the drone's autonomous flight capabilities, despite the variability in IoT node response times.

The response time analysis highlights the impact of the IoT node's operational cycle on its ability to detect and respond to sound events. While the drone's flight time remains reliable and consistent, the IoT node's response time can vary significantly due to its periodic sleep mode. This underscores the importance of optimizing the operational cycle of IoT nodes to minimize response times and improve the overall efficiency of the monitoring system.

4.4. *Drone-based real-time human detection and alarm system*

The IoT nodes, equipped with microcontrollers and microphones, detect chainsaw sounds using a CNN model and send alarm signals via LoRaWAN to a gateway. The gateway forwards these signals to a cloud server, which processes the alerts and sends location data to a drone. The drone streams live video back to the cloud for AI-based human presence detection. If a human is detected, the cloud commands the drone to activate sound and light alarms to deter illegal logging activities. This entire workflow is illustrated in Fig 16.

The real-time monitoring system utilizes drones and AI to detect illegal logging activities. The image shown in Fig. 17A was captured by a drone equipped with a camera, part of the real-time monitoring system for detecting illegal logging activities. The drone transmits live video streaming to the cloud, where frames are processed using AI to detect the presence of humans. In this particular image, the AI has successfully identified a person holding a chainsaw, indicated by the bounding box around the individual.

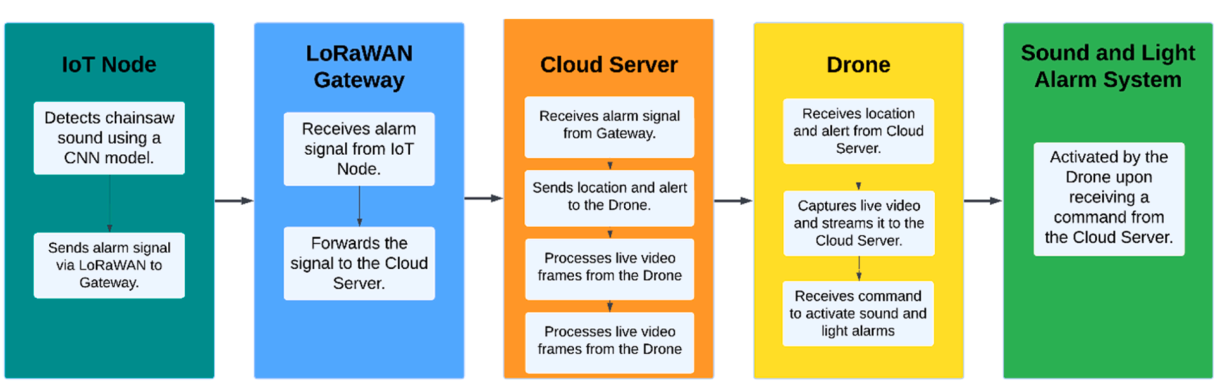


Fig. 16. Block diagram of real-time human detection and alarm system.

Fig. 17. Drone-captured image demonstrating human detection in a forested area: (a) image illustrating the detection of a human presence within the forest, (b) AI-powered drone arriving at the designated detection area.

Upon detecting a human in the area from which an alarm was previously triggered by an IoT sound detection node, the cloud server sends a command back to the drone to activate both sound and light alarms. This response aims to deter the detected individual from continuing illegal logging activities. The system's ability to provide real-time detection and immediate feedback enhances its effectiveness in preventing illegal logging, combining advanced AI techniques with practical field applications.

5. Conclusion

This research presents a comprehensive and innovative solution to the pervasive issue of illegal logging through the integration of UAVs, IoT, and AI technologies. The proposed system, which incorporates low-cost IoT nodes equipped with microphones and microcontrollers, leverages a CNN model to accurately detect chainsaw sounds. The use of a special power-saving technique ensures that these IoT nodes can operate for at least 8 years on a single battery, making the system both sustainable and cost-effective.

