Babylonian Journal of Networking
Vol.2025, **pp**. 207–241
DOI: https://doi.org/10.58496/BJN/2025/019; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Blockchain and Deep Q-Learning for Trusted Cloud-Enabled Drone Network in Smart Forestry: A Survey

Guma Ali [1,2,*], Wamusi Robert [1], Maad M. Mijwil [3,4], Hassan A. Hameed Al-Hamzawi [5], Ali S. Abed Al Sailawi [6], Ayodeji Olalekan Salau [7,8]

1 Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda

2 Department of Computer Science and Engineering, Saveetha Institute of Medical and Technical Sciences, Tamilnadu, India.

3 College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq.

4 Computer Techniques Engineering Department, College of Engineering Technologies, Al-Iraqia Science University, Baghdad, Iraq.

5 Ministry of Construction, Housing, Municipalities and Public Works, Diwaniyah, Iraq.

6 College of Law, University of Misan, Al Amarah City, Maysan, Iraq.

7 Department of Electrical/Electronic and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria.

8 Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India.

ARTICLE INFO

Article History

Received 19 Aug 2025
Revised 21 Sep 2025
Accepted 6 Nov 2025
Published 14 Dec 2025

Keywords
Smart Forestry,
Cloud Computing,
Drone Network,
Blockchain Technology,
Deep Q-Learning.

ABSTRACT

The convergence of drone technology, cloud computing, and intelligent decision-making is revolutionizing precision forestry. However, deploying large-scale drone networks in smart forestry faces challenges such as trust, security, data integrity, and autonomous coordination. This survey examines how combining Blockchain technology with deep Q-learning (DQL) can address these issues within cloud-enabled drone networks. Drawing on 102 peer-reviewed sources published between 2022 and 2025 from reputable platforms such as ACM Digital Library, Frontiers, Wiley Online Library, PLoS, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, Taylor & Francis, Sage, and Google Scholar, this work highlights recent advancements in secure and intelligent drone ecosystems. Blockchain provides a decentralized, tamper-resistant framework for validating transactions and securing data exchange among autonomous drones, ensuring the integrity, confidentiality, and authenticity of environmental data. This is critical in forestry, where data manipulation and unauthorized access pose significant risks. Complementing this, DQL enables drones to make autonomous decisions by interpreting real-time environmental data and learning from past experiences, allowing drones to adjust their flight paths, optimize resource utilization, and enhance data collection in dynamic forest environments, such as wildfires or illegal logging operations. Together, Blockchain and DQL create a resilient, scalable architecture that supports secure, real-time, and intelligent forest monitoring. This framework lays the groundwork for developing autonomous and trustworthy drone networks that promote sustainable and climate-smart forestry management.

1. INTRODUCTION

Emerging technologies have significantly transformed traditional forestry by enhancing environmental monitoring and resource management. Forests, which provide critical ecological, economic, and social benefits such as carbon sequestration, biodiversity conservation, timber production, and climate regulation, face growing threats from deforestation, illegal logging, wildfires, and biodiversity loss [1]. In response, smart forestry has emerged as a promising approach that integrates the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, autonomous drones, and Unmanned Aerial Vehicles (UAVs) to enhance the monitoring, management, and preservation of forest ecosystems [2]. This technology-driven approach addresses the growing demand for sustainable forest management by providing real-time data collection, analysis, and support for informed decision-making.

*Corresponding author. Email: a.guma@muni.ac.ug

Smart forestry leverages technologies such as the IoT, Wireless Sensor Networks (WSN), remote sensing, Geographic Information Systems (GIS), AI, and autonomous drones to enable real-time forest monitoring and data-driven management [3]. Sensors placed on trees, in soil, and in water bodies continuously monitor environmental parameters, including temperature, humidity, soil moisture, and air quality. Remote sensing tools and GIS integrate these data streams to offer comprehensive insights into forest health, enabling early detection of diseases, illegal logging, and ecological disturbances [4]. AI and machine learning algorithms analyze large datasets to predict forest growth, assess biodiversity, and identify wildfire risks. Autonomous drones equipped with high-resolution cameras, LiDAR, and AI-powered analytics conduct aerial surveillance, support reforestation, and manage timber operations by capturing real-time imagery across challenging terrains [5]. Their agility and cost-effectiveness make drones essential for monitoring deforestation hotspots, tracking wildlife, and assessing the impacts of climate change. When connected to cloud platforms, drone networks can process and share data at scale, facilitating applications such as forest inventory mapping, fire detection, and surveillance against illegal activities. AI-powered drones support precision forestry by optimizing tasks like tree planting, thinning, and harvesting through advanced decision-support systems. Their use increases timber yield, minimizes environmental impact, and promotes biodiversity conservation [6]. By integrating these technologies, smart forestry enhances decision-making, promotes sustainability, and ensures balanced management of forests to meet economic, environmental, and social goals. Trusted cloud-enabled drone networks integrate autonomous drones with secure cloud infrastructure to facilitate real-time data collection, storage, processing, and informed decision-making in forestry management [7]. These networks serve as the foundation of smart forestry systems by enabling drones to collaborate, share environmental data, and carry out automated tasks driven by cloud-based analytics and AI [8]. Equipped with sensors such as cameras, LiDAR, infrared, and GPS, the drones gather diverse data on tree health, temperature, fire risks, and potential illegal activities. They transmit this information to the cloud in real-time, where powerful computational tools analyze it and coordinate responses, such as detecting early signs of a wildfire and deploying nearby drones to verify and assess its severity [9]. By ensuring trust, data integrity, security, and real-time intelligence, these networks support scalable, autonomous operations across large and often inaccessible forest areas. They meaningly enhance the accuracy and efficiency of forestry activities, including threat detection, biodiversity monitoring, and environmental compliance, while reducing the need for manual intervention [10-12]. Smart forestry supports the global Sustainable Development Goals (SDGs) by promoting environmental protection, climate resilience, and responsible resource management. It advances SDG 13 (Climate Action) by increasing forest carbon sequestration and reducing climate change impacts through reforestation [13]. By preventing deforestation, preserving biodiversity, and sustaining healthy ecosystems, it contributes to SDG 15 (Life on Land). The integration of Blockchain in forestry supply chains furthers SDG 12 (Responsible Consumption and Production) by enabling sustainable logging and ethical trade. Additionally, smart forestry drives SDG 9 (Industry, Innovation, and Infrastructure) by encouraging the adoption of AI, IoT, and Blockchain technologies in forest management [14]. Integrating drones with cloud infrastructures in smart forest environments introduces numerous security threats and challenges that can compromise their effectiveness and safety. These include unauthorized access, data privacy issues, authentication weaknesses, denial-of-service (DoS) and distributed DoS (DDoS) attacks, man-in-the-middle (MitM) attacks, spoofing, eavesdropping, false data injection, malware attacks, physical capture, GPS jamming, insider threats, IoT botnets, vulnerabilities in edge devices and cloud platforms, trust and data integrity concerns, lack of standardization, complex data processing, scalability and coordination difficulties, resource limitations, design flaws, and regulatory compliance risks [15-34]. Maintaining the integrity, confidentiality, and availability of data collected and transmitted by drones remains critical, mainly when real-time decisions rely on the accuracy and trustworthiness of that information [35]. Blockchain and DQL have emerged as pivotal technologies in advancing smart forestry. Blockchain secures drone communication and transaction logs through a decentralized, tamper-proof system, enabling trusted interactions within cloud-enabled drone networks. It ensures data provenance, access control, and integrity verification while promoting transparency, accountability, and security in forestry operations. Blockchain systems maintain immutable records of timber supply chains, helping verify the legal and sustainable origins of wood products and combat illegal logging [36]. They also enhance carbon credit management by linking forest conservation efforts to transparent, auditable carbon offset transactions, thereby encouraging sustainable investments in reforestation. Cloud computing complements this by offering scalable storage, real-time data sharing, and computational power for AI-driven models. A trusted cloud-enabled drone network securely stores and processes forestry data in a decentralized manner, reducing cybersecurity risks associated with centralized systems [37]. Blockchain further strengthens this framework by recording logging activities transparently, supporting compliance with sustainability standards. Meanwhile, DQL offers an intelligent and adaptive framework for UAV path planning, task allocation, and real-time resource management. This reinforcement learning approach enables drones to autonomously determine optimal flight paths, avoid obstacles, and prioritize critical areas, thereby improving operational efficiency, reducing the need for human intervention, and enhancing the accuracy of forest monitoring [38][39]. This survey explores the convergence of Blockchain and DQL as powerful tools for building a secure, intelligent, and cloud-enabled drone network for smart forestry. Blockchain enables transparent and tamper-proof data sharing across distributed nodes, while DQL supports adaptive and autonomous drone control in dynamic forest environments. Despite growing interest, research in this interdisciplinary area remains scattered and fragmented. To address this gap, the survey offers a comprehensive review of recent advancements in Blockchain and DQL technologies applied to cloud-connected drone networks in smart forestry. Several recent studies have explored the integration of Blockchain technology and DQL to

improve the security and efficiency of drone networks in smart forestry. Hafeez et al. [40] proposed a Blockchain-enabled UAV framework for post-disaster response, and Mishra et al. [5] introduced a Blockchain-based authentication and key management system with big data analytics for secure drone communication in 5G and beyond. However, none of these studies examined the integration of Blockchain and deep Q-learning (DQL) for a trusted Cloud-enabled drone network in smart forestry. This study addresses that gap by providing the first comprehensive survey of Blockchain and DQL integration in this context. This survey makes several key contributions to the field of smart forestry. It presents the latest advancements in smart forestry, drone technology, and cloud computing and explains how a trusted cloud-enabled drone network enhances forestry operations. It examines the security threats, attacks, and challenges associated with such networks, highlighting the role of Blockchain technology and DQL in addressing these issues. The survey introduces a unified conceptual framework that integrates these technologies within a trusted drone network. Additionally, it identifies key challenges and limitations in applying Blockchain and DQL to secure smart forestry networks and outlines future research directions to advance this emerging area. This survey is structured as follows. Section 2 outlines the materials and methods, followed by a review of the state of the art in Section 3. Section 4 introduces Blockchain technology and DQL, emphasizing their role in enhancing the security of trusted cloud-enabled drone systems and presenting an integrated framework for smart forestry applications. Section 5 further examines the technical aspects of Blockchain and DQL, while Section 6 details a conceptual framework for implementing a trusted cloud-enabled drone network using these technologies. Section 7 explores real-world scenarios and practical applications of this integration in smart forestry. Section 8 highlights the associated challenges and limitations, and Section 9 outlines future research directions. The survey concludes in Section 10.

2. MATERIALS AND METHODS

This survey comprehensively collects, evaluates, analyzes, and organizes relevant literature on Blockchain and DQL for a trusted cloud-enabled drone network in smart forestry. The researchers systematically identified key research questions and applied explicit inclusion and exclusion criteria to select the most pertinent studies published between 2022 and 2025. They conducted thorough searches using targeted keywords across major academic databases and digital libraries, including ACM Digital Library, Frontiers, Wiley Online Library, PLoS, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, Taylor & Francis, Sage, and Google Scholar, with a focus on peer-reviewed journal articles, conference proceedings, book chapters, and books. By organizing the literature around core themes such as smart forestry objectives, Blockchain and DQL frameworks, and associated security challenges, the survey highlights key findings, identifies research gaps, and synthesizes advances in the field. The study emphasizes Blockchain and DQL components, features, and security threats to provide a structured and up-to-date overview of current developments. The following keyword combinations were used to perform the literature search: "Blockchain" AND "Drones" AND "Cloud Computing" OR "Deep Q-Learning" AND "Unmanned Aerial Vehicles (UAVs)" OR "Blockchain" AND "Smart Forestry" OR "Trusted Drone Network" AND "Cloud-Enabled" OR "Blockchain" AND "Reinforcement Learning" AND "Drones" OR "Deep Q-Learning" AND "Smart Forestry" OR "UAV" AND "Blockchain" AND "Trust Management" OR "Cloud Computing" AND "Drone Network" AND "Security" OR "Reinforcement Learning" AND "UAV Communication" OR "Blockchain" AND "Cloud Services" AND "Forestry Applications" OR "DQL" AND "Trusted Communication" AND "Drones" OR "Drone Swarm" AND "Blockchain Integration" OR "Secure UAV Network" AND "Deep Learning" OR "Blockchain" AND "Autonomous Drones" AND "Forestry" OR "Edge Computing" AND "UAV" AND "Trust Mechanisms." Boolean operators were utilized to narrow or expand the search as necessary, and additional references were manually identified from the bibliographies of selected papers. The survey applied specific inclusion and exclusion criteria to ensure the relevance and quality of this review. It included peer-reviewed articles, conference proceedings, and book chapters written in English that focus on smart forestry and related domains involving Blockchain and DQL, address security concerns in smart forestry, explore Blockchain and DQL applications for securing smart forestry systems, or examine trusted cloud-enabled drone network security and vulnerabilities. The survey also considered reviews and meta-analyses, which offered significant insights, as well as studies with transparent methodologies. It also considered research papers published between January 2022 and the date of this survey's publication. It excluded articles not written in English, studies unrelated to smart forestry or lacking a focus on Blockchain and DQL, research papers with incomplete or technically irrelevant content, those with vague methodologies or inconclusive findings, non-peer-reviewed publications, and any research published before January 2022. Five authors independently retrieved relevant materials from selected research databases using predefined key criteria. These included: (1) title, authors, and publication year; (2) objectives and research questions; (3) study design; (4) methods of analysis; (5) results; (6) conclusions; (7) Blockchain; (8) Blockchain and DQL; (9) vulnerabilities in trusted cloud-enabled drone networks; (10) benefits of smart forestry; (11) comparison of Blockchain and DQL in smart forestry; and (12) challenges and limitations. They organized the extracted data in a consistent format to ensure uniformity and accuracy. The survey followed a structured, multi-stage approach. Researchers initially identified over 3,250 publications through academic search engines and databases. After removing duplicates and screening abstracts, they narrowed the dataset to 1,273 publications. They then assessed each for eligibility, further reducing the number to 913. Finally, they selected 102 publications that met the study's inclusion criteria. The researchers thoroughly evaluated 102 publications for

relevance to the study objectives, drawing from various sources: 3 from ACM Digital Library, 1 from Frontiers, 5 from Wiley Online Library, 1 from PLoS, 2 from Nature, 8 from Springer, 17 from ScienceDirect, 14 from MDPI, 31 from IEEE Xplore Digital Library, 3 from Taylor & Francis, 1 from Sage, and 16 from Google Scholar. They categorized and assessed each publication to ensure alignment with the study's aims. Fig. 1 shows the distribution of these selected publications by number of publications.

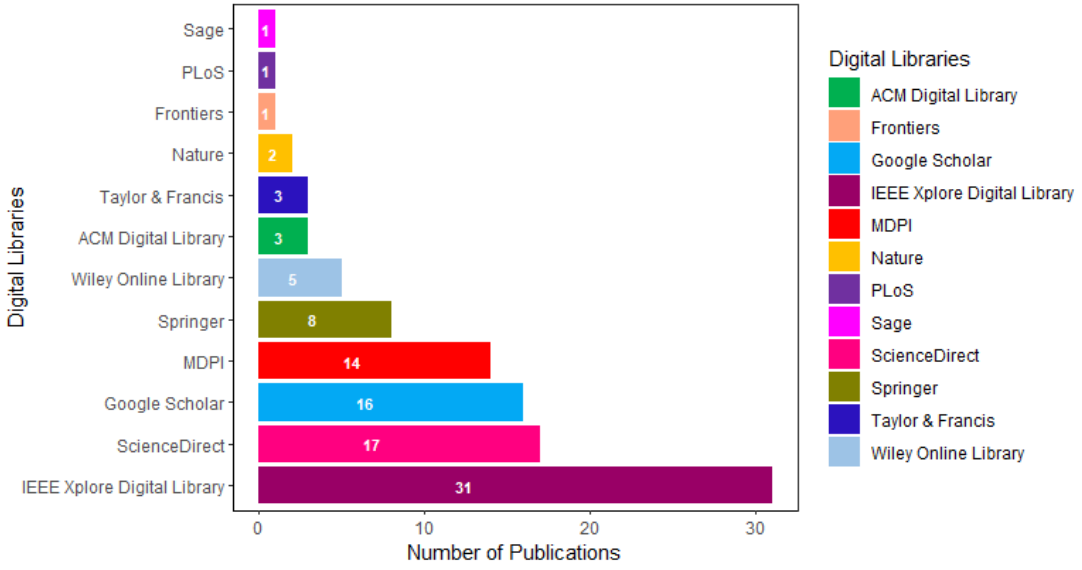

Fig. 1. Depicts the distribution of selected research publications across digital libraries.

Fig. 2 illustrates the distribution of research paper sources across digital libraries.

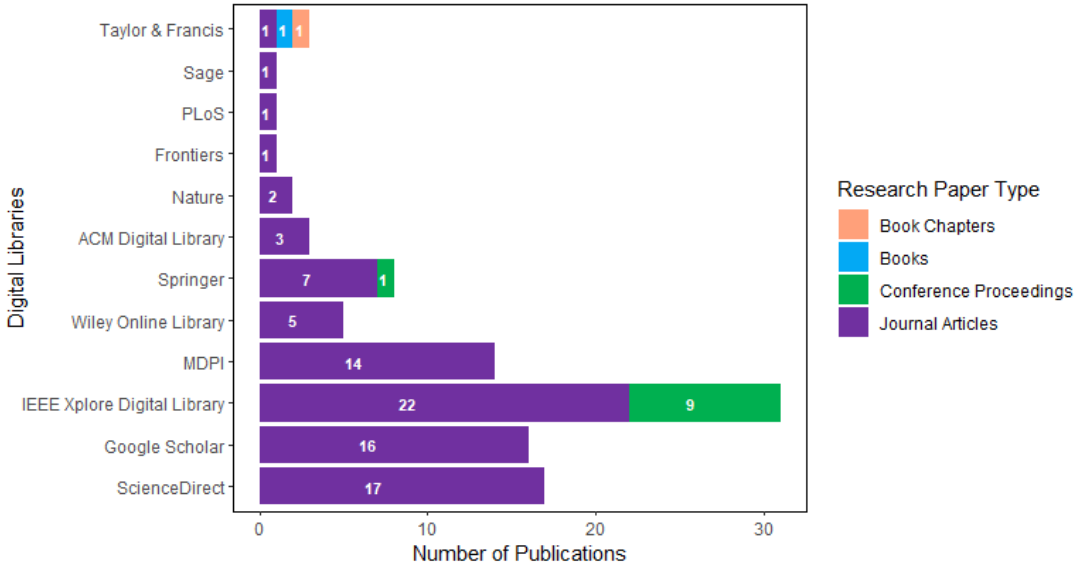

Fig. 2. Depicts the distribution of research paper sources based on digital libraries.

Fig. 3 illustrates the distribution of selected papers by digital libraries, categorized by the year of publication.

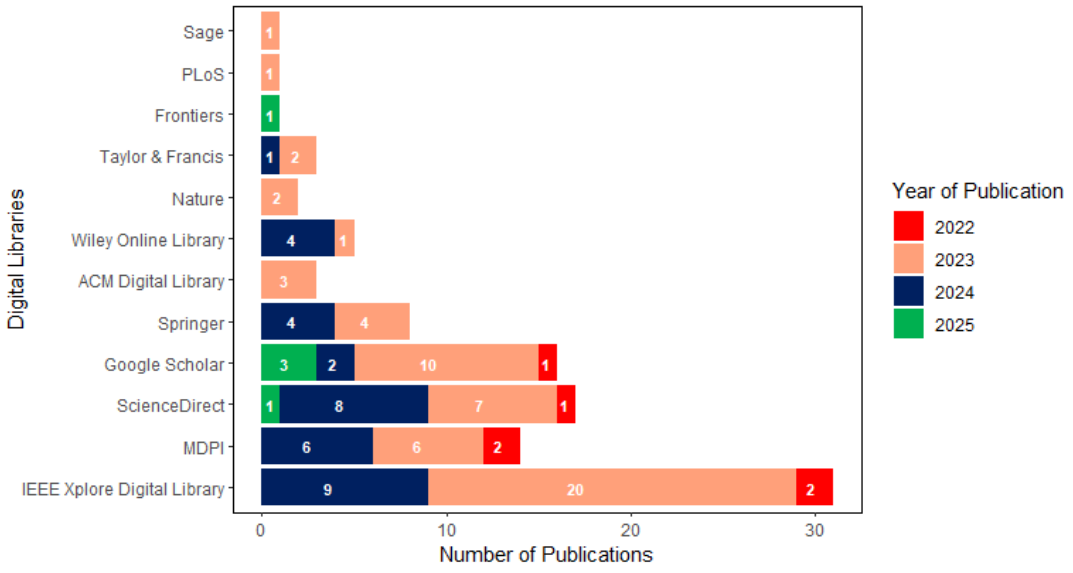

Fig. 3. Depicts the distribution of selected papers by digital libraries based on the year of publication.

The researchers selected research papers based on several criteria, including timeliness, citation count, relevance, methodological rigor, coherence, validity, dependability, peer-review status, source credibility, potential bias, and the presence of confounding variables. To ensure the reliability and validity of their results, they conducted comprehensive database searches, documented all references, created a dedicated reference database, and removed duplicates using a reference management tool. They then applied a multi-step screening process, comprising keyword analysis, title and abstract review, and full-text evaluation, to refine the selection. At each stage, they recorded the reasons for exclusion and discarded studies that failed to meet the eligibility criteria. Finally, they compiled the selected papers into a final database for analysis. The researchers conducted a qualitative synthesis and applied thematic analysis to examine the collected material. They validated their findings by consulting subject-matter experts, comparing the results with those of prior studies, and critically evaluating the validity of their conclusions. They included only high-quality research papers in the final selection, using a grading system that assessed methodological rigor, the reliability of findings, and relevance to smart forestry applications involving Blockchain and DQL in trusted cloud-enabled drone networks. As the study relied solely on previously published research, it did not require ethical approval; however, the researchers ensured proper citation of all sources. The paper identifies several limitations. It may have missed relevant studies not included in the selected databases. Publication bias could have influenced the findings, as studies with favorable outcomes are more likely to be published. The review does not comprehensively address Blockchain and DQL within trusted cloud-enabled drone network methodologies in smart forestry. The paper relies heavily on qualitative assessments without incorporating quantitative analysis or empirical data, which undermines the strength and credibility of its conclusions. Additionally, it tends to emphasize theoretical applications while underrepresenting practical challenges such as cost, scalability, and user acceptance. Finally, the rapid advancement of Blockchain and DQL technologies in this domain may outpace the scope of the reviewed literature.

3. STATE-OF-THE-ART

3.1. Smart Forestry

Smart forestry is an emerging approach that uses advanced digital technologies and data-driven methods to manage forest ecosystems more efficiently, sustainably, and adaptively. It incorporates tools such as the IoT, remote sensing, GIS, drones, AI, and big data analytics to monitor, assess, and manage forest resources instantly. By automating the collection and analysis of large volumes of ecological data, smart forestry enables evidence-based decision-making that supports the long-term health and productivity of forests. It also emphasizes the need to reform forestry education and build a skilled workforce capable of driving economic growth in forest-dependent rural communities [15]. Smart forestry promotes transparency, traceability, and accountability in forest governance while reforming forestry education and training. It prioritizes recruiting and equipping a skilled workforce to strengthen economic opportunities in forest-dependent rural communities. The smart forestry market has experienced rapid growth in recent years, increasing from US$4.95 billion in 2024 to an expected US$8.25 billion by 2029 at a compound annual growth rate (CAGR) of 10.7%. This growth reflects a growing environmental awareness, the need for efficient forest management, stricter regulations on deforestation, heightened concerns about climate change, and a shift toward sustainable resource use. Key drivers of this anticipated growth include the expansion of IoT

networks, increased investment in precision agriculture, a stronger emphasis on climate resilience, greater funding for green technologies, and rising consumer demand for sustainably sourced forest products. Smart forestry initiatives aim to transform the traditional wood supply chain into a digital twin-based value network that enhances commissioning, harvesting operations, and mill acceptance [28]. Emerging trends shaping the future of smart forestry include AI-driven analytics, widespread deployment of IoT-enabled sensors, advances in drone and satellite imaging, Blockchain integration for supply chain transparency, improved data interoperability via open platforms, and the rise of climate-smart forestry technologies. Smart forestry centers on the use of drone technology to generate high-resolution aerial imagery, enabling real-time monitoring of forests [28]. UAVs map forest cover, track deforestation, monitor wildfires, and assess forest health without disturbing the environment. Equipped with sensors and cameras, drones gather critical data non-invasively, offering a more efficient alternative to manual surveys. Integrated into forest sensor networks, drones continuously measure weather variables such as temperature, humidity, soil moisture, and air quality [29], providing insights into microclimatic changes and early signs of environmental stress. AI and machine learning technologies analyze these extensive datasets to deliver predictive models and recognize patterns, enabling foresters to anticipate threats such as pest infestations, drought, or fire outbreaks [41]. Deep learning enhances tree species identification, biomass collection, and carbon sequestration estimation, thereby supporting biodiversity conservation and climate change mitigation. Cloud computing platforms store this data and ensure remote access for various stakeholders, fostering real-time collaboration and more efficient decision-making [30]. The growing emphasis on responsible forestry practices is driving the expansion of the smart forestry market. These practices involve managing forest resources in ways that preserve ecosystem health, productivity, and biodiversity while meeting the social, economic, and environmental needs of present and future generations. Rising ecological awareness, stricter regulations, and an increasing demand for sustainable products and certifications are fueling this trend. Smart forestry supports these efforts by leveraging advanced technologies to enable precise monitoring, promote sustainable resource use, and minimize environmental impact. Fig. 4 illustrates the conceptual diagram of smart forestry.

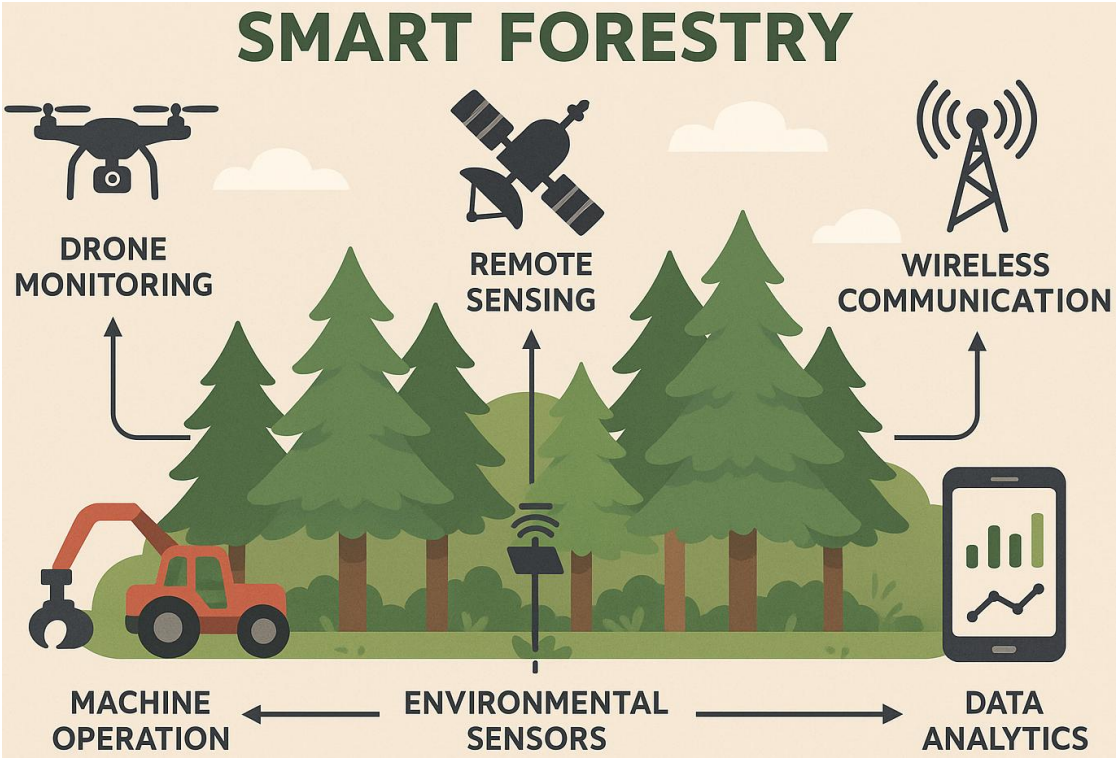

Fig. 4. Illustrates the conceptual diagram of smart forestry.

Smart Forestry enables a range of applications that enhance sustainability and ecosystem management. It supports sustainable timber production by optimizing harvesting schedules and routes to promote forest regeneration and minimize waste. Advanced monitoring systems detect diseases and pests early, allowing for targeted interventions that prevent widespread outbreaks. In wildfire management, real-time detection and fire spread modeling provide critical decision support for firefighting operations. Smart technologies also enhance carbon sequestration accounting by accurately measuring and tracking carbon stocks, thereby strengthening carbon credit markets and informing climate policy. They aid biodiversity conservation by mapping habitat conditions and monitoring species distributions to guide effective conservation planning. Smart forestry succeeds by collecting high-quality data, integrating sensors effectively, and combining human expertise with

digital tools to drive informed decision-making. This collaboration ensures that technology enhances traditional forestry knowledge without replacing it [1][28][29].

3.2. Components of Smart Forestry

Smart forestry integrates advanced technologies to enable precise, efficient, and sustainable forest management. By combining these tools, traditional forestry is transformed into data-driven, automated systems that can address today's environmental and resource challenges. Below are brief descriptions of the key components that form the technological backbone of smart forestry.

3.2.1. Unmanned Aerial Vehicles/Drones

Drones play a central role in smart forestry by rapidly capturing high-resolution aerial imagery of forest landscapes. Equipped with sensors such as RGB, thermal, LiDAR, and multispectral cameras, these autonomous or semi-autonomous aerial vehicles collect diverse data on vegetation health, canopy cover, soil moisture, and other environmental factors. They enable efficient forest mapping, tree species classification, biomass estimation, and the early detection of threats such as fires, pests, and illegal logging. When combined with deep learning algorithms and real-time decision-making models, drones act as intelligent agents that monitor forests and support timely interventions [42].

3.2.2. Internet of Things (IoT) and environmental sensor networks

IoT-enabled sensor networks continuously monitor ecological parameters, such as temperature, humidity, soil pH, carbon dioxide levels, and wind speed, across forest ecosystems. These sensors deliver real-time data that drives forest growth models, detects anomalies, and enable automated decision-making. By evaluating microclimatic changes and forecasting fire risks, the sensor data plays a vital role in optimizing forest resource management. Integrating IoT with cloud platforms and AI enables systems to process and analyze massive, heterogeneous data efficiently [43].

3.2.3. Geospatial Technologies – GIS and GPS

GIS and GPS technologies play a crucial role in mapping and analyzing forested areas. GIS enables users to visualize and assess spatial patterns, such as deforestation, forest degradation, and land-use changes, over time. At the same time, GPS provides precise geolocation and navigation, which proves especially useful for guiding drones and ground-based monitoring activities. By combining these technologies, forest managers can effectively plan, zone, and enforce conservation efforts [43].

3.2.4. Artificial Intelligence and Machine Learning Algorithms

AI, primarily through machine learning and deep learning, advances smart forestry by automating pattern recognition and enabling predictive analytics. These technologies support tasks such as species identification, biomass forecasting, disease diagnosis, and yield prediction. By training machine learning models on historical and real-time data, researchers can more effectively predict potential threats and optimize resource allocation. DQL plays a key role in guiding intelligent drone navigation and facilitating adaptive monitoring in complex forest environments [44].

3.2.5. Blockchain technology

Blockchain provides a secure, decentralized framework for recording and managing forestry data, thereby enhancing transparency, traceability, and resistance to tampering - key elements that foster trust in forest governance, carbon trading, and timber certification. By deploying smart contracts, stakeholders can automate transactions and enforce regulatory compliance in forest-related activities, such as verifying sustainable logging practices or distributing payments for ecosystem services. This approach plays a crucial role in strengthening trust among local communities, governments, and conservation organizations [44].

3.2.6. Edge computing

Edge computing enhances cloud infrastructure by processing data locally at or near its source. In remote forest regions with limited connectivity, edge devices handle initial data filtering, analytics, and response actions without depending on real-time cloud access. Local processing is crucial for time-sensitive applications, such as wildfire detection and intrusion monitoring, where minimizing latency is essential [45].

3.2.7. Fog computing

These components work together to create a robust, interconnected ecosystem that defines smart forestry. Their synergy drives efficient forest monitoring and resource management while promoting ecological sustainability through intelligent, responsive, and trustworthy technological interventions.

3.2.8. Cloud computing

Cloud computing offers a scalable and centralized solution for managing the vast amount of data generated by sensors, UAVs, and smart devices in forests. It enables remote access to forest data, supports real-time analytics, and promotes collaborative decision-making among stakeholders. By integrating smoothly with machine learning frameworks, cloud platforms allow users to continuously train and deploy predictive models that enhance sustainable forest management [43].

3.2.9. Big data analytics

Smart forestry leverages big data architectures to collect, store, and analyze massive volumes of sensor and digital system data. By efficiently processing this information, it enables rapid and reliable decision-making, supporting applications such as growth modeling, resource allocation, and sustainability assessments. Through big data analytics, forestry management can organize complex datasets to inform better decisions and optimize resource utilization.

Fig. 5 summarizes the components of smart forestry.

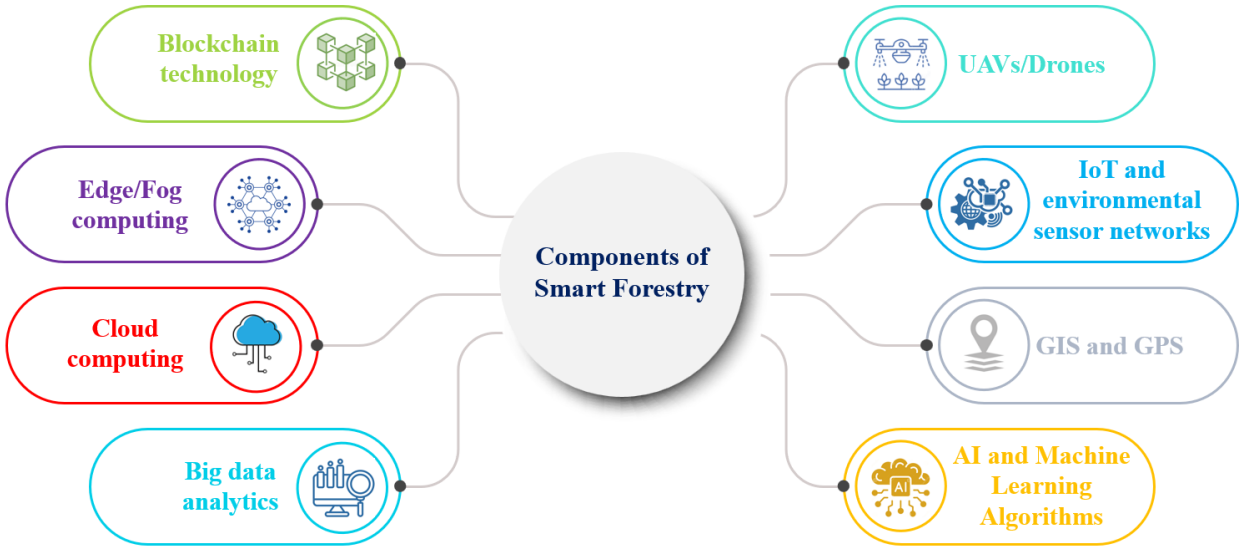

Fig. 5. Summary of the components of smart forestry.

3.3. Goals of Smart Forestry

The main goals of the smart forest are briefly described below:

3.3.1. Enhancing security and trust in forestry data management

The primary aims of smart forestry are to enhance it by securing, transparently managing, and ensuring the trustworthiness of forestry data. By integrating Blockchain technology, it establishes a decentralized, immutable ledger that records drone-collected information on deforestation rates, fire outbreaks, pest infestations, and reforestation efforts. This approach prevents data tampering, guarantees authenticity, and boosts stakeholder confidence in forest management decisions. Additionally, a trusted cloud-enabled network facilitates seamless data access and sharing among forest management authorities, policymakers, and conservationists [42].

3.3.2. Strengthening real-time monitoring and rapid response capabilities

Smart forestry aims to enable real-time monitoring of forest ecosystems through the use of drone networks. Drones instantly transmit data to a central repository via cloud computing, where AI-driven analytics detect patterns and potential threats. This process strengthens early warning systems for forest fires, pest outbreaks, and deforestation. By utilizing Blockchain to ensure data integrity, stakeholders can make informed decisions more quickly, thereby improving response times and reducing environmental damage [43].

3.3.3. Improving efficiency in reforestation and forest regeneration efforts

Drones equipped with AI and Blockchain technology are transforming reforestation by automating seed dispersal and monitoring the health of newly planted trees. Using DQL, drones identify optimal seed planting locations based on soil quality, moisture levels, and ecosystem suitability. Meanwhile, Blockchain technology transparently records all reforestation activities, preventing fraudulent claims and enabling governments and environmental organizations to track progress and evaluate the effectiveness of forest restoration initiatives [43].

3.3.4. Enhancing data sharing and collaboration in forestry conservation

Smart forestry relies on collaboration among government agencies, non-governmental organizations (NGOs), researchers, and private-sector stakeholders. Blockchain technology creates a decentralized, tamper-proof system that allows all parties to access verified forestry data, minimizing conflicts over land use and conservation claims. Cloud-enabled networks facilitate seamless data sharing, enabling organizations to leverage AI-driven insights for informed decision-making and more efficient resource allocation in forest conservation [44].

3.3.5. Strengthening climate change mitigation and carbon sequestration tracking

Smart forestry integrates AI-driven drone monitoring with Blockchain technology to accurately measure carbon capture rates and support compliance with carbon credit programs, recognizing the vital role forests play in carbon sequestration as a key strategy to combat climate change. By recording verifiable data on forest biomass and carbon stock, Blockchain ensures transparency in carbon offset initiatives. Additionally, DQL improves drones' ability to precisely identify deforested areas that need reforestation, enabling more efficient carbon sequestration strategies [43].

3.3.6. Reducing environmental and operational costs in forestry management

Traditional forestry management demands significant labor, time, and expense. By deploying AI-driven drones, managers reduce human resource costs and boost efficiency in data collection and analysis. DQL optimizes drone energy consumption, extending flight times and maximizing coverage. Additionally, Blockchain-based smart contracts automate payments for verified reforestation efforts and incentivize conservation initiatives, streamlining financial transactions in forest management [46].

3.3.7. Mitigating illegal logging and forest exploitation

Illegal logging poses a significant threat to forest ecosystems, leading to biodiversity loss and environmental degradation. Smart forestry addresses this issue by integrating AI and Blockchain to enhance forest surveillance and bolster law enforcement. Drones equipped with high-resolution cameras and machine-learning models can rapidly detect unauthorized logging. Meanwhile, Blockchain technology secures a tamper-proof record of logging activities, enabling authorities to track timber supply chains and enforce environmental regulations effectively [45].