The IoT nodes communicate via a LoRaWAN network, transmitting alerts to a cloud server that processes the data in real-time. The deployment of a drone equipped with a visual camera further enhances the system's capability by providing live video streaming to the cloud, where AI algorithms detect human presence. This enables immediate activation of sound and light alarms to deter illegal loggers, thereby integrating both passive detection and active intervention mechanisms.

Experimental results validate the efficacy of the system, demonstrating the IoT nodes' ability to detect chainsaw sounds up to a distance of 100 m. The CNN model achieved an impressive accuracy of 99.37 % and a loss of 0.0185, outperforming other machine learning models such as Logistic Regression, Decision Tree, Random Forest, and SVM in terms of both accuracy and generalization. The scalability, reliability, and real-time capabilities of this UAV-IoT system make it a robust tool for environmental monitoring and conservation. By leveraging advanced AI and IoT technologies, this system not only improves the detection and prevention of illegal logging but also sets a new standard for automated environmental protection solutions. Future research can build on this work by exploring further enhancements in AI algorithms, expanding the system's applications to other environmental monitoring areas, and integrating additional sensors to broaden the scope of detection capabilities.

CRediT authorship contribution statement

Montaser N.A. Ramadan: Writing – original draft, Software, Project administration, Methodology. **Mohammed A.H. Ali:** Writing – review & editing. **Shin Yee Khoo:** Writing – review & editing. **Mohammad Alkhedher:** Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Montaser Ramadan reports writing assistance was provided by University of Malaya. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

ADU author acknowledges financial support from Abu Dhabi University's Office of Research and Sponsored Programs.

Data availability

Data will be made available on request.

References

[1] G.M.A.S. Wibawa, M. Muhibbin, B. Parmono, Criminal actions of illegal logging in the perspective of forestry law, Int. J. Law, Environ. Natural Resour. 3 (1) (2023) 84–95.
[2] Z. Hasan, M.Z. Astarida, Penegakan hukum lingkungan sebagai upaya pembangunan yang berkelanjutan, Jurnal Ilmiah Advokasi 11 (1) (2023) 128–140.
[3] A.C. Cozma, M.V. Achim, I.L. Safta, Economic and financial crime in the forest industry—internationally and in Romania, in: 24th RSEP international conference on economics, Finance & Business, 2022, pp. 72–88.
[4] O. Rosadi, D. Afrizal, Criminal law policy against illegal logging as an effort to protect national forest areas (study on Solok protection forest management unit), Ekasakti J. Law Justice 1 (1) (2023) 30–36.
[5] D. Bremiardika, R.B. Suharto, and R.S. Sugiharto, "The criminological ideas in the criminal enforcement of illegal logging," *Law Develop. J.*, vol. 4, no. 3, pp. 454–460.
[6] S. Assembe-Mvondo, A. Kan, An overview of interactions between wildlife and forest illegalities in Cameroon, Int. Forestry Rev. 24 (4) (2022) 459–468.
[7] A. Mujetahid, M. Nursaputra, A.S. Soma, Monitoring illegal logging using google earth engine in Sulawesi Selatan Tropical Forest, Indonesia, Forests. 14 (3) (2023) 652.
[8] M.C. Low, et al., Tracing the world's timber: the status of scientific verification technologies for species and origin identification, IAWa J. 44 (1) (2022) 63–84.
[9] R.K. Boateng, J.D. Agyeman, S. Inyong, E.S.K. Agbadzah, H. Adjarko, Exploring species extraction volume and residues of illegal and conventional logging operations, Asian J. Environ. Ecol. 20 (2) (2023) 59–68.
[10] J.L. Carpio-Domínguez, The harms and crimes of logging and deforestation. Oxford Research Encyclopedia of Criminology and Criminal Justice, 2024.
[11] N. Yoh, D.J.I. Seaman, N.J. Deere, H. Bernard, J.E. Bicknell, M.J. Struebig, Benign effects of logging on aerial insectivorous bats in Southeast Asia revealed by remote sensing technologies, J. Appl. Ecol. 60 (7) (2023) 1210–1222.
[12] S. Xu, H.A. Klaiber, D.A. Miteva, Impacts of forest conservation on local agricultural labor supply: evidence from the Indonesian forest moratorium, Am. J. Agric. Econ. 105 (3) (2023) 940–965.