3.4.Benefits of Smart Forestry

Smart forestry offers several significant benefits, which are briefly described in Table I.

TABLE I: SUMMARY OF KEY BENEFITS OF SMART FORESTRY.

S/No	Benefits	Description	References
1	Enhancing forest monitoring and management efficiency	Smart forestry utilizes advanced technologies, including drones, IoT sensors, and AI-driven analytics, to provide real-time insights into forest conditions. This enables precise monitoring of tree growth, deforestation, illegal logging, and ecosystem health. This research integrates Blockchain and DQL to develop a reliable, autonomous, cloud-enabled drone network that enhances data accuracy and automates forest surveillance. By ensuring transparency and preventing data manipulation, the secure and immutable nature of Blockchain fosters trust in forest data and supports informed decision-making.	[47]
2	Strengthening reforestation and carbon sequestration efforts	Reforestation plays a vital role in combating climate change by boosting carbon sequestration and restoring degraded forests. However, traditional methods often suffer from slow planting, poor monitoring, and high operational costs. Smart forestry addresses these issues by using AI-powered drones to autonomously disperse seeds, evaluate soil conditions, and monitor tree growth. This study enhances these capabilities by applying DQL to optimize drone operations and incorporating Blockchain technology to record reforestation data securely. Together, these innovations promote accountability and support the long-term sustainability of afforestation efforts.	[48]
3	Improving early detection and prevention of forest fires	Wildfires pose a severe threat to forest ecosystems, causing extensive environmental and economic damage. To address this, smart forestry employs thermal imaging drones and AI-driven predictive analytics for real-time fire detection and early identification of potential outbreaks. This study advances fire management by introducing a Blockchain-secured, cloud-enabled drone network that facilitates real-time communication among drones, authorities, and firefighting agencies. By integrating DQL, the system enables drones to learn from past fire events and make faster, more effective decisions in developing and executing fire containment strategies.	[43]
4	Advancing pest and disease monitoring	Invasive pests and diseases pose significant threats to forests, often spreading rapidly if not detected early. Traditional monitoring methods are slow and inefficient, delaying effective responses. This research addresses these challenges by integrating drone-based imaging with AI-driven pattern recognition to enhance the early detection and control of infestations. It further improves current practices by implementing a decentralized, Blockchain-based data-sharing system that provides conservationists and government agencies with secure, verified	[42]

		access to critical information. Additionally, it utilizes DQL algorithms to optimize drone patrol routes, thereby increasing detection accuracy and reducing response times.	
5	Enabling secure and trustworthy data management in forestry operations	A significant challenge in forest conservation lies in ensuring the reliability and security of collected data, as traditional forest management systems often suffer from data tampering, unauthorized access, and inefficient data sharing. This research addresses these issues by integrating Blockchain technology, which creates an immutable ledger to securely store forest-related data, including drone imagery, fire alerts, and biodiversity records. By decentralizing data storage and access, the Blockchain framework enhances transparency and trust in smart forestry operations, allowing stakeholders to make informed decisions based on verified and unaltered information.	[49]
6	Optimizing resource allocation and reducing operational costs	Smart forestry leverages automated drone networks and AI-driven analytics to optimize resource allocation for forest conservation. Using DQL, drones autonomously adjust their flight paths, manage energy use, and prioritize tasks based on real-time environmental data. This adaptive capability enhances operational efficiency and reduces the costs associated with manual forest monitoring, large-scale seed planting, and firefighting. Additionally, Blockchain technology enhances cost-effectiveness by streamlining administrative processes and reducing the risk of fraudulent reporting in forest management projects.	[43]
7	Enhancing sustainable logging and legal compliance	Illegal logging poses a significant obstacle to forest conservation, as it accelerates biodiversity loss and environmental degradation. Traditional enforcement methods often fail to provide real-time tracking, limiting their effectiveness in preventing unauthorized deforestation. To address this, smart forestry leverages AI-powered drones to monitor logging activities and automatically report violations. This study enhances legal enforcement by integrating Blockchain-based smart contracts that track, authenticate, and legally verify all logging operations before they proceed. Additionally, the application of DQL boosts the efficiency of drone surveillance in detecting patterns of illegal deforestation.	[43]
8	Facilitating global collaboration and data sharing	Effective forest conservation relies on coordinated efforts among government agencies, environmental organizations, and research institutions. Traditional data-sharing methods in forestry, however, remain fragmented and inefficient. This study introduces a Blockchain-based system that decentralizes and secures forestry data, enabling real-time access and tamper-proof sharing among diverse stakeholders. By enhancing transparency and collaboration, this smart forestry approach strengthens global conservation initiatives and supports the fight against deforestation, biodiversity loss, and climate change.	[45]

3.5. Drone Technology

Drone technology, also known as UAV technology, involves aircraft systems that operate without a human pilot onboard, either through remote control or autonomous navigation using onboard computers and sensors [2]. Initially developed for military purposes, drones have rapidly expanded into civilian, commercial, and industrial sectors due to their flexibility, affordability, and ease of use. The global drone market, valued at over US$30 billion in 2023, is expected to surpass US$90 billion by 2030. This surge is primarily fueled by growing demand in forestry and environmental applications. Governments and conservation agencies increasingly rely on drones for tasks such as biodiversity monitoring, ecological protection, and real-time surveillance of deforestation [50]. A typical drone integrates several key components that enable it to fly and collect data effectively. Its main frame supports the propulsion system, comprising motors, propellers, and electronic speed controllers, that generate lift and maneuverability [31]. At its core, the flight controller functions as an onboard computer, processing input from sensors such as the GPS module and Inertial Measurement Unit (IMU) to determine altitude, velocity, and orientation. High-resolution cameras mounted on stabilized gimbals allow the drone to capture sharp images and videos during flight. A lithium-polymer battery powers the system, while a communication module transmits real-time data and video to a ground control station. Drone types vary by application. Multi-rotor drones, such as quadcopters and hexacopters, are popular for tasks like aerial photography, mapping, and short-range surveys due to their vertical take-off and landing (VTOL) capabilities. Fixed-wing drones, which resemble airplanes, excel in long-distance missions like agricultural monitoring and environmental mapping, as they can cover large areas on a single charge. Single-rotor drones, similar in design to helicopters, offer longer flight times and greater payload capacity. Hybrid VTOL drones combine the strengths of rotor and fixed-wing models, making them well-suited for complex operations such as drone delivery [45]. Drones have transformed smart forestry by enabling efficient monitoring of forest health, detecting illegal logging, estimating biomass, and mapping forest areas using high-resolution aerial imagery and multispectral sensors [51][52]. They offer a cost-effective alternative to manned aircraft and satellite imaging, especially in remote or hard-to-access regions. By delivering real-time, high-resolution data, drones accelerate and enhance decision-making processes. Their use reduces the need for human presence in hazardous environments, thereby improving safety. Additionally, automating routine monitoring tasks lowers labor costs and enhances operational efficiency [53]. Despite their advantages, drones face several significant challenges. Limited battery life remains an important constraint, as most consumer and commercial models can only operate for 20 to 40 minutes per charge. Adverse weather conditions, such as strong winds and heavy rain, can disrupt flight stability and reduce data accuracy. Regulatory hurdles further complicate deployment, with airspace restrictions and permit requirements varying widely across regions and countries [54]. Growing concerns about privacy and potential misuse have also prompted demands for stricter regulations. Moreover, limited payload capacity restricts the type and quantity of equipment drones can carry, reducing their operational flexibility.

3.6. Components of Drone Technology

Drone technology, also known as UAV systems, comprises several essential components that work together to support autonomous or remote-controlled flight. Table II provides a brief description of the significant components of drone technology.

TABLE II: SUMMARY OF KEY COMPONENTS OF DRONE TECHNOLOGY.

S/No	Components	Description	References
1	Multispectral and thermal imaging cameras	In smart forestry, drones utilize multispectral and thermal imaging cameras to capture data that extends beyond human vision. Multispectral cameras detect various light wavelengths, such as red, green, blue, and near-infrared, to assess vegetation health, identify diseased trees, and measure chlorophyll levels. Thermal cameras detect temperature variations in tree canopies, allowing the identification of water stress, pest infestations, and animal activity. Together, these imaging systems supply essential data that supports forest health assessments and management planning.	[55]
2	GPS and GNSS modules	Accurate GPS or GNSS modules play a crucial role in forestry drones by enabling precise geolocation tagging. They map forest areas, mark boundaries, and georeference images for integration into GIS. By ensuring spatial alignment of data collected from multiple flights over large forested regions, these modules support the creation of detailed forest inventory maps, monitor deforestation trends, and track reforestation efforts over time.	[56]
3	LiDAR Sensors	Drones equipped with Light Detection and Ranging (LiDAR) sensors play a crucial role in smart forestry by emitting laser pulses and measuring the return times of these pulses after striking objects, such as tree branches or the forest floor. This process enables them to create high-resolution 3D models of forest structures, capturing details such as tree height, canopy density, and the volume of undergrowth. LiDAR proves particularly effective in dense forests, where thick foliage can block traditional optical imaging. It supports applications including biomass estimation, carbon stock assessment, and forest inventory analysis.	[57]
4	Flight controller with autonomous capabilities	Advanced flight controllers enable smart forestry drones to execute automated and pre-programmed missions, such as following waypoints, flying grid patterns, or maintaining altitude while collecting data. By automating these tasks, the drones reduce the need for manual piloting in rugged or expansive forest areas, enhancing both data consistency and operational safety. These autonomous features also facilitate repeated surveys over time, which are essential for analyzing temporal changes in forests caused by climate factors or human activity.	[58]
5	Powerful propulsion and an extended battery system	Forested areas often cover vast and varied terrains, so drones used in smart forestry require robust propulsion systems and long-lasting batteries. Brushless motors deliver the necessary thrust to carry heavy payloads, such as LiDAR or multispectral sensors, while large-capacity lithium-polymer batteries enable flight times of an hour or more. Efficient energy management systems monitor power consumption and automatically initiate return-to-home functions when battery levels run low, preventing drone loss within dense canopies.	[59]
6	Real-time data transmission and storage	Smart forestry drones typically carry communication systems that transmit telemetry data, such as altitude, battery status, and live video feeds, in real-time to ground stations. They sometimes store data onboard using high-capacity memory cards for later analysis and review. Real-time transmission proves especially valuable during disasters, such as forest fires or illegal logging, enabling immediate responses based on drone footage. This capability also supports collaborative decision-making by allowing remote experts to access and analyze data as it is collected.	[60]
7	Obstacle avoidance and terrain-following sensors	Forests contain numerous physical obstacles, including trees, branches, hills, and uneven terrain. Smart forestry drones detect and avoid collisions during flight by using obstacle avoidance systems with ultrasonic, visual, or infrared sensors. Additionally, some drones use terrain-following technology to adjust their altitude, maintaining a consistent height above uneven ground. These capabilities enable drones to navigate safely and efficiently, especially during low-altitude flights beneath dense canopies or in mountainous forest areas.	[61]
8	Integrated software and analytics platforms	Smart forestry drones use specialized software designed for environmental data analysis and decision support. After collecting data, the drones upload it to cloud-based platforms or forestry-specific GIS tools, where AI and machine learning analyze vegetation indices (such as NDVI), classify land cover, detect anomalies, and generate automated reports. This seamless integration enables forest managers to make informed, data-driven decisions for conservation, logging planning, and afforestation projects.	[62]
9	Environmental sensors	Some forestry drones carry additional environmental sensors, such as air quality monitors, humidity detectors, and temperature sensors, that collect data on	[19]

		microclimate conditions within the forest. Researchers utilize this information to investigate the effects of climate change on forest ecosystems, forecast wildfire risks, and evaluate the suitability of habitats for wildlife. By combining environmental data with imagery, they improve the holistic management of forest resources.	
10	Gimbal stabilization system	In forestry missions, drones rely on 2-axis or 3-axis gimbal stabilization systems to keep their cameras steady, especially when navigating rugged terrain or flying at low altitudes. This stabilization prevents drone movement from blurring or distorting images and videos, ensuring clear and stable footage. By capturing sharp visuals, drones enable accurate mapping and detailed observation of forest conditions, including the detection of signs of disease or illegal activity.	[55]

3.7. Benefits of Drone Technology in Smart Forestry

Drone technology is transforming smart forestry by combining aerial data collection with advanced analytics to enhance forest monitoring, resource management, and environmental conservation. Below are brief descriptions of the multifaceted benefits of drone applications in forestry.

3.7.1. Efficient forest monitoring and assessment

Drone technology enables rapid, efficient, and cost-effective tracking of extensive forested areas. Unlike traditional ground-based surveys, which are time-consuming, labor-intensive, and often hindered by rugged terrain, drones equipped with high-resolution cameras and sensors can fly over extensive forests to collect real-time data on canopy structure, tree height, density, and health. This capability enables forest managers to conduct frequent and timely assessments, thereby improving decision-making without the need to access every part of the forest physically [63].

3.7.2. Early detection of disease and pest infestation

Drones play a crucial role in forestry by enabling early detection of tree diseases and pest infestations. Equipped with multispectral or thermal imaging sensors, they identify subtle changes in foliage health, such as discoloration, reduced chlorophyll, or temperature anomalies, before these signs become visible to the naked eye. This early detection empowers forest managers to respond quickly, containing or treating affected areas to minimize damage and prevent the spread of pathogens or pests [25][64].

3.7.3. Enhanced reforestation and tree planting

Drones are transforming reforestation by mapping degraded areas and automating the process of tree planting. Equipped to shoot seed pods directly into the ground, they cover large areas faster than manual methods. Forestry teams utilize drone-based aerial surveys to pinpoint optimal planting sites, assess soil conditions, and monitor the survival rates of newly planted trees over time, thereby enhancing the regeneration of deforested and degraded ecosystems [64].

3.7.4. Real-time surveillance against illegal logging

Illegal logging frequently threatens forests, especially in remote or protected regions. Drones monitor these areas by providing real-time aerial surveillance, enabling authorities to detect unauthorized logging activities quickly. Equipped with live video feeds and GPS tracking, enforcement teams receive precise location information, allowing them to respond rapidly to suspicious movements. This approach enhances the effectiveness of forest protection and deters potential offenders.

3.7.5. Accurate inventory and resource management

Accurate maintenance of forest inventory data is essential for sustainable forestry. Drones rapidly collect information on tree counts, biomass volumes, and species distributions, enabling precise planning for timber harvesting, economic valuation, and balancing conservation with resource use. Advanced drone software automates data analysis, producing digital maps, 3D models, and detailed reports that enhance forest management strategies [2].

3.7.6. Support for fire prevention and management

In fire-prone regions, drones are supporting fire prevention and firefighting efforts. By using thermal cameras, they detect dry areas, heat signatures, and small fires early, preventing their spread. During wildfires, drones map affected zones, track fire movement, and assess damage, all while keeping human responders safe. They deliver crucial information that enables firefighters to devise precise containment strategies and protect personnel on the ground [51].

3.7.7. Environmental and wildlife monitoring

Drones support biodiversity conservation by tracking wildlife populations and monitoring changes in habitat. In forestry, they observe the presence and movements of key species, particularly within protected or endangered ecosystems. By doing

so, drones help evaluate the ecological health of forests and assess the impact of human activities on wildlife. Their non-intrusive operation enables researchers to gather data without disturbing animals or their natural habitats [65].

3.7.8. Cost reduction and operational efficiency

Drones significantly reduce the cost of forest management operations by offering a more affordable and personnel-efficient alternative to traditional methods, such as helicopters, satellite imagery, or ground crews. By automating data collection and minimizing the need for repeated manual labor, drones enable forest organizations to optimize their resources, cut expenses, and focus their efforts on analysis and strategic planning [52].

3.7.9. Improved decision-making with geospatial data

Drones generate georeferenced data that integrates with GIS, enabling detailed analysis and visualization. This integration allows forest managers to make informed decisions regarding land use, conservation priorities, and resource allocation. Using drone-produced 2D and 3D maps, stakeholders visualize forest conditions, monitor changes over time, and simulate various management scenarios to identify the most sustainable strategies [54].

3.7.10. Enhanced community engagement and education

In community-based forest management, drones empower community members by providing clear visualizations of their forests' condition. They enable residents to engage directly in mapping activities and gain a deeper understanding of how forestry practices affect their environment. By capturing aerial footage, drones support awareness campaigns, training programs, and stakeholder presentations, promoting collective responsibility for sustainable forest stewardship [50]. Fig. 6 summarizes the benefits of drone technology in smart forestry.

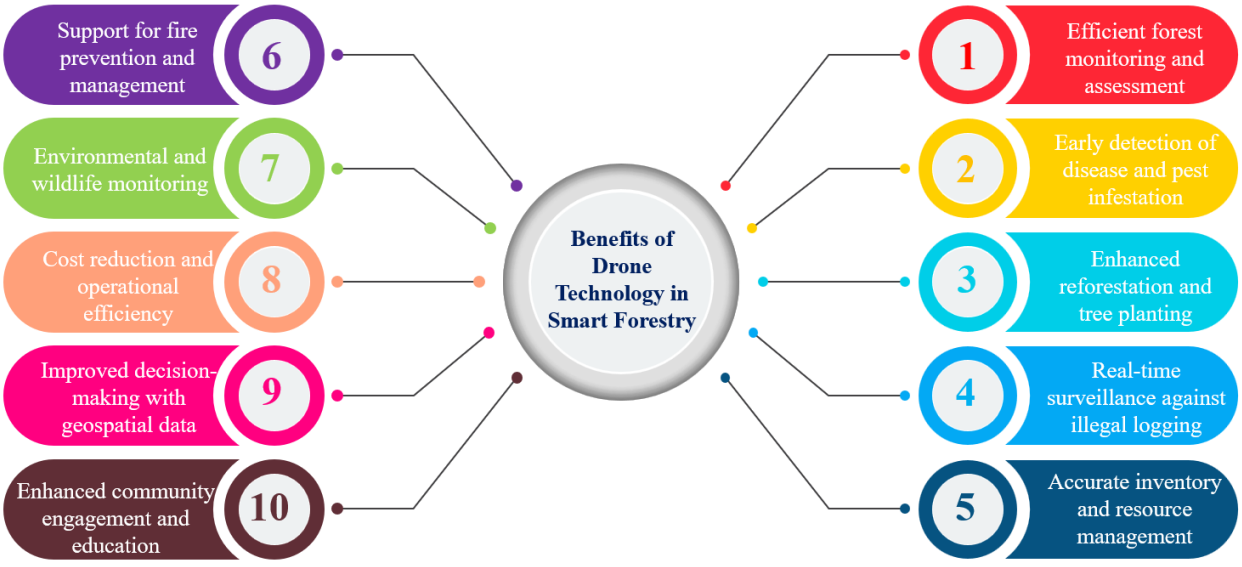

Fig. 6. Summary of the benefits of drone technology in smart forestry.

3.8. Trusted Cloud-Enabled Drone Network

A trusted cloud-enabled drone network integrates cloud computing with drone technology to create a secure, scalable ecosystem for managing drone operations [66]. In this system, drones gather large volumes of data, such as imagery, environmental metrics, and real-time video, and transmit it to the cloud for processing, storage, and analysis. Cloud platforms provide the computational power needed to manage this data efficiently and offer real-time global access. This infrastructure supports remote diagnostics, software updates, and flight scheduling, enabling operators to monitor and control their drone fleets effectively [67]. By centralizing data and operations, the cloud facilitates seamless collaboration among multiple drones and streamlines mission coordination. The trusted aspect of a cloud-enabled drone network ensures the security, privacy, and integrity of transmitted and stored data. Because drones often capture sensitive information, such as surveillance footage, environmental monitoring data, and geospatial records, it is paramount to implement robust encryption protocols, strict access controls, and adherence to data protection regulations. Trusted cloud platforms verify the authenticity and integrity of drone data, preventing tampering or compromise [68]. This trustworthiness boosts the reliability of cloud-based drone systems, making them well-suited for critical forestry applications. By harnessing the scalability and flexibility of cloud computing, the network can seamlessly accommodate an increasing number of drones, diverse data types, and a broader range of stakeholders without compromising security or performance [69].

3.9. How a Trusted Cloud-Enabled Drone Network Helps in Improving Smart Forestry

Below are brief descriptions of the numerous benefits a trusted cloud-enabled drone network delivers for smart forestry.

3.9.1. Scalable and flexible data management

A cloud-enabled drone network centralizes data storage, processing, and management, providing a scalable solution for drone operations. Drones transmit data, such as imagery, video footage, or environmental readings, directly to the cloud in real-time, where systems immediately process and analyze it. By eliminating the need for local hardware, cloud storage offers virtually unlimited capacity, making it ideal for managing large volumes of data during extended missions. Its inherent flexibility also allows users to scale resources quickly, such as adding drones or increasing processing power, to meet evolving operational demands [70].

3.9.2. Improved real-time collaboration and decision-making

Cloud-enabled drone networks offer a significant advantage by enhancing collaboration among multiple stakeholders. By leveraging a shared cloud platform, authorized users can access real-time drone data, including live feeds, status updates, and analytics, from any location with Internet connectivity. This immediate access enables teams to make faster decisions and coordinate more effectively. In forestry, such rapid data sharing and streamlined collaboration significantly reduce response times and boost operational efficiency [69].

3.9.3. Increased reliability and security

A trusted cloud platform offers robust security features that safeguard drone data against unauthorized access, loss, or tampering. By implementing encryption, multi-factor authentication, and other advanced security protocols, cloud services restrict data access to authorized personnel only. Cloud-enabled drone networks also leverage the reliability and redundancy of cloud infrastructure, with data backed up across multiple servers and geographic locations. This setup ensures uninterrupted access to data even if one server fails, maintaining continuity in drone operations [71].

3.9.4. Advanced data analytics and AI integration

Cloud platforms deliver the processing power needed to run advanced analytics and AI algorithms on data collected by drones. By integrating AI tools, cloud-enabled drone networks can automatically analyze large datasets, identify patterns, and generate actionable insights. In smart forestry, for instance, AI analyzes multispectral drone images to detect tree diseases and monitor forest health. Cloud computing accelerates this process by running complex models without relying on local hardware, thereby enhancing operational decision-making and improving outcomes [63].

3.9.5. Enhanced drone fleet management

A cloud-enabled network allows operators to efficiently manage multiple drones by centralizing control and providing real-time access to their status, health, and performance. Using a cloud interface, operators track drone locations, check battery levels, and receive real-time alerts for any issues. This system streamlines fleet coordination and supports seamless operations across large geographical areas. It also allows operators to deploy drones strategically, plan mission routes, and automate tasks, thereby minimizing human error and enhancing operational efficiency [25].

3.9.6. Cost efficiency and reduced infrastructure needs

Leveraging cloud infrastructure enables businesses and organizations to eliminate the need for expensive local servers, data centers, and ongoing maintenance. Instead of investing in physical hardware, they pay only for the resources they use, which significantly lowers upfront capital expenses and enhances resource efficiency. Cloud providers also offer features such as load balancing and auto-scaling, which dynamically allocate resources based on workload demands, further optimizing operational costs.

3.9.7. Remote monitoring and control

Cloud-based platforms enable operators to remotely monitor and control drones from virtually any location with Internet access. This capability proves especially valuable for managing drones in large or hard-to-reach areas, such as forests. By connecting drones to a cloud network, operators can control flights, receive live updates, and adjust flight plans in real time, thereby enhancing operational efficiency and safety.

3.9.8. Enhanced compliance and regulatory reporting

In industries with strict regulatory compliance, a trusted cloud-enabled drone network streamlines record-keeping and reporting by automatically storing and cataloging flight logs, mission data, and other essential records, ensuring that organizations accurately document all activities to meet aviation and environmental monitoring regulations. Moreover, cloud platforms generate compliance reports automatically, saving time and ensuring that records are complete and current.

3.9.9. Optimized drone performance through continuous updates

Cloud-enabled drone networks continuously update and improve drone software by remotely pushing the latest firmware and application versions to the entire fleet. This approach optimizes performance, fixes bugs, and introduces new features without manual intervention. By synchronizing all drones through cloud-based updates, the network maximizes operational efficiency, enhances mission success rates, and minimizes downtime [31].

3.9.10. Enhanced disaster recovery and data backup

In mission-critical applications, such as disaster management, cloud-enabled drone networks enhance disaster recovery by continuously storing data in the cloud, thereby facilitating rapid data retrieval and recovery. This proactive storage protects data from loss caused by hardware failures, drone crashes, or environmental factors. Cloud services incorporate data redundancy, so if a server is compromised or a drone is lost, backup copies of all critical data remain accessible. As a result, valuable data remains secure and accessible for analysis and decision-making even in the face of unexpected events [72].

Fig. 7 illustrates the key benefits that a trusted cloud-enabled drone network provides for smart forestry.

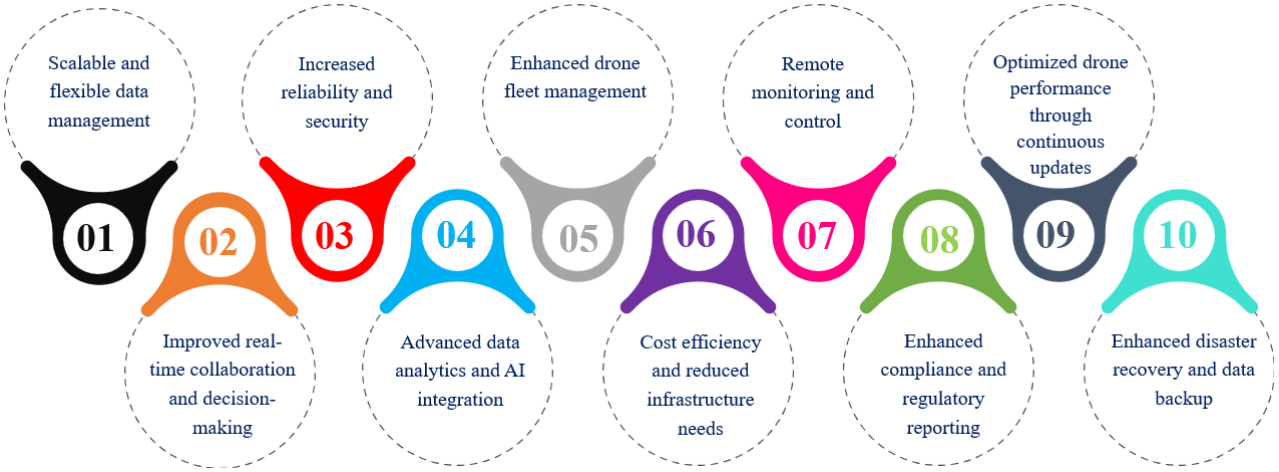

Fig. 7. Summary of the key benefits that a trusted cloud-enabled drone network provides for smart forestry.

3.10. Security Threats, Attacks, and Challenges Faced by Trusted Cloud-Enabled Drone Networks in Smart Forestry

Trusted cloud-enabled drone networks in smart forestry significantly advance environmental monitoring, precision forestry, and wildfire management. However, integrating UAVs with cloud computing and IoT technologies exposes the system to various security threats, attacks, and challenges. Below are brief descriptions of these concerns.

3.10.1. Unauthorized access and intrusion

Unauthorized access is when an attacker gains entry to the drone network, cloud infrastructure, or control systems without proper authentication or permission, often exploiting weak authentication protocols, default credentials, or insecure communication channels, such as unencrypted Wi-Fi or telemetry signals. For example, attackers may use leaked credentials to access a cloud dashboard managing drones monitoring Amazon deforestation, enabling them to alter flight paths, turn off drones, or steal sensitive data. They might also hijack unencrypted sessions during real-time forest fire monitoring to inject unauthorized commands and disrupt drone operations. Unauthorized access can result in data loss, operational disruptions such as misdirected fire detection, and diminished trust in public-private monitoring systems. Intrusion, a deliberate breach resulting from unauthorized access, involves manipulating data, payloads, or control commands through methods such as MitM attacks, command injection, or data spoofing. For instance, attackers may intercept and replace surveillance footage from drones monitoring illegal logging, inject false GPS data to redirect drones to hazardous locations, enable physical capture, or introduce malware via cloud APIs to maintain persistent control. These intrusions compromise mission integrity, produce inaccurate environmental data, create safety hazards, impose economic losses from damaged equipment and delays, and raise risks of drones being weaponized or used for illicit surveillance. Attackers can launch DoS, brute-force, and port-scanning attacks to disrupt operations and compromise data integrity [17].

3.10.2. Data privacy concerns

Data privacy presents a significant challenge in cloud-enabled drone networks used in smart forestry. Drones routinely collect sensitive information, such as images, soil conditions, species populations, and even human activity in forested areas, which,

if not adequately protected, can be exploited by unauthorized parties. This misuse risks violating the privacy of local communities and organizations [28]. Privacy risks increase when drones unintentionally capture private property or individuals, when cloud systems are breached, or when aggregated data enables unauthorized profiling. For example, drones mapping forest boundaries might inadvertently record backyard activities, or cyberattacks on geospatial data could provide competitors with unfair advantages. These risks not only compromise the integrity of environmental monitoring but also raise serious ethical and legal concerns for nearby communities [32].

3.10.3. Authentication vulnerabilities

Authentication vulnerabilities in cloud-enabled drone networks for smart forestry expose critical weaknesses that compromise data integrity, drone control, and operational security. Attackers exploit weak or hardcoded credentials, such as default logins or unencrypted API keys, to gain unauthorized access to drone controls or cloud dashboards. They hijack improperly managed tokens transmitted without encryption or regularly refreshed, allowing for impersonation and the injection of false data. A lack of mutual authentication allows drones to connect to rogue cloud servers, enabling attackers to issue malicious commands. Insecure API authentication, without measures such as IP whitelisting or multi-factor authentication, grants unauthorized access to sensitive data and operational patterns. Credential leakage through unsecured logging or debugging exposes authorization details to attackers, compromising security. At the same time, the absence of role-based access control permits users with excessive privileges to cause accidental or intentional harm. Replay attacks succeed when systems fail to implement time-sensitive tokens, allowing the reuse of intercepted credentials. Finally, poor validation of biometric or certificate-based authentication enables attackers to forge credentials and impersonate trusted users, collectively undermining the security of smart forestry drone networks. Inefficient authentication mechanisms enable malicious drones or users to infiltrate the network, increasing the risk of data theft, spoofing, and impersonation attacks [16]. Without robust verification protocols, unauthorized entities can exploit system vulnerabilities to gain access, compromise sensitive information, and disrupt legitimate communication within the network.

3.10.4. Denial-of-service (DoS) and distributed Denial-of-Service (DDoS) attacks

A DoS attack disrupts the availability of a service or resource by overwhelming it with excessive traffic or requests, usually originating from a single source. In drone networks, attackers may target drone control servers (e.g., ground stations or cloud APIs), communication channels (e.g., Wi-Fi, LTE, LoRaWAN), or onboard processing units (e.g., embedded AI modules). For instance, in a smart forestry operation, an attacker might flood a cloud-based drone management API with malformed or repetitive requests, causing connected drones to lose mission commands or real-time environmental updates. This disruption can result in the loss of telemetry and control, forcing drones to return to base or become unresponsive, which can lead to mission failure for tasks such as fire detection or anti-poaching surveillance and accelerate battery depletion due to processing excessive traffic. A DDoS attack exacerbates this threat by leveraging multiple compromised devices to overwhelm the target system, rendering detection and mitigation significantly more challenging. During a wildfire detection mission, for example, thousands of zombie devices may launch a coordinated DDoS attack against the cloud-based AI module that processes thermal images from drones. This can cause severe network congestion, cloud service degradation, delayed or lost sensor data, and an increased risk of drone crashes due to the loss of GPS corrections or flight instructions. By flooding network resources and critical systems, DDoS attacks severely impair the reliability, responsiveness, and safety of drone operations in smart forestry applications [26-28].

3.10.5. Man-in-the-middle (MitM) attacks

A MitM attack occurs when a malicious actor intercepts and alters communications between legitimate entities without their knowledge or consent. In cloud-enabled drone networks used for smart forestry, attackers exploit vulnerabilities in the data transmission between drones, ground control stations (GCS), and cloud services responsible for command and control, telemetry, and analytics. These drones collect high-resolution images and sensor data to monitor tree health, detect forest fires or illegal logging, and survey biodiversity. When this data travels over unsecured communication channels, such as unencrypted HTTP, weak SSH keys, or compromised Wi-Fi or LTE networks, attackers can intercept and manipulate it. They may use rogue base stations or steal session tokens to hijack active sessions, gaining unauthorized control over drones or cloud platforms. For instance, an attacker could feed false temperature readings to firefighting teams, redirect a drone to an unsecured location, or exfiltrate sensitive ecological data, jeopardizing national environmental monitoring efforts [26][33].

3.10.6. Spoofing and address spoofing

Spoofing in drone networks involves attackers impersonating legitimate entities, such as drones, ground control stations (GCS), or GPS satellites, to manipulate, intercept, or disrupt normal operations. In smart forestry, attackers employ various spoofing techniques to compromise drone missions. GPS spoofing misleads drones about their location, diverting them from designated monitoring zones, which results in data gaps or coverage of irrelevant areas, for instance, sending a fire-monitoring drone in the wrong direction during an emergency. Command spoofing enables malicious actors to intercept and

alter control instructions, potentially forcing drones to land prematurely or abandon surveillance tasks, such as those involved in illegal logging. Identity spoofing enables attackers to pose as trusted drones or GCS units, thereby accessing or redirecting sensitive data, often by mimicking legitimate credentials. Address spoofing—altering packet headers, such as IP or MAC addresses—allows attackers to gain unauthorized access to networks or cloud services. For example, a spoofed IP address may grant access to secure cloud-stored footage, while a manipulated MAC address can bypass network restrictions and join the drone mesh network. These attacks threaten operational continuity, compromise data integrity, mislead forest management efforts, and breach environmental data security. Furthermore, attackers may exploit spoofed identities to inject malicious traffic into the system, further undermining trust and functionality in smart forestry drone networks [33].

3.10.7. Eavesdropping attacks

Eavesdropping refers to the unauthorized interception of data transmitted over a network. It poses a significant threat to cloud-enabled drone networks in smart forestry, as they rely on wireless communication with cloud servers, edge devices, and other drones. Adversaries equipped with radio frequency sniffers, MitM tools, or software-defined radios can exploit unencrypted or weakly encrypted transmissions to access sensitive data, such as GPS coordinates, camera feeds, and sensor readings. Vulnerabilities arise from unprotected wireless links, compromised ground stations or cloud nodes using outdated protocols, and insecure inter-drone communications that lack mutual authentication. Real-world risks include poachers intercepting GPS data to target endangered wildlife, illegal loggers evading surveillance by monitoring drone patrol routes, and malicious actors disrupting fire detection efforts by delaying the transmission of thermal data. These breaches can lead to privacy violations, operational disruptions, legal liabilities under regulations such as the GDPR, and a decline in trust in drone-based automation. Without robust encryption and authentication, attackers can easily exploit drone networks to intercept and misuse ecological and operational data [16][33][73].

3.10.8. Data interception

Data interception involves unauthorized access to wireless communication between drones and the cloud, where sensitive information, such as forest imagery, sensor readings, and monitoring data, is transmitted. Drones typically use Wi-Fi, 4G, or 5G networks to send data to cloud platforms, and without proper encryption and secure communication protocols, these transmissions become vulnerable to interception. Malicious actors can exploit this vulnerability through several methods: (i) MitM attacks, where they intercept and potentially alter data—such as manipulating NDVI readings to hide illegal logging; (ii) signal jamming and GPS spoofing, which misguide drones by feeding them false coordinates, leading to misidentification of protected areas; (iii) compromising drones or edge gateways to leak or corrupt data before it reaches the cloud, thereby distorting analytics, such as in deforestation monitoring; and (iv) intercepting unencrypted transmissions, such as thermal images during wildfire surveillance, which can then be sold, thereby undermining public safety efforts [15].

3.10.9. GPS jamming

Trusted drone networks rely on real-time geolocation data to perform autonomous tasks, including precision mapping, forest health monitoring, detecting illegal logging, wildfire surveillance, and biodiversity assessment. These drones coordinate with each other and cloud-based systems to collect, process, and transmit large volumes of spatially tagged data. However, GPS jamming—by disrupting signal reception—can severely impair navigation, compromise data integrity, and destabilize coordinated operations. Affected drones may drift off course, initiate emergency landings, or become lost, particularly during autonomous missions. In swarm operations, jamming can prevent drones from maintaining formation, increasing the risk of mid-air collisions and mission failure. Cloud systems that rely on accurate timestamps and geotags may receive corrupted data, rendering large-scale analyses unreliable. Such disruptions can also trigger trust violations in secure systems, prompting shutdowns or re-authentication protocols that halt operations [29].

3.10.10. False data injection

False data injection (FDI) attacks are cyber threats in which adversaries deliberately insert deceptive, erroneous, or misleading data into a system to disrupt operations, mislead decision-making, or manipulate outcomes. In smart forestry, which relies on drones, IoT sensors, cloud computing, and AI for real-time monitoring and data-driven management, FDI attacks pose significant risks. Attackers may target any stage of the data pipeline—onboard drones, during wireless transmission, or at the cloud server—resulting in misclassified forest health, undetected wildfires or pest outbreaks, false alerts, and misdirected conservation efforts. For example, attackers might simulate fire conditions by injecting false heat or smoke data, conceal illegal logging by manipulating canopy density readings, misroute drones through GPS spoofing, or mask infestations by falsifying vegetation health data. These attacks can lead to environmental degradation, economic losses resulting from wasted or misallocated resources, operational disruptions due to eroded trust in automated systems, and broader security risks, including potential state or corporate espionage through manipulated environmental data [17][33][34].

3.10.11. Malware attacks

Malware attacks pose a serious security threat to cloud-enabled drone systems in smart forestry, particularly when these drones operate within broader networks integrated with cloud services. Attackers can inject malware into drone software or cloud platforms, compromising both the drone's functionality and the integrity of the collected data. In ransomware incidents, attackers encrypt critical data, such as ecological records, wildlife monitoring information, or forest health metrics, and demand payment for decryption [30]. Malware often infiltrates drone operations through compromised firmware updates, unsecured application programming interfaces (APIs), or infected ground control stations. Once inside, it enables attackers to hijack drones, turn off essential functions, leak sensitive information, or conduct espionage. For instance, malware embedded in a cloud-based update could turn off GPS and obstacle sensors, potentially leading to crashes and data loss. These threats disrupt operations, damage the environment, compromise data integrity, waste resources, and escalate security risks. Exploiting vulnerabilities in drone firmware, such as PX4 and Ardupilot, attackers employ tactics including malicious firmware injection, sensor tampering, and SQL/NoSQL attacks, underscoring the urgent need for robust cybersecurity measures in smart forestry [17][33][34].