[13] S. Giljum, et al., A pantropical assessment of deforestation caused by industrial mining, Proc. National Acad. Sci. 119 (38) (2022) e2118273119.
[14] J.M. Torres-Rojo, Illegal logging and the productivity trap of timber production in Mexico, Forests. 12 (7) (2021) 838.
[15] M. Bösch, Institutional quality, economic development and illegal logging: a quantitative cross-national analysis, Eur. J. For. Res. 140 (5) (2021) 1049–1064.
[16] D. Blum, et al., Subnational institutions and power of landholders drive illegal deforestation in a major commodity production frontier, Global Environ. Change 74 (2022) 102511.
[17] E. Bunney, et al., Safeguarding sandalwood: a review of current and emerging tools to support sustainable and legal forestry, Plants. People Planet. 5 (2) (2023) 190–202.
[18] S. Wolff, J. Schweinle, Effectiveness and economic viability of forest certification: a systematic review, Forests. 13 (5) (2022) 798.
[19] F.W.C. Andrade, et al., The legal roundwood market in the Amazon and its impact on deforestation in the region between 2009 and 2015, Forests. 13 (4) (2022) 558.
[20] W.A. Chaves, D. Valle, A.S. Tavares, E.M. von Mühlen, D.S. Wilcove, Investigating illegal activities that affect biodiversity: the case of wildlife consumption in the Brazilian Amazon, Ecol. Appl. 31 (7) (2021) e02402.
[21] A.-J. Welsink, et al., Towards the use of satellite-based tropical forest disturbance alerts to assess selective logging intensities, Environ. Res. Lett. 18 (5) (2023) 054023.
[22] M. Bryson, A. Reid, C. Hung, F.T. Ramos, S. Sukkarieh, Cost-effective mapping using unmanned aerial vehicles in ecology monitoring applications, in: Experimental robotics: the 12th international symposium on experimental robotics, Springer, 2014, pp. 509–523.
[23] D. Ballaria, D. Orellana, E. Acostaa, A. Espinoza, V. Morocho, Uav monitoring for enviromental management in galapagos islands, Int Arch Photogrammetry, Remote Sens. Spatial Inf. Sci. 41 (2016) 1105–1111.
[24] M.N.A. Ramadan, et al., Towards early forest fire detection and prevention using AI-powered drones and the IoT, Internet Things (2024) 101248.
[25] A. Tripolitsiotis, N. Prokas, S. Kyritsis, A. Dollas, I. Papaefstathiou, P. Partsinevelos, Dronesourcing: a modular, expandable multi-sensor UAV platform for combined, real-time environmental monitoring, Int. J. Remote Sens. 38 (8–10) (2017) 2757–2770.
[26] S.K. Saravanan, T.P.K. Kumar, D.U.S. Rajkumar, R. Krishnamoorthy, R.N. Rao, R. Thiagarajan, IoT alert reflexion of forbidden deforestation regions with drone observation, in: 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), IEEE, 2023, pp. 1650–1655.
[27] B. Anđelić, M. Radonjić, S. Djukanović, Sound-based logging detection using deep learning. 2022 30th Telecommunications Forum (TELFOR), IEEE, 2022, pp. 1–4.
[28] H. Bandaranayake, D. Mahamohottala, W. Wijekoon, K. Sandakelum, N. Gamage, W. Rankothge, GreenSoal: illegal tree logging detection system using IOT, in: 2022 International Conference on ICT for Smart Society (ICISS), IEEE, 2022, pp. 1–6.
[29] M. Arunkumar, B.P. Raj, Surveillance of forest areas and detection of unusual exposures using deep learning, in: 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), IEEE, 2023, pp. 145–150.