3.10.12. Insider threats

Insider threats arise when authorized individuals, such as employees, contractors, or third-party vendors, intentionally or inadvertently compromise the security and operations of drone systems and cloud platforms. In smart forestry, insiders with access to drone-collected data may exfiltrate sensitive information, such as timber inventories, locations of rare species, or proprietary AI models used for image recognition and analysis. For example, a data analyst may sell high-resolution imagery and classification models to a competitor. Technicians or administrators might deliberately alter system configurations, introduce vulnerabilities, or tamper with flight control software, causing drones to crash or deviate from planned paths. Cloud administrators could abuse elevated privileges to hijack drone fleets for unauthorized surveillance or data manipulation. Others may falsify sensor data, such as underreporting thermal readings to hide forest fire risks, while some may embed malicious code in firmware during development or maintenance. Insiders can also create vulnerabilities by misusing remote access tools or VPNs, or by neglecting cybersecurity best practices, such as sharing passwords or disabling security features for convenience. These actions can lead to data breaches, loss of drone control, or manipulation of critical environmental data [74].

3.10.13. Drone hijacking and remote-control takeover

Drone hijacking involves malicious actors gaining unauthorized control over a drone's communication and navigation systems, often by exploiting vulnerabilities in cloud-enabled networks such as weak communication protocols, unsecured cloud interfaces, or outdated firmware. Techniques such as GPS spoofing, Wi-Fi or telemetry interception, and MitM attacks are commonly used to intercept or manipulate drone operations. Remote control takeover occurs when an attacker gains unauthorized access to a drone's command channels and assumes complete control over its actuators and payload, including cameras and sensors. Unlike simple interception, this type of attack allows the intruder to operate the drone, making it significantly more dangerous. In smart forestry, attackers pose a serious threat by compromising edge devices, exploiting insecure cloud services, or conducting Firmware Over-the-Air (FOTA) attacks to install malicious software. For instance, an adversary might use a vulnerable firmware update mechanism to embed a backdoor in drones monitoring illegal logging. Such hijacking enables complete control over actuators and payloads, allowing attackers to divert, disable, or misuse drones for espionage or sabotage. Notably, researchers at Johns Hopkins demonstrated remote drone hijacking in 2018 by exploiting flaws in radio protocols. Reports from forestry applications have linked drone crashes or disappearances to GPS spoofing near illicit logging zones. The consequences include corrupted environmental data, disrupted operations like fire or pest detection, financial losses from lost assets, and heightened security risks due to the misuse of drones equipped with sensitive sensors. Implementing encrypted communication and strong authentication for remote control commands remains essential to preventing such attacks [19].

3.10.14. Physical capture

Drones operating in remote forestry environments face significant risks of physical capture, which can lead to data breaches, hardware tampering, and network compromise. Malicious actors who seize a drone can extract stored data such as GPS logs, images, and telemetry; reverse-engineer its components to uncover vulnerabilities; alter its firmware or software for future cyberattacks; or spoof its identity to re-enter the system as a legitimate node. These threats are particularly acute in cloud-enabled drone networks that depend on continuous connectivity for real-time processing and decision-making. Forests exacerbate these risks due to their vast, isolated terrain, unpredictable weather, and lack of security infrastructure. For example, illegal loggers might destroy or exploit a surveillance drone to erase evidence, while poachers could use a captured wildlife monitoring drone to locate animal habitats or deploy decoys. Similarly, unauthorized access to a fire-mapping drone could leak or manipulate critical data, delaying emergency responses. The consequences include data leakage, network infiltration, disrupted monitoring, and financial losses, making physical capture a vital security concern for smart forestry systems [73].

3.10.15. IoT Botnets and edge device vulnerabilities

Smart forestry relies on cloud-enabled drone networks and IoT devices to monitor forest health, detect illegal logging, track wildlife, and assess wildfire risks. These systems collect and transmit data via edge gateways to centralized cloud services, but their interconnectivity exposes them to significant cybersecurity threats. IoT botnets, which exploit weak authentication, outdated firmware, and unsecured communication protocols, can compromise drones and edge devices, allowing attackers to launch DDoS attacks, exfiltrate data, or manipulate drone behavior. For instance, a variant of the Mirai botnet could target unsecured edge controllers in drone networks, turning off real-time environmental monitoring. Resource-constrained and remotely deployed edge devices, such as drone control units and field sensors, often lack multi-factor authentication, run outdated firmware, and use unencrypted communication protocols, making them vulnerable to exploitation. Attackers can intercept data, inject malicious commands, or physically tamper with devices to extract credentials or reprogram firmware. If compromised, edge analytics software can transmit manipulated data to cloud systems, triggering false wildfire alerts or corrupting forest management databases. Simulated attacks on LoRaWAN-based forestry sensor networks demonstrate how unauthenticated access enables the injection of false data, highlighting the urgency of securing drone-IoT ecosystems against botnet-driven threats.

3.10.16. Cloud vulnerabilities

Cloud-enabled drone networks in smart forestry integrate sensor-equipped drones with cloud computing to monitor forest health, detect wildfires, track biodiversity, and manage resources efficiently. While this architecture enhances scalability, real-time access, and centralized control, it also expands the system's attack surface, introducing significant cloud-related vulnerabilities. These include data breaches, insecure APIs, DoS attacks, data integrity compromises, and insider threats. For example, attackers may exploit misconfigured APIs to hijack drones or access the GPS coordinates of rare species, enabling illegal activities such as logging or poaching. Cloud service outages, insider misuse, and poor configuration management can disrupt operations or expose sensitive ecological data. Inadequate logging, lack of encryption, and legal non-compliance further compound these risks, potentially leading to undetected tampering, data theft, or legal penalties. By relying heavily on cloud and IoT platforms, smart forestry systems become susceptible to both traditional and emerging cybersecurity threats, necessitating robust security measures across all layers of the architecture [17][18].

3.10.17. Trust and data integrity challenges

In smart forestry, cloud-enabled drone networks automate critical tasks, including data collection, surveillance, forest health monitoring, wildfire detection, preventing illegal logging, and assessing biodiversity. However, integrating these drones with cloud infrastructure introduces serious trust and data integrity challenges that threaten the reliability and security of the entire system. Trust concerns arise at multiple levels: drones and sensors may become compromised through malware, unauthorized access, or hardware faults, leading to manipulated data and flawed environmental models; communication channels are susceptible to interception, spoofing, and data injection attacks, potentially triggering false alarms or misdirecting emergency responses; and cloud service providers introduce dependencies on third-party security practices and data governance, where breaches could expose sensitive, geo-referenced information. Data integrity faces similar risks, including tampering and spoofing by malicious actors, transmission errors caused by environmental interference, and a lack of end-to-end verification mechanisms such as cryptographic hashes or digital signatures. These vulnerabilities can distort machine learning outcomes, hinder timely decision-making, and mask illegal activities [22][23][75][76].

3.10.18. Standardization issues

Cloud-enabled drone networks offer transformative capabilities for real-time data collection, forest health monitoring, and precision silviculture. However, gaps in standardization across data formats, communication protocols, cloud service APIs, cybersecurity, regulatory compliance, time synchronization, sensor calibration, metadata, and workflows hinder their scalability and interoperability. For example, drones from different manufacturers often use proprietary formats that prevent seamless integration of LiDAR or multispectral data, and mismatched telemetry protocols impede real-time swarm coordination. Divergent cloud APIs create vendor lock-in that complicates multi-stakeholder analytics, while inconsistent encryption and authentication measures expose sensitive geospatial data to breaches. Without harmonized beyond-visual-line-of-sight regulations and airspace standards, cross-border deployments stall, and a lack of uniform timestamping and geospatial referencing introduces spatial-temporal errors when fusing data from drones, satellites, and IoT sensors. Inconsistent sensor calibration protocols also yield incomparable measurements, such as divergent NDVI values from different multispectral cameras. Absent metadata schemas undermine the provenance, reproducibility, and long-term archiving of ecological assessments. Ultimately, these fragmented standards degrade data quality and security across smart forestry applications [77].

3.10.19. Data processing complexity

Cloud-enabled drone networks in smart forestry offer powerful capabilities for monitoring, data collection, and environmental management; however, they introduce significant processing challenges due to the volume, variety, and speed of the data involved, as well as the demand for real-time decision-making. Drones equipped with sensors such as LiDAR, hyperspectral, RGB, and thermal cameras generate vast, heterogeneous datasets—including high-resolution images, 3D models, and environmental metrics—that require scalable cloud infrastructure and optimized data pipelines to ensure timely processing. Integrating diverse data types—structured GPS coordinates, semi-structured sensor metadata, and unstructured imagery—demands careful preprocessing, normalization, and synchronization to enable effective analysis, such as tree species classification or disease detection. Real-time applications, such as fire detection or wildlife tracking, require low-latency processing, where delays in transmission or analysis can lead to serious ecological consequences. Limited connectivity in remote forests exacerbates these issues, often forcing drones to store data locally and delaying analysis. Running AI/machine learning models on high-dimensional data adds further computational strain, requiring dynamic resource allocation and GPU acceleration to manage simultaneous data streams. Coordinating multiple drones introduces synchronization challenges, as accurate analytics depend on temporally and spatially aligned data. Projects operating in ecologically or culturally sensitive regions must comply with strict data security and privacy protocols, implementing encryption and access controls throughout the cloud workflow. Due to limited onboard power, drones rely on edge computing for preliminary processing, which raises complex trade-offs between edge and cloud computation. Ultimately, the use of complex AI models can compromise interpretability and erode stakeholder trust, underscoring the importance of integrating explainable AI to enhance transparency, accountability, and safe deployment [24][77].

3.10.20. Scalability and coordination

In smart forestry, drone networks are increasingly performing critical tasks such as forest monitoring, wildlife tracking, disease detection, and fire prevention; however, scaling these networks across vast forested areas presents significant challenges. As the number of drones grows, they generate massive volumes of data—high-resolution images, multispectral sensor inputs, and real-time video—that strain bandwidth and introduce latency, especially given the limitations of cellular and satellite infrastructure. For instance, a fleet of 50 drones can produce terabytes of data daily, potentially overwhelming communication channels and delaying responses. Simultaneously, cloud systems must be able to elastically scale to process this influx in real-time, particularly during peak events like wildfire season, where delays could undermine early warnings. Energy constraints further limit scalability, as coordinating drones with limited flight times demands efficient, cloud-integrated scheduling. Operational coordination adds complexity: drones must avoid collisions in obstacle-rich environments, such as forests, dynamically reallocate tasks in response to events like pest outbreaks, and maintain synchronization despite unreliable connectivity. These issues intensify with scale as centralized cloud control becomes a bottleneck and a potential point of failure. Decentralized solutions offer resilience but require sophisticated, fault-tolerant protocols [25].

3.10.21. Resource constraints

Cloud-enabled drone networks play a vital role in smart forestry by enabling efficient monitoring, data collection, and forest resource management; however, they face critical resource constraints that limit performance, reliability, and scalability. Drones rely on limited battery life, which restricts flight duration and operational range, especially in vast or remote forest areas where complex terrain increases energy consumption. For instance, a drone conducting multispectral imaging for tree health may only operate for 20–30 minutes before needing to be recharged, disrupting continuous data acquisition. Bandwidth limitations and poor connectivity, caused by dense canopy cover and remote locations, hinder real-time data transmission, resulting in latency and potential data loss during critical operations, such as wildfire monitoring. Despite leveraging cloud computing, drones must still perform real-time tasks, such as obstacle avoidance and adaptive navigation, locally, which is constrained by their limited onboard computational power. Storage capacity also poses challenges, as drones must temporarily store large volumes of raw data, which can sometimes lead to data loss or compression that compromises quality, particularly during long surveys. Latency from cloud-based processing further hampers real-time applications, such as pest outbreak detection, where an immediate response is crucial. Rain, fog, and wind degrade sensor performance and communication reliability, thereby increasing energy consumption and necessitating mission repetition. These constraints not only affect operational efficiency but also complicate the implementation of robust security protocols, prompting researchers to explore lightweight encryption and edge computing solutions to protect data and maintain functionality [32].

3.10.22. Regulatory and compliance risks

Trusted cloud-enabled drone networks in smart forestry face significant regulatory and compliance risks that can hinder deployment, scalability, and the effective use of data. These challenges arise from the intersection of advanced technologies, such as drones, cloud computing, and AI, with sensitive domains, including environmental monitoring, land ownership, and data privacy. Key risks include violations of aviation and airspace regulations, as drones must comply with national rules, such as Federal Aviation Administration (FAA) certification in the U.S. A research group in Oregon was fined for

unauthorized drone operations. Data privacy laws, such as the European Union General Data Protection Regulation and California Consumer Privacy Act (CCPA), pose risks when drones capture personally identifiable information, as seen in Scandinavia, where footage of individuals on private land led to GDPR violations. Cross-border data transfer adds complexity, as exemplified by a Canadian project halted due to concerns that data stored by a U.S. cloud provider did not meet Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) standards. Environmental laws also present challenges; in Indonesia, a project was shut down for flying drones in protected ecosystems without required permits. Cybersecurity lapses, such as a ransomware attack on an Australian agency's cloud-stored drone data, reveal the consequences of not meeting standards like ISO/IEC 27001. Disputes over intellectual property and data ownership can arise, as illustrated by a German startup that commercialized an AI model without obtaining consent from the data-owning agency. Finally, relying on third-party cloud providers introduces shared responsibility risks, as seen when an EU forestry analytics company lost funding due to its vendor's non-compliance with GDPR [31].

3.10.23. Design flaws

Cloud-enabled drone networks in smart forestry hold significant promise but face critical challenges due to inherent design flaws and a lack of operational and technical standards. Many systems rely on centralized architectures that route data to remote cloud servers, resulting in high latency, bandwidth bottlenecks, and potential communication failures, particularly in remote forest areas with limited connectivity. For instance, drones monitoring forest fires may fail to transmit thermal imagery in real-time if uplinks are weak, thereby delaying crucial alerts. Scalability also poses a significant issue, as large fleets generate vast amounts of high-resolution data that can overwhelm processing and network capacity. This is evident in an Amazon-based project, where over 50 drones caused data upload failures and incomplete mapping. Inadequate edge-cloud collaboration forces drones to rely excessively on cloud computing for tasks such as image recognition, introducing delays in pest detection. This reliance also contributes to energy inefficiency, as continuous data streaming drains battery life and shortens mission range, limiting operational effectiveness in vast plantations. Compounding these problems, many networks lack built-in fault tolerance or redundancy, leaving them vulnerable to outages and data loss during missions. Combined with weak cybersecurity standards, these design flaws significantly undermine the reliability and resilience of drone-based forestry systems [17].

4. BLOCKCHAIN TECHNOLOGY AND DEEP Q-LEARNING

4.1. Blockchain Technology

Blockchain technology operates as a decentralized, distributed ledger that securely records transactions across a network of computers, ensuring transparency, immutability, and trust without relying on a central authority [78-80]. It groups transactions into blocks, links them cryptographically in chronological order, and prevents retroactive alterations unless one modifies all subsequent blocks and gains network consensus [78-80]. This structure enhances data integrity and security, making Blockchain particularly valuable in smart forestry. In this context, stakeholders can use Blockchain to track and verify forest resource data, monitor timber supply chains, ensure regulatory compliance, and promote transparency in conservation efforts. By integrating smart contracts—self-executing agreements encoded directly onto the Blockchain—systems can automate tasks such as logging permit approvals, carbon credit trading, and resource allocation with greater efficiency and security.

4.1.1. Features of Blockchain Technology

Table III provides a brief description of the features of Blockchain technology.

TABLE III: SUMMARY OF KEY FEATURES OF BLOCKCHAIN TECHNOLOGY.

S/No	Features	Brief Description	References
1	Decentralization	Blockchain technology is fundamentally decentralized, distributing control across a network of nodes rather than relying on a single authority, unlike traditional centralized systems. Each network participant has access to the same data, and a consensus mechanism ensures the validation of transactions. This structure removes the need for intermediaries, minimizes the risk of single points of failure, and fosters trust among users. Platforms like Bitcoin and Ethereum utilize decentralization to facilitate peer-to-peer transactions, thereby promoting greater transparency and user autonomy.	[79-81]
2	Immutability	Immutability ensures that once data is recorded on a Blockchain, it remains unchanged and cannot be deleted. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, thereby forming a secure and permanent record of transactions. To change information in a single block, one would need to modify all subsequent blocks across the entire network—a task nearly impossible without majority control. This immutability plays a vital role in applications that demand high integrity and auditability of records, including smart forestry.	[79][80][82]
3	Transparency	Blockchain technology enhances transparency by granting all authorized participants access to a shared ledger. In public Blockchains, every transaction is recorded and visible to all users,	[79][80][83]

		enabling independent verification and auditing. Even in private or permissioned Blockchains, participants can access data within predefined limits. This transparent structure fosters trust among users and proves especially valuable in supply chain tracking, public records management, and governance applications.	
4	Security	Blockchain ensures security through cryptographic techniques and consensus protocols. Each transaction is encrypted and linked to the previous one using hashing algorithms, forming an immutable chain of transactions. Consensus mechanisms—such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT)—validate transactions and prevent unauthorized changes. These features make it extremely difficult for hackers to tamper with data or carry out attacks. Due to its tamper-resistant design, Blockchain proves especially valuable in sectors such as smart forestry.	[79][80][84]
5	Consensus mechanism	A consensus mechanism enables a Blockchain network to validate transactions and reach an agreement on the current state of the ledger. Different Blockchains employ various algorithms, such as PoW, PoS, or Delegated Proof of Stake (DPoS), to achieve consensus. These mechanisms prevent any single entity from controlling or tampering with the data, thereby safeguarding the network's integrity. By facilitating collective agreement in decentralized and trustless environments, consensus mechanisms play a critical role in maintaining trust.	[79][80][85]
6	Distributed ledger	Blockchain operates as a distributed ledger that replicates the same data across all nodes in the network, giving every participant access to a shared, authoritative record. Unlike centralized databases managed by a single authority, distributed ledgers enable collective record-keeping, strengthen system resilience, and maintain functionality even when some nodes fail or are compromised. This decentralized structure proves essential in environments that demand continuous uptime and protection against tampering.	[12][79][80]
7	Anonymity and pseudonymity	Public Blockchains offer anonymity and pseudonymity by displaying transactions on a transparent ledger, representing users through cryptographic addresses rather than their real names. This approach protects user privacy yet allows for transaction traceability. However, advanced Blockchain analytics can sometimes deanonymize users. In contrast, private Blockchains can enforce complete user identification, depending on the specific application requirements.	[79][80][86]
8	Smart contracts	Smart contracts are self-executing agreements that encode predefined rules and conditions into code, allowing them to carry out transactions automatically once those conditions are met without requiring human intervention. Deployed on Blockchain platforms such as Ethereum, they power decentralized applications (DApps) and simplify complex processes across various sectors, including insurance, legal agreements, and supply chain management. By eliminating intermediaries, reducing human error, and boosting operational efficiency, smart contracts enhance the reliability and speed of digital transactions.	[2][79][80]
9	Traceability	Blockchain enhances asset and transaction traceability by recording every ledger entry with a timestamp and linking it to previous records. This structure enables users to follow the complete history of a digital asset or transaction. Industries such as agriculture, pharmaceuticals, and forestry benefit significantly from this capability, as it allows them to track the origin and movement of products or resources. For example, in smart forestry, Blockchain technology traces the entire lifecycle of timber—from the forest to the consumer.	[79][80][87]
10	Tokenization	Blockchain enables the tokenization of physical and digital assets, allowing tokens to represent a range of assets, including currency, property, stocks, forest carbon credits, and biodiversity assets. These tokens can be securely and efficiently transferred on the Blockchain, facilitating fractional ownership, enhancing liquidity, and lowering transaction costs. In smart forestry, stakeholders can use tokenization to transparently and efficiently manage and trade carbon credits or forest produce.	[20][79][80]

4.1.2. Importance of Blockchain Technology in Addressing Security Challenges in Cloud-Enabled Drone Network for Smart Forestry

Integrating drone technology with cloud computing has revolutionized smart forestry by enabling the collection, processing, and real-time remote monitoring of forest ecosystems. Drones equipped with high-resolution sensors and connected to cloud platforms enhance forest mapping, biodiversity assessment, detection of illegal logging, and fire surveillance. However, this integration also introduces significant cybersecurity risks. Blockchain technology offers a robust, decentralized solution that protects the integrity, confidentiality, and availability of data within these systems. Below are brief descriptions of the importance of Blockchain technology in addressing security challenges in a Cloud-enabled drone network for smart forestry.

- **Enhanced data integrity and tamper-proof records**

Blockchain technology guarantees that data collected by drones and stored in the cloud remains tamper-proof and immutable. In smart forestry, drones gather crucial information, such as forest density, fire risks, illegal logging activities, and biodiversity metrics, and record each data upload or modification on the Blockchain. By time-stamping and permanently logging every transaction, the system prevents undetected alterations, ensuring the integrity and reliability of the data. This trusted, accurate data supports effective, evidence-based decisions in forestry management and conservation efforts [88].

- **Decentralized and secure data storage**

Cloud-enabled drone systems face a critical vulnerability due to their reliance on centralized cloud storage, which creates a single point of failure. By utilizing Blockchain technology, the system distributes data across multiple network nodes, ensuring that even if one node is compromised or fails, the data remains accessible and protected from cyberattacks. In smart forestry, this decentralized approach enhances resilience against DDoS attacks and unauthorized data tampering, allowing for continuous and secure monitoring and management of forest resources [43].

- **Improved authentication and access control**

Blockchain enables robust authentication by assigning each drone, user, or device in the forestry ecosystem a unique cryptographic identity stored on the Blockchain. The system grants access to drone controls, data logs, and cloud interfaces only after verifying these identities through Blockchain authentication. This approach significantly reduces the risk of unauthorized access and insider threats, thereby maintaining operational control over drone networks and safeguarding sensitive ecological data [89].

- **Secure communication between drones and cloud services**

Integrating Blockchain with communication protocols secures drone-to-cloud and drone-to-drone communications through cryptographically signed transactions. This approach verifies and authenticates all commands, data transmissions, and updates on the Blockchain. In smart forestry, the system prevents spoofing, MitM attacks, and data injection by allowing only authorized commands and legitimate data to flow through the network [90].

- **Auditability and transparency**

Blockchain's transparent and traceable ledger enables easy auditing of all drone operations and data interactions by immutably recording every drone flight, data upload, system change, and access request. This transparency helps smart forestry projects track who accessed specific data, when, and for what purpose, thereby maintaining accountability among users, operators, and stakeholders. Additionally, it facilitates compliance with environmental regulations and supports reporting obligations to government agencies and donor organizations [10].

- **Smart contract automation for real-time response**

Blockchain enables smart contracts—self-executing agreements that automatically trigger actions when predefined conditions are met. In smart forestry, these contracts can deploy drones during emergencies such as forest fires, illegal logging, or pest outbreaks. When a drone detects a threat, the smart contract immediately notifies relevant authorities or activates a drone swarm for further monitoring. This approach enhances operational efficiency, reduces response times, and ensures that actions are based on secure, verifiable data [7].

- **Strengthened trust among stakeholders**

Forestry operations involve multiple stakeholders, including government agencies, NGOs, environmentalists, local communities, and drone operators, who require a trustworthy platform for transparent and secure data sharing. Blockchain enables these parties to share information directly without relying on a central authority, thereby building the shared trust essential for collaborative forest management. This technology supports fairness, minimizes conflicts, and encourages cooperation in data-driven forest governance, particularly in areas with sensitive environmental and community rights concerns [90].

4.2. Deep Q-learning

DQL is a reinforcement learning technique that enables drones to make intelligent decisions by interacting with their environment and optimizing actions based on the rewards they receive. In smart forestry applications such as forest monitoring, fire detection, and pest control, DQL offers an effective approach to autonomous decision-making. Unlike traditional Q-learning, which struggles with high-dimensional state spaces, DQL uses deep neural networks to approximate the optimal Q-values for selecting actions. This integration makes DQL well-suited for handling the real-time complexity and uncertainty of forestry environments [91]. By estimating the expected cumulative reward for each action in a given state, the deep neural network guides drones to follow an optimal policy, continuously improving their performance. DQL extends the classical Q-learning algorithm by using deep neural networks to approximate the Q-function. This function predicts the expected cumulative reward for taking a specific action in a given state and then following the optimal policy. Traditional Q-learning relies on a tabular representation of the Q-function, which becomes impractical in environments with large or continuous state spaces. To overcome this, DQL utilizes a deep neural network to approximate Q-values, enabling agents to process high-dimensional inputs, such as images or sensor data [92]. During training, the agent collects experiences as tuples of (state, action, reward, next state) while interacting with the environment and stores them in a replay buffer. The network then randomly samples mini-batches from this buffer to break the correlation between sequential data points, thereby stabilizing the learning process [83]. It minimizes the loss between predicted Q-values and target Q-values calculated using the Bellman equation. To further improve stability, DQL utilizes target networks that generate consistent target Q-values

and employs exploration strategies, such as the greedy method, to balance exploring new actions with exploiting learned policies. These techniques enable DQL to tackle complex decision-making problems across various domains effectively [93].

4.2.1. Importance of Deep Q-Learning in Improving the Security of Trusted Cloud-Enabled Drone Network for Smart Forestry

Some of the benefits of DQL in improving the security of trusted cloud-enabled drone network for smart forestry include the following.

- **Autonomous threat detection and response**

DQL enables drones to detect and respond to security threats in real-time autonomously. In trusted cloud-enabled drone networks, drones are constantly exposed to cyber threats, including spoofing, unauthorized access, and abnormal communication behavior. By combining Q-learning with deep neural networks, DQL enables drones to learn optimal actions through continuous interaction with their environment. When applied to security, a DQL agent can identify attack indicators, such as unusual traffic patterns, fake GPS signals, or unauthorized data requests, and respond accordingly. Based on its learned policy, the drone can proactively switch communication channels, return to base, or trigger an alert without human intervention. This adaptive, real-time decision-making significantly strengthens the drone's resilience to evolving cyber threats [39].

- **Dynamic network traffic analysis and anomaly detection**

DQL dynamically analyzes network traffic to detect anomalies that may signal cyberattacks. In cloud-enabled drone systems, where large volumes of data are constantly transmitted to and from the cloud, DQL models learn to monitor traffic patterns and distinguish between normal and abnormal behavior. Unlike static rule-based intrusion detection systems, DQL continuously updates its policy based on new data, allowing it to adapt to emerging threats. For instance, when it detects a sudden spike in data packets or irregular transmission intervals, the DQL agent can identify potential DDoS attacks or data leaks and respond by rerouting traffic, limiting connections, or isolating compromised nodes. This proactive approach helps maintain secure and stable communication within the system [11].

- **Adaptive security policy management**

DQL enables drone-cloud systems to implement adaptive, context-aware security policies that respond effectively to dynamic threats. Unlike traditional security mechanisms that rely on static rules, DQL agents learn optimal policies by maximizing long-term rewards through continuous environmental feedback. In smart forestry applications, drones can adjust their security behavior in real-time based on factors such as terrain, weather conditions, mission-criticality, and risk levels. For example, a drone might switch between high and low encryption modes to conserve battery life or modify authentication requirements based on its location. This context-driven adaptability allows drones to maintain both effective and efficient security under varying operational conditions [20].

- **Proactive resource allocation for security tasks**

DQL enables intelligent allocation of limited drone resources, such as battery power, bandwidth, and computational capacity, for security tasks. Given the constraints of onboard resources, drones must carefully balance security operations with mission-critical activities. A DQL-based system learns to optimize resource allocation for functions such as intrusion detection, encryption, and data verification without compromising overall performance. For instance, it can prioritize stronger security measures when flying over sensitive areas or transmitting critical data while conserving energy during less critical periods by scaling back security efforts. This adaptive approach enhances both the efficiency and security of cloud-enabled drone operations [9].

- **Improved trust evaluation and access control**

DQL strengthens trust evaluation mechanisms to manage access in cloud-based drone networks. In multi-agent drone systems operated through cloud platforms, accurately assessing the trustworthiness of each node —whether a drone or a user —is critical. DQL models continuously analyze the behavior of drones, users, and cloud nodes by learning from their interactions over time. Based on these observations, the system assigns trust scores and dynamically decides whether to grant, restrict, or deny access. For example, suppose a drone exhibits abnormal behavior or tries to access restricted cloud resources. In that case, the DQL model can immediately revoke its access rights, effectively mitigating risks from insider threats or compromised devices [21].

- **Real-time decision-making in high-risk scenarios**

DQL enables real-time decision-making in high-risk scenarios such as cyberattacks or physical intrusions. In smart forestry, drones often operate in environments where swift responses are critical to prevent data breaches or bodily harm, including

theft, fire, or illegal logging. DQL agents continuously assess the environment, evaluate possible actions, and select optimal responses with minimal delay. For instance, if a drone detects interference with its navigation system—potentially caused by GPS spoofing—the DQL model can activate secondary navigation protocols, adjust altitude, or initiate an emergency landing based on prior learned experiences. This capability significantly strengthens operational security and improves mission success [20]. Fig. 8 summarizes the importance of DQL in enhancing the security of a trusted cloud-enabled drone network for smart forestry.

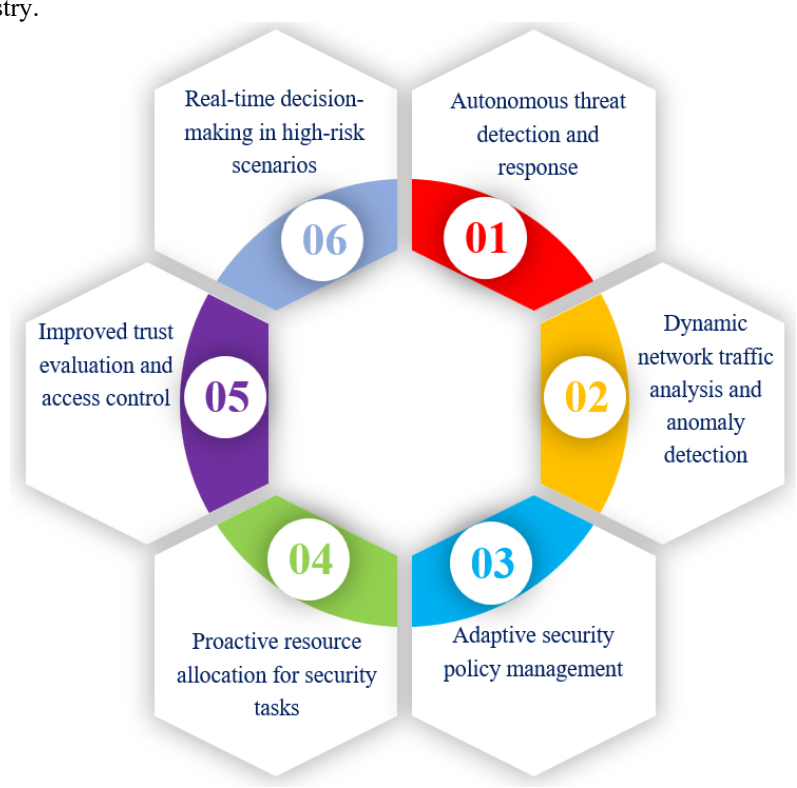

Fig. 8. Summary of the importance of DQL in enhancing the security of trusted cloud-enabled drone technology.

4.3. Framework for Blockchain Technology and DQL in Trusted Cloud-Enabled Drone Network for Smart Forestry

A multi-layered framework integrates Blockchain technology, DQL, and trusted cloud-enabled drone networks to advance smart forestry through enhanced data integrity, autonomous decision-making, and secure communication. At its core, Blockchain ensures transparency, immutability, and traceability of the environmental data drones collect. The cloud infrastructure provides scalable storage and computational resources, enabling real-time processing and secure access to this data. Drones, equipped with IoT sensors and connected via trusted cloud networks, monitor forest conditions by detecting tree health, fire outbreaks, and illegal logging. DQL empowers these drones to autonomously learn and optimize flight paths, data collection strategies, and energy use in response to environmental feedback. This integrated approach enables intelligent, efficient, and secure forest monitoring and management, ultimately promoting sustainable forestry and biodiversity conservation [52][94]. Integrating Blockchain technology with DQL creates a robust framework that strengthens the security and reliability of cloud-enabled drone systems in smart forestry. This synergy addresses emerging threats and operational challenges while promoting smarter, safer, and more autonomous environmental monitoring. Fig. 9 depicts the proposed framework.

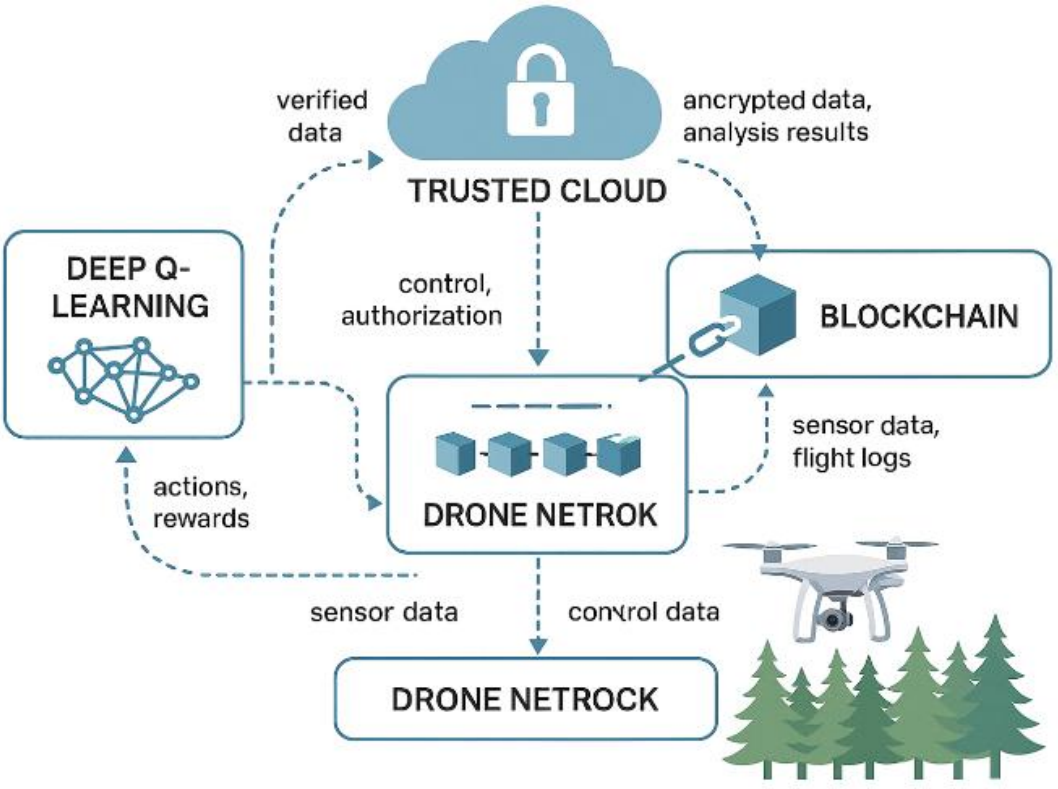

Fig. 9. Depicts the proposed framework.

Below are the brief descriptions of the key benefits of this proposed framework.

4.3.1. Secure data sharing and integrity

Blockchain technology secures drone-collected data in smart forestry by creating a decentralized, tamper-proof ledger for recording activities, environmental data, and operational logs. As drones gather sensitive information, such as deforestation patterns, wildlife movements, and fire risks, Blockchain preserves the integrity of this data once it is transmitted via the cloud. By ensuring the data remains immutable and protected from alteration, Blockchain fosters trust among stakeholders, including government agencies, NGOs, and researchers [37].

4.3.2. Decentralized authentication and access control

Traditional authentication systems rely on centralized structures, making them susceptible to single points of failure and cyberattacks. By contrast, Blockchain enhances security through decentralized identity management and access control. Developers can utilize smart contracts to specify which drones, users, or systems are authorized to access specific data or perform particular functions. This approach ensures that only authorized entities interact with drones or cloud services, thereby minimizing the risk of unauthorized access or tampering [67].

4.3.3. Adaptive threat detection

DQL empowers drones and cloud systems to learn optimal responses to evolving cybersecurity threats. In smart forestry environments, where drones operate under dynamic and unpredictable conditions, traditional static security measures often fall short. DQL enables the system to adapt in real time by learning from interactions, detecting anomalous behavior patterns, and deploying optimal defense strategies. This adaptive capability makes DQL highly effective in countering complex and continuously changing cyber threats [95].

4.3.4. Optimized resource allocation and energy efficiency

Smart forestry operations often deploy drones with constrained battery life and limited computational power. DQL optimizes flight paths, schedules data transmissions, and manages energy consumption by learning from environmental and network conditions. At the same time, Blockchain technology ensures transparency, auditability, and security in these decisions, which are critical factors for ensuring long-term sustainability and meeting regulatory requirements [96].

4.3.5. Resilient coordination of multi-drone systems

Forestry surveillance often involves deploying multiple drones simultaneously to monitor large areas. DQL efficiently coordinates these drones, optimizing coverage while preventing redundancy and collisions. Integrating Blockchain technology enables real-time logging of each drone's decisions and updates, creating a shared, trusted, and synchronized mission view. This integration minimizes the risk of miscommunication, spoofing, and conflicting commands [97].

4.3.6. Improved trust and accountability

The combination of Blockchain's transparency and the decision-making intelligence of DQL creates a traceable and accountable system that fosters trust among operators, environmental agencies, and local communities. For example, when a drone detects a deforestation incident, Blockchain records the precise time, location, and verification steps. At the same time, DQL determines the optimal response, such as alerting authorities or redirecting another drone [91].

4.3.7. Scalability and future-readiness

Blockchain combined with DQL enables scalable deployments that are crucial for expanding smart forestry initiatives across larger ecosystems. As more drones and sensors are added, Blockchain's decentralized structure eliminates bottlenecks, while DQL continuously refines its learning models to manage growing complexity. This synergy ensures that the system remains future-proof and adaptable to new technologies and emerging environmental threats [41].

5. REAL-WORLD SCENARIOS AND PRACTICAL IMPLEMENTATIONS OF INTEGRATING BLOCKCHAIN AND DQL FOR TRUSTED CLOUD-ENABLED DRONE NETWORKS IN SMART FORESTRY

Trusted cloud-enabled drone networks have significantly advanced smart forestry applications by integrating Blockchain and DQL technologies. Below are real-world scenarios and examples illustrating their implementation:

5.1. UAV-Assisted Internet of Vehicles: A Framework Empowered by Reinforcement Learning and Blockchain

In 2025, researchers proposed a framework to address the challenges of selecting relay nodes and coordinating UAVs in the Internet of Vehicles (IoV). The framework employs a two-sided UAV relay selection mechanism, a decentralized Multi-Agent Deep Reinforcement Learning (MDRL) model that autonomously coordinates UAV mobility to maintain network coverage and connectivity, and a Blockchain system to ensure transparency and traceability. By training the MDRL model to manage UAV movements, the framework enables effective decentralized coordination among UAVs. Evaluation results show that these mechanisms enhance the stability of relay selection while maximizing both coverage and connectivity [98].

5.2. Blockchain-Enhanced UAV Networks for Post-Disaster Communication

In 2024, a consortium developed a Blockchain-enabled framework to address challenges in coordinating heterogeneous UAVs during post-disaster scenarios. They implemented a consortium Blockchain architecture to secure and privatize multi-agency coordination, utilizing a hybrid consensus protocol that combined DPoS with PBFT. The system employed decentralized flocking algorithms to enable adaptable and autonomous operations among UAV clusters, ensuring effective disaster relief despite uncertain connectivity. Simulations demonstrated that the framework scaled throughput linearly with up to 500 UAV nodes while maintaining high throughput and low latency, even under cyberattacks [40][104].