[30] S. Sharma, K. Sato, B.P. Gautam, A Methodological literature review of acoustic wildlife monitoring using artificial intelligence tools and techniques, Sustainability. 15 (9) (2023) 7128.
[31] J.V. Solórzano, J.F. Mas, J.A. Gallardo-Cruz, Y. Gao, A.F.M. de Oca, Deforestation detection using a spatio-temporal deep learning approach with synthetic aperture radar and multispectral images, ISPRS J. Photogrammetry Remote Sens. 199 (2023) 87–101.
[32] J.S. Estrada, A. Fuentes, P. Reszka, F. Auat Cheein, Machine learning assisted remote forestry health assessment: a comprehensive state of the art review, Front. Plant Sci. 14 (2023) 1139232.
[33] S. Li, H. Lideskog, Realization of autonomous detection, positioning and angle estimation of harvested logs, Croatian J. Forest Eng.: J. Theory Appl. Forestry Eng. 44 (2) (2023) 369–383.
[34] J.C. Iacarella, et al., Application of AIS-and flyover-based methods to monitor illegal and legal fishing in Canada's Pacific marine conservation areas, Conserv. Sci. Pract. 5 (6) (2023) e12926.
[35] L. Shumilo, N. Kussul, M. Lavreniuk, U-Net model for logging detection based on the Sentinel-1 and Sentinel-2 data, in: 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS, IEEE, 2021, pp. 4680–4683.
[36] C. Aquino, et al., Reliably mapping low-intensity forest disturbance using satellite radar data, Front. For. Glob. Change 5 (2022) 1018762.
[37] D. Mo, "Further developing processing techniques of optical satellite images in the context of forest monitoring," 2018.
[38] H. Harris, Illegal logging, corruption and the limitations of destination country laws in the pacific context. in *New Zealand Yearbook of International Law*, Brill Nijhoff, 2022, pp. 64–96.
[39] A. Salaria, A. Singh, K.K. Sharma, A unified approach towards effective forest fire monitoring systems using wireless sensor networks and satellite imagery, in: Artificial Intelligence and Machine Learning in Satellite Data Processing and Services: Proceedings of the International Conference on Small Satellites, ICSS 2022, Springer, 2023, pp. 151–161.
[40] P. Mohammadpour, C. Viegas, Applications of multi-source and multi-sensor data fusion of remote sensing for forest species mapping, Adv. Remote Sens. Forest Monitoring (2022) 255–287.
[41] A. Morchid, et al., IoT-enabled fire detection for sustainable agriculture: a real-time system using flask and embedded technologies, Results. Eng. 23 (2024) 102705.
[42] G. Lazrek, K. Chetioui, Y. Balboul, S. Mazer, An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system, Results. Eng. 23 (2024) 102659.
[43] M.N.A. Ramadan, M.A.H. Ali, S.Y. Khoo, M. Alkhedher, M. Alherbawi, Real-time IoT-powered AI system for monitoring and forecasting of air pollution in industrial environment, Ecotoxicol. Environ. Saf. 283 (2024) 116856.
[44] J.A. Leonov, A.A. Kuzmenko, R.A. Filippov, L.B. Filippova, A.S. Sazonova, Models and methods for automating the analysis of logging for the tasks of geographically distributed socio-economic systems, Appl. Math. Control Sci. (4) (2021) 92–115.
[45] B. Chehreh, A. Moutinho, C. Viegas, Latest trends on tree classification and segmentation using UAV data—A review of agroforestry applications, Remote Sens. (Basel) 15 (9) (2023) 2263.
[46] Y. Wang, W. Zhang, R. Gao, Z. Jin, X. Wang, Recent advances in the application of deep learning methods to forestry, Wood. Sci. Technol. 55 (5) (2021) 1171–1202.