5.3. Blockchain-Based Crowdsourced Deep Reinforcement Learning as a Service

Alagha et al. [99] proposed a novel framework that enhances accessibility to Deep Reinforcement Learning (DRL) services by leveraging Blockchain technology. This system delivers DRL-related services, including training and model sharing, directly to users. Crowdsourcing enables users to tap into the expertise and computational power of workers to train DRL solutions. Built on a Consortium Blockchain, the framework ensures traceable and autonomous execution through smart contracts that manage the allocation of workers and models. The authors demonstrate the framework's effectiveness across several DRL applications.

5.4. Blockchain-Powered IoT Platform for Autonomous Drone Operations in Smart Farming

Devi et al. [100] developed a Blockchain-powered IoT platform to enhance autonomous drone operations in smart farming, prioritizing environmental sustainability. By combining a public Blockchain for transparent transaction recording with a private Blockchain for secure storage of sensitive data, the platform addresses key challenges such as flight safety, data privacy, and supply chain management. By integrating UAVs, IoT, and Blockchain technologies, the platform enhances precision farming practices and supports sustainable agriculture.

5.5. Blockchain-Based Data Management and Optimization in Secure Fog Environments

Khan et al. [101] proposed B-Drone, a collaborative system that integrates Blockchain technology, specifically Hyperledger Fabric, with a metaheuristic-enabled genetic algorithm to manage fog nodes efficiently. B-Drone securely handles drone-based data collection, scheduling, optimization, processing, management, and preservation within fog nodes. They

implemented and deployed Blockchain smart contracts to automatically manage all connectivity and communication protocols between drones and fog nodes in a private permissioned network. The simulations demonstrate that this approach reduces computing costs and enhances performance, highlighting its effectiveness in drone-led data management. Integrating Blockchain and DQL into trusted cloud-enabled drone networks transforms smart forestry by enhancing secure communication, data management, and autonomous operations. These advancements enable more efficient and sustainable forestry practices, demonstrating the significant potential of these technologies in modernizing and optimizing forest management.

6. CHALLENGES AND LIMITATIONS

Integrating Blockchain technology and DQL into trusted, cloud-enabled drone systems for smart forestry holds great promise for improving security, trust, and operational efficiency. However, to implement these technologies effectively, it is essential to address several challenges and limitations that currently hinder their full potential. These challenges and limitations include the following:

6.1. High computational and energy demands

Both Blockchain and DQL require substantial computational resources. Blockchain systems, particularly those utilizing consensus mechanisms such as Proof of Work (PoW), consume substantial energy and processing power to validate transactions and maintain a decentralized ledger. Likewise, training and updating DQL models involve intensive computations using neural networks. In smart forestry applications, where drones and sensors operate with limited battery capacity and constrained hardware, these high resource demands pose a critical challenge [1][58].

6.2. Scalability issues

Blockchain and DQL technologies face significant scalability challenges. Blockchain networks typically experience slow transaction speeds and limited throughput as they scale, which can impede real-time communication and logging among hundreds of drones and cloud services operating in large forest areas. Similarly, DQL struggles to maintain efficient performance when confronted with large state and action spaces, reducing its effectiveness in managing complex and diverse forest environments [1][94].

6.3. Data storage and bandwidth limitations

Blockchain does not efficiently handle the large volumes of sensor or image data typically generated by drones in smart forestry. Instead, it serves better as a platform for storing hashed summaries and metadata. However, using external storage solutions such as the cloud raises concerns about trust and security. Moreover, real-time drone operations driven by DQL depend on stable, high-speed bandwidth for learning updates and cloud synchronization—conditions that are often lacking in remote forested regions [1][57].

6.4. Training complexity and data requirements in DQL

DQL relies on large, diverse datasets for effective training; however, collecting such data in forest ecosystems poses significant challenges due to environmental variability, sensor inaccuracies, and the rarity of events like forest fires or illegal logging. These limitations can cause DQL models to overfit or perform poorly in unfamiliar conditions. Inadequate training may lead drones to make unsafe or ineffective decisions, undermining both security and environmental objectives [1][60].

6.5. Interoperability and integration challenges

Integrating Blockchain and DQL into existing smart forestry systems poses significant challenges because drones, sensors, and cloud platforms use diverse protocols and data formats. Ensuring seamless interoperability among these components demands standardized interfaces and middleware. Without effective integration, the system may experience performance issues and increased security risks due to miscommunication between subsystems [1][102][103].

6.6. Latency and real-time constraints

Consensus protocols in Blockchain can delay the validation and recording of transactions, posing a serious risk in time-sensitive applications such as forest fire detection or intrusion response. These delays can hinder timely action and compromise effectiveness. Likewise, DQL models must adapt quickly to dynamic environmental changes; however, overly complex models or slow systems can reduce responsiveness, allowing threats to outpace the system and ultimately weakening overall security [1][8].

6.7. Cost of implementation and maintenance

Forestry departments and environmental NGOs often face significant barriers due to tight budgets when deploying Blockchain nodes, training DQL models, maintaining drones, and securing cloud infrastructure. They must also manage

ongoing system maintenance, such as updating smart contracts, retraining AI models, and ensuring cybersecurity, which increases both operational complexity and costs [1][20].

6.8. Security vulnerabilities and attack vectors

Although Blockchain is inherently secure, attackers can still exploit vulnerabilities. For example, internal collusion or majority control attacks can compromise private Blockchains. Likewise, adversaries can manipulate data subtly to deceive DQL models and influence their decisions. Developing robust defense mechanisms to counter these threats remains an ongoing challenge [1].

7. FUTURE RESEARCH DIRECTIONS

As Blockchain and DQL continue to integrate into cloud-enabled drone networks for smart forestry, researchers and technologists must explore several critical frontiers to enhance efficiency, scalability, and security. These future research directions will drive innovation and advance the capabilities of this emerging field. Below are detailed future research directions that can drive this innovation in smart forestry.

7.1. Enhancing Blockchain scalability and energy efficiency

Blockchain-based drone networks face a significant challenge due to the high computational and energy demands of consensus mechanisms, such as PoW. To address this, future research should prioritize the development of lightweight, energy-efficient alternatives, such as PoS, DPoS, and PBFT. Researchers can also enhance transaction speed and scalability by implementing layer-2 solutions, such as sidechains and sharding, allowing drones to register and verify forestry data instantly without delays.

7.2. Improving the adaptability and learning capabilities of DQL models

DQL models rely on large datasets and ongoing training to adapt to the dynamic conditions of forest environments. To enhance adaptability, future research should prioritize meta-reinforcement learning and transfer learning, enabling drones to respond quickly to emerging forestry challenges, such as detecting new pest species or identifying fire hazards. Additionally, by implementing federated learning, drones can securely share learned policies across different regions without compromising sensitive data, thereby improving overall model efficiency.

7.3. Integration with IoT and edge computing for real-time decision-making

The integration of IoT devices, edge computing, and cloud-based drone networks offers a powerful means to improve real-time decision-making in smart forestry. Future research should aim to reduce latency by enabling edge nodes, such as forest sensors, edge servers, and mobile base stations, to handle computation locally. By allowing drones to process environmental data on-site before transmitting it to the cloud, this approach enhances response times for fire detection, poaching alerts, and illegal logging monitoring while also minimizing bandwidth usage.

7.4. Privacy-preserving mechanisms for secure data sharing

Blockchain-based drone networks must prioritize privacy and secure access control when handling sensitive environmental data. Future research should integrate zero-knowledge proofs, homomorphic encryption, and differential privacy to enable stakeholders, such as government agencies and environmental organizations, to verify data authenticity while maintaining confidentiality and data privacy. Smart contract-powered role-based access control mechanisms can further ensure that only authorized personnel access critical forestry data collected by drones.

7.5. Development of decentralized autonomous organizations (DAOs) for forestry management

Decentralized Autonomous Organizations (DAOs) have the potential to revolutionize forest conservation and resource management by enabling transparent, Blockchain-driven governance. Through smart forestry initiatives, stakeholders such as conservationists, researchers, and local governments can collaborate within decentralized frameworks powered by automated smart contracts. These systems facilitate fair resource allocation, ensure equitable funding distribution for reforestation projects, and enable the verifiable enforcement of environmental policies.

7.6. Multi-drone collaboration and swarm intelligence

Future research should investigate how multi-agent reinforcement learning (MARL) and swarm intelligence can enhance drone coordination in smart forestry. By applying collective learning techniques, drones can dynamically cooperate to carry out large-scale tasks such as mapping forest health, detecting fire outbreaks, and monitoring wildlife movements. Incorporating Blockchain smart contracts can ensure secure, tamper-proof coordination, effectively blocking malicious interference with drone operations.

7.7. AI-optimized Blockchain for reducing storage overhead

Blockchain systems require substantial storage capacity to maintain decentralized records, presenting a challenge for drone networks with limited onboard storage. To address this, future research should develop AI-optimized Blockchain solutions that incorporate dynamic compression, pruning mechanisms, and off-chain storage to minimize storage requirements while preserving security and immutability. Integrating the InterPlanetary File System (IPFS) and distributed cloud storage can further enhance the efficient handling of high-resolution images and videos captured by drones in forestry applications.

7.8. Sustainable energy solutions for drone operations

To support the long flight durations required in smart forestry, future research should focus on optimizing the energy efficiency of drones. Researchers should investigate the integration of solar-powered drones, wireless charging stations within forest environments, and energy-harvesting technologies to extend the flight times of drones. Incorporating AI-driven energy management systems can further enhance efficiency by predicting optimal flight routes and dynamically adjusting power consumption based on mission priorities.

7.9. Legal and ethical frameworks for Blockchain-enabled drone surveillance

Deploying autonomous drone networks at scale for forestry monitoring raises significant concerns about regulatory compliance, data sovereignty, and ethical considerations in surveillance. Future research should prioritize the development of standardized legal frameworks for cross-border drone operations, ethical applications of AI, and secure, responsible data-sharing protocols supported by Blockchain technology. Governments and environmental agencies must collaborate to develop policies that promote ecological sustainability and human rights while fostering technological innovation.

7.10. Interoperability with other smart environmental systems

To maximize impact, Blockchain and AI-powered drone networks in forestry must interoperate with other smart environmental systems, including climate monitoring networks, biodiversity databases, and carbon credit trading platforms. Future research should focus on developing cross-chain interoperability protocols that allow forestry Blockchain systems to integrate seamlessly with global environmental initiatives, thereby enhancing data transparency and fostering collaboration across organizations.

Blockchain and DQL will revolutionize trusted, cloud-enabled drone networks in smart forestry by transforming forest conservation, resource management, and environmental sustainability. Advances in Blockchain scalability, AI learning adaptability, decentralized governance, privacy-preserving techniques, swarm intelligence, and sustainable energy solutions will drive innovation in this domain. By addressing these research challenges, we can develop secure, autonomous, and intelligent forestry management systems that safeguard the long-term health of global forests while leveraging cutting-edge technology.

8. CONCLUSION

Integrating Blockchain technology and DQL into cloud-enabled drone networks marks a significant shift in smart forestry, enabling real-time decision-making, secure data management, and efficient resource allocation. Blockchain ensures the integrity and authenticity of drone-collected data through its decentralized, tamper-proof ledger, preventing unauthorized access and promoting transparency among stakeholders. Smart contracts automate critical forestry tasks such as fire detection, reforestation, and anti-logging efforts, ensuring reliable and timely execution. This survey examines how Blockchain strengthens data integrity, access control, and trust among diverse agents in drone networks, particularly in decentralized settings that require secure and verifiable data logging. Meanwhile, DQL enables drones to autonomously adapt to dynamic forest environments by optimizing flight paths, managing energy consumption, and responding to potential threats. By leveraging DQL for control and decision-making, drones can navigate complex forestry terrains with greater efficiency, effectively avoid obstacles, and operate in a more energy-efficient and scalable manner. Integrating these technologies within Cloud computing frameworks enables drones to offload computational tasks and collaborate efficiently across large forest areas. However, this integration introduces several technical and operational challenges, including latency, scalability, high computational demands, energy constraints, model convergence difficulties, and the overhead of Blockchain consensus mechanisms, all of which require careful and strategic resolution. This survey analyzes existing literature to identify research gaps. It proposes a potential framework for Blockchain Technology and DQL in a trusted cloud-enabled drone network for smart forestry. It emphasizes the need for interdisciplinary collaboration across forestry, AI, cybersecurity, and wireless communication to drive real-world implementation. Advancing lightweight Blockchain systems, energy-efficient drones, and scalable DQL frameworks remains critical. By integrating Blockchain and DQL, smart forestry can promote sustainable resource management while enhancing global biodiversity conservation and environmental resilience. These technologies, when combined, create an intelligent and secure ecosystem that enables autonomous monitoring, predictive analytics, and automated interventions. As a result, applications such as early wildfire detection, reforestation tracking, and carbon credit verification can be conducted with greater accuracy and efficiency. The integration of Blockchain and deep Q-learning in cloud-enabled drone networks offers significant potential to transform smart forestry. Future research should prioritize the development of energy-efficient, scalable, and secure frameworks that can adapt to the environmental

variability and operational demands of large-scale forestry applications. Tackling these challenges will enable the creation of more transparent, autonomous, and sustainable forest monitoring systems, thereby advancing global environmental conservation efforts.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

Non.

References

[1] G. Ali, M. M. Mijwil, I. Adamopoulos, and J. Ayad, "Leveraging the Internet of Things, Remote Sensing, and Artificial Intelligence for Sustainable Forest Management," *Babylonian Journal of Internet of Things*, vol. 2025, pp. 1–65, 2025, doi: 10.58496/BJIoT/2025/001.

[2] D. Commey, B. Mai, S. G. Hounsinou, and G. V. Crosby, "Securing blockchain-based IoT systems: A review," *IEEE Access*, vol. 12, pp. 98856–98881, 2024, doi: 10.1109/ACCESS.2024.3428490.

[3] D. Bhardwaj, A. Kanjiya, N. K. Jadav, S. Desai, and S. Tanwar, "Deep Q-network-based stock market optimization for improving stock trends," in *Proc. 2nd Int. Conf. Futuristic Technologies (INCOFT)*, Belagavi, India, Nov. 24–26, 2023, pp. 1–6, doi: 10.1109/INCOFT60753.2023.10425365.

[4] P. Zhao, Y. Lu, Y. Wei, and S. Leng, "Blockchain and DQN enabled co-evolutionary routing scheme in UAV networks," in *Proc. IEEE INFOCOM Workshops*, Hoboken, NJ, USA, May 20, 2023, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225997.

[5] R. Mishra, M. Kaif, A. Raj, and R. Deep, "Blockchain enabled farmer centric supply chain management using reinforcement learning," in *Proc. 14th Int. Conf. Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, Jul. 6–8, 2023, pp. 1–7, doi: 10.1109/ICCCNT56998.2023.10307187.

[6] Z. Qawaqneh and A. A. Mallouh, "A deep reinforcement learning framework for training SARSA agents to improve consensus in blockchain networks," in *Proc. 3rd Int. Conf. Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, Tenerife, Spain, Jul. 19–21, 2023, pp. 1–7, doi: 10.1109/ICECCME57830.2023.10253427.

[7] Y. Liang *et al.*, "Distributed dynamic pricing strategy based on deep reinforcement learning in a presale mechanism," *Sustainability*, vol. 15, no. 13, pp. 1–20, 2023, doi: 10.3390/su151310480.

[8] A. A. Mallouh *et al.*, "An efficient method for refining reinforcement learning to reach consensus in P2P networks," *IEEE Access*, vol. 11, pp. 38665–38679, 2023, doi: 10.1109/ACCESS.2023.3268283.

[9] D. S. Gadiraju, V. Lalitha, and V. Aggarwal, "An optimization framework based on deep reinforcement learning for prism blockchain," *IEEE Trans. Services Computing*, vol. 16, no. 4, pp. 2451–2461, 2023, doi: 10.1109/TSC.2023.3242606.

[10] G. Kabanda, C. T. Chipfumbu, and T. Chingoriw, "Utilizing deep reinforcement learning and Q-learning for improved Ethereum cybersecurity," *Int. J. Advanced Networking and Applications*, vol. 14, no. 6, pp. 5742–5753, 2023, doi: 10.35444/ijana.2023.14612.

[11] W. Zhang, W. Fan, G. Zhang, and S. Mao, "Learning-based joint service caching and load balancing for MEC blockchain networks," *China Communications*, vol. 20, no. 1, pp. 125–139, 2023, doi: 10.23919/JCC.2023.01.011.

[12] K. Moghaddasi and M. Masdari, "Blockchain-driven optimization of IoT in mobile edge computing environments with deep reinforcement learning and multi-criteria decision-making techniques," *Cluster Computing*, vol. 27, no. 4, pp. 4385–4413, 2024, doi: 10.1007/s10586-023-04195-4.

[13] D. Daoun, Z. Alom, and M. A. Azim, "Reinforcement learning in blockchain-enabled IIoT networks," in *Proc. 3rd Int. Conf. Computing, Networks and Communications (CNC)*, Gwalior, India, Dec. 8–10, 2022, pp. 226–240, doi: 10.1007/978-3-031-43145-6_19.

[14] A. Singh, "Application of mobile edge computing and deep learning in mobile blockchain for security and safety," in *Proc. 3rd Int. Conf. Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, May 12–13, 2023, pp. 2034–2038, doi: 10.1109/ICACITE57410.2023.10183155.

[15] L. Cooper and D. MacFarlane, "Climate-smart forestry: Promise and risks for forests, society, and climate," *PLOS Climate*, vol. 2, no. 6, pp. 1–26, 2023, doi: 10.1371/journal.pclm.0000212.

[16] R. Amin *et al.*, "IoDseC++: Authenticated key exchange protocol for cloud-enabled internet of drone communication," *J. Ambient Intelligence and Humanized Computing*, vol. 14, pp. 9529–9542, 2023, doi: 10.1007/s12652-023-04623-8.

[17] S. Ashraf *et al.*, "IoT-empowered smart cybersecurity framework for intrusion detection in internet of drones," *Scientific Reports*, vol. 13, pp. 1–20, 2023, doi: 10.1038/s41598-023-45065-8.

[18] S. van der Haar *et al.*, "Climate-smart cocoa in forest landscapes: Lessons from institutional innovations in Ghana," *Land Use Policy*, vol. 132, pp. 1–17, 2023, doi: 10.1016/j.landusepol.2023.106819.

[19] D. Varveris *et al.*, "Distributed and collaborative tree architecture: A low-cost experimental approach for smart forest monitoring," *Baltic J. Modern Computing*, vol. 11, no. 4, pp. 653–685, 2023, doi: 10.22364/bjmc.2023.11.4.07.

[20] T. Kwantwi *et al.*, "Blockchain-based computing resource trading in autonomous multi-access edge network slicing: A dueling double deep Q-learning approach," *IEEE Trans. Network and Service Management*, vol. 20, no. 3, pp. 2912–2928, 2023, doi: 10.1109/TNSM.2023.3240301.

[21] M. J. J. Rakkini and K. Geetha, "Q-learning model for selfish miners with optional stopping theorem for honest miners," *Int. Trans. Operational Research*, vol. 31, no. 6, pp. 3975–3998, 2024, doi: 10.1111/itor.13359.

[22] T. Hai *et al.*, "Blockchain-based trustworthiness in cross-border data exchange in 5G-powered intelligent connected vehicles," *IEEE Network*, vol. 38, pp. 90–97, 2024, doi: 10.1109/MNET.2024.3399751.

[23] T. Garg *et al.*, "Drones as a service for 5G networks and blockchain-assisted IoT-based smart city infrastructure," *Cluster Computing*, vol. 27, pp. 8725–8788, 2024, doi: 10.1007/s10586-024-04354-1.

[24] A. Buchelt *et al.*, "Exploring artificial intelligence for applications of drones in forest ecology and management," *Forest Ecology and Management*, vol. 551, pp. 1–15, 2024, doi: 10.1016/j.foreco.2023.121530.

[25] A. Hafeez *et al.*, "Implementation of drone technology for farm monitoring and pesticide spraying: A review," *Information Processing in Agriculture*, vol. 10, no. 2, pp. 192–203, 2023, doi: 10.1016/j.inpa.2022.02.002.

[26] O. Stefan and A. Codrean, "Networked control of a small drone resilient to cyber attacks," *Drones*, vol. 8, no. 10, pp. 1–21, 2024, doi: 10.3390/drones8100552.

[27] W. Guo *et al.*, "A DDoS tracking scheme utilizing adaptive beam search with unmanned aerial vehicles in smart grid," *Drones*, vol. 8, no. 9, pp. 1–19, 2024, doi: 10.3390/drones8090437.

[28] M. Hoppen *et al.*, "Smart forestry: A forestry 4.0 approach to intelligent and fully integrated timber harvesting," *Int. J. Forest Engineering*, vol. 35, no. 2, pp. 137–152, 2024, doi: 10.1080/14942119.2024.2323238.

[29] F. Ehrlich-Sommer *et al.*, "Sensors for digital transformation in smart forestry," *Sensors*, vol. 24, no. 3, pp. 1–26, 2024, doi: 10.3390/s24030798.

[30] C. Rodriguez Franco *et al.*, "Biochar utilization as a forestry climate-smart tool," *Sustainability*, vol. 16, no. 5, pp. 1–15, 2024, doi: 10.3390/su16051714.

[31] Y. Du and J. Q. Li, "A deep reinforcement learning-based algorithm for distributed precast concrete production scheduling," *Int. J. Production Economics*, vol. 268, Art. no. 109102, 2024, doi: 10.1016/j.ijpe.2023.109102.

[32] N. Singh, R. Buyya, and H. Kim, "Securing cloud-based Internet of Things: Challenges and mitigations," *Sensors*, vol. 25, no. 1, pp. 1–45, 2024, doi: 10.3390/s25010079.

[33] B. Bera *et al.*, "BioKA-ASVN: Biometric-based key agreement scheme for air smart vehicular networks using blockchain service," *IEEE Trans. Vehicular Technology*, vol. 73, pp. 9478–9494, 2024, doi: 10.1109/TVT.2024.3380392.

[34] S. Sumaidaa *et al.*, "Enhancing security of mobile crowd sensing in unmanned aerial vehicle ecosystems," *Frontiers in Communications and Networks*, vol. 6, pp. 1–21, 2025, doi: 10.3389/frcmn.2025.1443592.

[35] H. Shamshad *et al.*, "Forecasting and trading of stable cryptocurrencies with machine learning and deep learning algorithms," *IEEE Access*, vol. 11, pp. 122205–122220, 2023, doi: 10.1109/ACCESS.2023.3327440.

[36] R. Bar-Zur, A. Abu-Hanna, I. Eyal, and A. Tamar, "WeRLman: To tackle whale transactions using deep reinforcement learning," in *Proc. IEEE Symp. Security and Privacy (SP)*, San Francisco, CA, USA, May 21–25, 2023, pp. 93–110, doi: 10.1109/SP46215.2023.10179444.

[37] B. Yao *et al.*, "Optimal sharding for dynamic throughput optimization in blockchain systems with deep reinforcement learning," in *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC)*, Honolulu, HI, USA, Oct. 1–4, 2023, pp. 51–55, doi: 10.1109/SMC53992.2023.10394337.

[38] Y. Guo, Y. Wang, and Q. Qian, "Intelligent edge network routing architecture with blockchain for the IoT," *China Communications*, vol. 20, no. 11, pp. 151–163, 2023, doi: 10.23919/JCC.ea.2022-0006.202302.

[39] X. Wang *et al.*, "A privacy-enhanced multiarea task allocation strategy for healthcare 4.0," *IEEE Trans. Industrial Informatics*, vol. 19, no. 3, pp. 2740–2748, 2023, doi: 10.1109/TII.2022.3189439.

[40] S. Hafeez *et al.*, "Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach," *arXiv*, pp. 1–11, 2024, doi: 10.48550/arXiv.2403.04796.

[41] J. Li and J. Liu, "PointDMS: An improved deep learning neural network for large-scale point cloud segmentation in urban forestry," *Forests*, vol. 14, no. 11, pp. 1–25, 2023, doi: 10.3390/f14112169.

[42] R. Kothari, "Integration of blockchain and edge computing in healthcare: Accountability and collaboration," *Transdisciplinary J. Engineering and Science*, vol. 14, pp. 205–220, 2023, doi: 10.22545/2023/00230.

[43] P. Liu *et al.*, "A caching-enabled permissioned blockchain scheme for industrial IoT based on deep reinforcement learning," *Wireless Communications and Mobile Computing*, vol. 2023, Art. no. 2852085, pp. 1–16, 2023, doi: 10.1155/2023/2852085.

[44] A. Muminov, O. Sattarov, and D. Na, "Enhanced bitcoin price direction forecasting with DQN," *IEEE Access*, vol. 12, pp. 29093–29112, 2024, doi: 10.1109/ACCESS.2024.3367719.

[45] A. Kumari *et al.*, "Multi-agent-based decentralized residential energy management using deep reinforcement learning," *Journal of Building Engineering*, vol. 87, Art. no. 109031, 2024, doi: 10.1016/j.jobe.2024.109031.

[46] A. Mishra *et al.*, "A novel resource management framework for blockchain-based federated learning in IoT networks," *IEEE Trans. Sustainable Computing*, vol. 9, no. 4, pp. 648–660, 2024, doi: 10.1109/TSUSC.2024.3358915.

[47] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, "Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning," *J. Network and Computer Applications*, vol. 224, Art. no. 103834, 2024, doi: 10.1016/j.jnca.2024.103834.

[48] K. Moghaddasi, S. Rajabi, and F. S. Gharehchopogh, "Multi-objective secure task offloading for blockchain-enabled IoV-MEC systems using double deep Q-network," *IEEE Access*, vol. 12, pp. 3437–3463, 2024, doi: 10.1109/ACCESS.2023.3348513.

[49] A. Heidari *et al.*, "A green, secure, and deep intelligent method for dynamic IoT-edge-cloud offloading," *Sustainable Computing: Informatics and Systems*, vol. 38, Art. no. 100859, 2023, doi: 10.1016/j.suscom.2023.100859.

[50] W. Li, M. Yang, B. Xi, and Q. Huang, "Framework of virtual plantation forest modeling and data analysis for digital twin," *Forests*, vol. 14, no. 4, pp. 1–18, 2023, doi: 10.3390/f14040683.

[51] K. Qiu *et al.*, "DeepSIG: A hybrid heterogeneous deep learning framework for radio signal classification," *IEEE Trans. Wireless Communications*, vol. 23, no. 1, pp. 775–788, 2024, doi: 10.1109/TWC.2023.3281896.

[52] V. Ogrean and R. Brad, "Deep reinforcement learning architectures for automatic organ segmentation," *Biomedical Signal Processing and Control*, vol. 90, Art. no. 105919, 2024, doi: 10.1016/j.bspc.2023.105919.

[53] M. Qi *et al.*, "Species identification through deep learning and geometrical morphology in oaks (Quercus spp.): Pros and cons," *Ecology and Evolution*, vol. 14, no. 2, Art. no. e11032, 2024, doi: 10.1002/ece3.11032.

[54] H. Wang *et al.*, "Investigating the properties of neural network representations in reinforcement learning," *Artificial Intelligence*, vol. 330, Art. no. 104100, 2024, doi: 10.1016/j.artint.2024.104100.

[55] Y. H. B. A. Nugroho, F. Christian, and S. Sardjiyo, "The effect of application of E-SKP and competency assessment systems on performance with work discipline as an intervening variable," *Technium Social Sciences Journal*, vol. 40, no. 1, pp. 258–270, 2023, doi: 10.47577/tssj.v40i1.8363.

[56] R. Fernandez-Fernandez, J. G. Victores, and C. Balaguer, "Deep robot sketching: An application of deep Q-learning networks for human-like sketching," *Cognitive Systems Research*, vol. 81, pp. 57–63, 2023, doi: 10.1016/j.cogsys.2023.05.004.

[57] Q. Han *et al.*, "Retrospective-based deep Q-learning method for autonomous pathfinding in three-dimensional curved surface terrain," *Applied Sciences*, vol. 13, no. 10, pp. 1–19, 2023, doi: 10.3390/app13106030.

[58] S. Almutairi *et al.*, "Breast cancer classification using deep Q-learning and gorilla troops optimization," *Applied Soft Computing*, vol. 142, Art. no. 110292, 2023, doi: 10.1016/j.asoc.2023.110292.

[59] A. Kopacz, L. Csató, and C. Chira, "Evaluating cooperative-competitive dynamics with deep Q-learning," *Neurocomputing*, vol. 550, Art. no. 126507, 2023, doi: 10.1016/j.neucom.2023.126507.

[60] N. Gholizadeh, N. Kazemi, and P. Musilek, "A comparative study of reinforcement learning algorithms for distribution network reconfiguration with deep Q-learning-based action sampling," *IEEE Access*, vol. 11, pp. 13714–13723, 2023, doi: 10.1109/ACCESS.2023.3243549.

[61] I. Tunc and M. T. Soylemez, "Fuzzy logic and deep Q-learning-based control for traffic lights," *Alexandria Engineering Journal*, vol. 67, pp. 343–359, 2023, doi: 10.1016/j.aej.2022.12.028.

[62] N. Nayyer *et al.*, "A framework for fraud detection in bitcoin transactions through ensemble stacking models in smart cities," *IEEE Access*, vol. 11, pp. 90916–90938, 2023, doi: 10.1109/ACCESS.2023.3308298.

[63] S. S. Ali, R. Kaur, and S. Khan, "Identification of innovative technology enablers and drone technology adoption determinants," *Operations Management Research*, vol. 16, no. 2, pp. 830–852, 2023, doi: 10.1007/s12063-023-00346-3.

[64] F. Terribile *et al.*, "The LANDSUPPORT geospatial decision support system vision: Tools for sustainability policies in land planning and management," *Land Degradation & Development*, vol. 35, no. 2, pp. 813–834, 2024, doi: 10.1002/ldr.4954.

[65] L. Chen and J. Lyu, "Reinforcement learning technology applied to innovative models of informatization in classroom teaching," *Applied Mathematics and Nonlinear Sciences*, vol. 9, no. 1, pp. 1–14, 2024, doi: 10.2478/amns.2023.2.00988.

[66] A. Vangala *et al.*, "Cloud-assisted security framework for drone-enabled offshore communications," in *Proc. IEEE INFOCOM Workshops*, Hoboken, NJ, USA, May 20, 2023, pp. 1–6, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225952.

[67] J. B. R. Rose *et al.*, "IoD-enabled swarm of drones for air space control," in *Internet of Drones*, 1st ed. Boca Raton, FL, USA: CRC Press, 2023, p. 22, doi: 10.1201/9781003252085-10.

[68] K. T. Lai *et al.*, "AI wings: An AIoT drone system for commanding ArduPilot UAVs," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2213–2224, 2023, doi: 10.1109/JSYST.2022.3189011.

[69] M. De Marchi, A. Diantini, and S. E. Pappalardo, *Drones and Geographical Information Technologies in Agroecology and Organic Farming*. Boca Raton, FL, USA: CRC Press, 2023, doi: 10.1201/9780429052842.

[70] A. Mukherjee *et al.*, "Dew as a service for intermittently connected internet of drone things," in *Internet of Things*, pp. 241–260, 2024, doi: 10.1007/978-981-99-4590-0_12.

[71] S. Aggarwal, N. Kumar, and M. S. Obaidat, "Blockchain-based secure data aggregation for Internet of Drones," *IEEE Network*, vol. 37, no. 2, pp. 180–187, 2023, doi: 10.1109/MNET.2022.3211764.

[72] M. Aloqaily *et al.*, "AI-enabled blockchain-assisted unmanned aerial vehicles for sustainable smart cities," *IEEE Network*, vol. 37, no. 1, pp. 148–155, 2023, doi: 10.1109/MNET.2022.3205276.

[73] H. B. Salameh *et al.*, "UAV-assisted blockchain-enabled intelligent transportation systems: Architecture and challenges," *IEEE Communications Magazine*, vol. 61, no. 2, pp. 50–56, 2023, doi: 10.1109/MCOM.001.2200357.

[74] S. K. Singh, A. Boukerche, and Y. Wu, "AI-powered blockchain for resilient and secure UAV communications," *IEEE Wireless Communications*, vol. 30, no. 1, pp. 76–83, 2023, doi: 10.1109/MWC.002.2200175.

[75] R. K. Singh *et al.*, "Secure and privacy-preserving data sharing for UAV networks using federated learning and blockchain," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7936–7948, 2023, doi: 10.1109/JIOT.2022.3226761.

[76] M. A. Ferrag *et al.*, "UAV-assisted blockchain-based crowd sensing: Architecture, challenges, and future directions," *IEEE Network*, vol. 37, no. 3, pp. 248–255, 2023, doi: 10.1109/MNET.2022.3223787.

[77] S. U. Khan *et al.*, "Trust management in UAV networks: A blockchain-based approach," *IEEE Access*, vol. 11, pp. 48712–48728, 2023, doi: 10.1109/ACCESS.2023.3268897.

[78] A. Al-Hourani *et al.*, "Airborne blockchain for aerial network security," *IEEE Communications Magazine*, vol. 61, no. 4, pp. 34–40, 2023, doi: 10.1109/MCOM.001.2200543.

[79] Y. Zhou *et al.*, "Deep reinforcement learning-based resource allocation for UAV-assisted mobile edge computing," *IEEE Trans. Mobile Computing*, vol. 23, no. 1, pp. 312–326, 2024, doi: 10.1109/TMC.2022.3229867.

[80] A. Mahmoud *et al.*, "Energy-efficient trajectory design for UAV-enabled IoT networks using deep reinforcement learning," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1685–1697, 2024, doi: 10.1109/JIOT.2023.3299148.

[81] J. Zhang *et al.*, "Secure task offloading in UAV-assisted MEC systems with blockchain and deep reinforcement learning," *IEEE Trans. Vehicular Technology*, vol. 73, no. 3, pp. 3561–3574, 2024, doi: 10.1109/TVT.2023.3321489.

[82] H. Liu *et al.*, "Joint trajectory and computation offloading optimization for UAV-assisted edge computing," *IEEE Trans. Wireless Communications*, vol. 23, no. 4, pp. 4212–4226, 2024, doi: 10.1109/TWC.2023.3314521.

[83] X. Chen *et al.*, "Federated reinforcement learning for UAV swarm intelligence," *IEEE Trans. Neural Networks and Learning Systems*, vol. 35, no. 6, pp. 8221–8234, 2024, doi: 10.1109/TNNLS.2023.3309841.

[84] Y. Li *et al.*, "Blockchain-empowered UAV swarms: Architecture, applications, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 1–33, 2024, doi: 10.1109/COMST.2023.3327215.

[85] M. R. Jabbar *et al.*, "Privacy-preserving data collection for UAV-enabled IoT networks," *IEEE Access*, vol. 12, pp. 14782–14796, 2024, doi: 10.1109/ACCESS.2024.3352218.

[86] A. Rehman *et al.*, "Secure UAV communication systems using blockchain and AI: A survey," *Computer Networks*, vol. 246, Art. no. 110429, 2024, doi: 10.1016/j.comnet.2024.110429.

[87] S. Alqahtani *et al.*, "Multi-UAV coordination using deep reinforcement learning for disaster response," *IEEE Access*, vol. 12, pp. 22511–22526, 2024, doi: 10.1109/ACCESS.2024.3360127.

[88] P. Wang *et al.*, "Blockchain-assisted secure UAV communication for smart grids," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 912–924, 2024, doi: 10.1109/TSG.2023.3318456.

[89] F. Al-Turjman *et al.*, "AI-driven blockchain-enabled UAV networks for beyond 5G communications," *IEEE Network*, vol. 38, no. 1, pp. 64–71, 2024, doi: 10.1109/MNET.2023.3332167.

[90] A. K. Bashir *et al.*, "Intelligent and secure UAV-assisted healthcare systems using blockchain and reinforcement learning," *IEEE Access*, vol. 12, pp. 40155–40169, 2024, doi: 10.1109/ACCESS.2024.3370142.

[91] Y. Sun *et al.*, "UAV-enabled secure data collection for smart cities using blockchain," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 6123–6136, 2024, doi: 10.1109/JIOT.2023.3332145.

[92] M. A. Khan *et al.*, "Deep reinforcement learning-based energy-efficient UAV communication networks," *IEEE Wireless Communications Letters*, vol. 13, no. 2, pp. 389–393, 2024, doi: 10.1109/LWC.2023.3339821.

[93] A. Alshamrani *et al.*, "Blockchain-assisted secure routing for UAV ad hoc networks," *Ad Hoc Networks*, vol. 152, Art. no. 103276, 2024, doi: 10.1016/j.adhoc.2023.103276.

[94] S. Verma and A. K. Singh, "AI-driven intrusion detection system for UAV networks," *Journal of Network and Computer Applications*, vol. 223, Art. no. 103826, 2024, doi: 10.1016/j.jnca.2024.103826.

[95] H. Zhang *et al.*, "Joint computation offloading and trajectory optimization for blockchain-enabled UAV edge networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 1, pp. 455–468, 2024, doi: 10.1109/TGCN.2023.3335647.

[96] R. Ahmad *et al.*, "Secure federated learning framework for UAV-assisted IoT networks," *IEEE Access*, vol. 12, pp. 58214–58229, 2024, doi: 10.1109/ACCESS.2024.3378214.

[97] M. Elhoseny *et al.*, "Lightweight blockchain for real-time UAV communication systems," *Future Generation Computer Systems*, vol. 150, pp. 623–635, 2024, doi: 10.1016/j.future.2023.10.041.

[98] S. Raza *et al.*, "Privacy-aware UAV swarm coordination using deep reinforcement learning," *IEEE Systems Journal*, vol. 18, no. 2, pp. 2145–2156, 2024, doi: 10.1109/JSYST.2023.3342156.

[99] T. Nguyen *et al.*, "Blockchain-based authentication for UAV networks in smart environments," *Computer Communications*, vol. 213, pp. 180–192, 2024, doi: 10.1016/j.comcom.2023.10.012.

[100] A. Mahmood *et al.*, "Deep learning-enabled anomaly detection for UAV communication security," *Security and Communication Networks*, vol. 2024, Art. no. 8845123, pp. 1–15, 2024, doi: 10.1155/2024/8845123.

[101] F. Jameel *et al.*, "Blockchain and reinforcement learning for secure UAV-enabled mobile edge computing," *IEEE Communications Letters*, vol. 28, no. 1, pp. 102–106, 2024, doi: 10.1109/LCOMM.2023.3337452.

[102] Y. Ali *et al.*, "Trust-aware routing for UAV networks using blockchain technology," *Wireless Networks*, vol. 30, pp. 2149–2163, 2024, doi: 10.1007/s11276-023-03341-9.

[103] A. S. Alqahtani *et al.*, "Secure UAV swarm communications using hybrid AI and blockchain," *IEEE Access*, vol. 12, pp. 73115–73130, 2024, doi: 10.1109/ACCESS.2024.3381129.

[104] M. B. Hasan *et al.*, "A comprehensive survey on blockchain-enabled UAV networks," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 1021–1054, 2024, doi: 10.1109/COMST.2024.3379451.