[47] M. Mascarello, et al., Genome skimming reveals novel plastid markers for the molecular identification of illegally logged African timber species, PLoS. One 16 (6) (2021) e0251655.
[48] S.M. Piabuo, P.A. Minang, C.J. Tieguhong, D. Foundjem-Tita, F. Nghobuoche, Illegal logging, governance effectiveness and carbon dioxide emission in the timber-producing countries of Congo Basin and Asia, Environ. Dev. Sustain. 23 (2021) 14176–14196.
[49] L. Luo, Z.J. Xu, B. Na, Building machine learning models to identify wood species based on near-infrared spectroscopy, Holzforschung. 77 (5) (2023) 326–337.
[50] K. Budnik, J. Byrtek, B. Skrabanek, J. Wajs, AI-accelerated decision making in forest management, in: IOP Conference Series: Earth and Environmental Science, IOP Publishing, 2023 012030.
[51] H.C. Teo, U.R. Hashim, S. Ahmad, L. Salahuddin, H.C. Ngo, K. Kanchymalay, A review of the automated timber defect identification approach, Int. J. Electr. Computer Eng. 13 (2) (2023) 2156.
[52] R. Alkhatib, W. Sahwan, A. Alkhatieb, B. Schütt, A brief review of machine learning algorithms in forest fires science, Appl. Sci. 13 (14) (2023) 8275.
[53] M.N.A. Ramadan, et al., Towards early forest fire detection and prevention using AI-powered drones and the IoT, Internet Things (2024) 101248.
[54] D. Datta, et al., TimberSleuth: visual anomaly detection with human feedback for mitigating the illegal timber trade, Inf. Vis. 22 (3) (2023) 223–245.
[55] H. Bandaranayake, D. Mahamohottala, W. Wijekoon, K. Sandakelum, N. Gamage, W. Rankothge, GreenSoal: illegal tree logging detection system using IOT, in: 2022 International Conference on ICT for Smart Society (ICISS), IEEE, 2022, pp. 1–6.
[56] H. Singh, R.K. Dwivedi, A. Kumar, V.K. Mishra, A review on AI techniques applied on tree detection in UAV and remotely sensed imagery, in: 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), IEEE, 2022, pp. 1446–1450.
[57] S.M. Murali, S.T. Shri, P. Roshini, C.Y. Rubavathi, R.S. Krishnan, K.L. Narayanan, Smart solar powered system for unauthorized logging, in: 2023 International Conference on Inventive Computation Technologies (ICICT), IEEE, 2023, pp. 1644–1649.
[58] G. Blanchard, et al., UAV-Lidar reveals that canopy structure mediates the influence of edge effects on forest diversity, function and microclimate, J. Ecol. 111 (7) (2023) 1411–1427.
[59] C. Taylor, D.B. Lindenmayer, The use of spatial data and satellite information in legal compliance and planning in forest management, PLoS. One 17 (7) (2022) e0267959.
[60] P. Samant, J.S.P. Kumar, R. Gupta, A. Agarwal, R. Agarwal, Machine learning-based electronic tree surveillance system for detection of illegal wood logging activity. Real-Life Applications of the Internet of Things, Apple Academic Press, 2022, pp. 421–437.
[61] A. Srisuphab, N. Kaakkurivaara, P. Silapachote, K. Tangkit, P. Meunpong, T. Sunetnanta, Illegal logging listeners using IoT networks, in: 2020 IEEE Region 10 conference (tencon), IEEE, 2020, pp. 1277–1282.
[62] V. KR, "Anti-Smuggling System for Trees in Forest Using Vibration Sensor and NRF," 2019.
[63] I. Mporas, I. Perikos, V. Kelefouras, M. Paraskevas, Illegal logging detection based on acoustic surveillance of forest, Appl. Sci. 10 (20) (2020) 7379.