Volume 10, Issue 1, January – 2025 *International Journal of Innovative Science and Research Technology (IJISRT)*
ISSN No:-2456-2165 *https://doi.org/10.5281/zenodo.14724977*
IJISRT25JAN755 *www.ijisrt.com*

Intelligent Drone Systems for Confidential Data Gathering

Pranav Shivanand Patil[1]; Prasanna Prasad Shenoy[2]; Pavan YDG[3]; Prajwal Prakash Shetti[4]; Sai Gagan Sirigeri[5]; Shobha T[6]

[1,2,3,4,5,6] Department of Information Science and Engineering, B.M.S College of Engineering, Bengaluru, India

Publication Date: 2025/01/24

Abstract

Artificial Intelligence integrated into Unmanned Aerial Vehicles has transformed data collection for a better cause in ensuring enhanced security, operation efficiency, and accuracy. Based on the literature available, the paper goes ahead to describe recent advances in the quest toward secure and autonomous acquisition techniques making use of drones by underlining state-of-the-art approaches: AI-based decision-making processes, real-time threat detection, and multi-layered encryption protocols. The proposed framework has incorporated the advanced model of machine learning, enabling the drones to navigate through difficult terrains and respond dynamically to environmental changes independently. It has enhanced the security and integrity of the data. Due to AI-driven algorithms, the system will be able to continuously monitor and respond to a possible threat. Real-time anomaly detection thus enables any cyberattack and unauthorized access to the data. Secure encryption and communication channels even further enhance this in high-risk or remote environments, disaster locations, and even zones of conflict. In all such scenarios, critical functions like safe surveillance, mapping, and gathering could be conducted without risking lives when the works are undertaken through UAVs. Integration with blockchain enhances the level of integrity of the information and its traceability with a unique permanent ledger to record data throughout, from creation until delivery. The capability for data verification and auditing in this blockchain component will, therefore, be very important for sectors dealing in sensitive or regulated information. By integrating machine learning into the tamper-proof record-keeping capability of blockchain, the system identifies any unauthorized access or tampering at any stage of operation and thus assures integrity in end-to-end data management. Versatile in their nature, their applications span diversified fields: environmental monitoring, emergency response, border security, where the secure, precise handling of data is essential. These would include industrial areas where drones are able to view hazardous areas like oil spills to offer a much safer and efficient alternative than human intervention could. This paper also considers emerging trends and possible applications that underline how continued technological advancements keep further extending the scope for AI-enabled secure UAV operations both in the public and private sectors.

Keywords:- *Secured Data Collection, Encryption, Machine Learning, Blockchain, Autonomous UAV.*

I. INTRODUCTION

Drones, or unmanned airborne vehicles (UAVs), have quickly advanced past their beginning military and recreational employments to gotten to be crucial instruments over businesses like calamity alleviation, foundation assessment, farming, and open wellbeing. A striking illustration is the 2019 ramble transport of a kidney in Baltimore, displaying UAVs' transformative potential in restorative coordinations and commercial applications. The worldwide commercial ramble showcase, anticipated to reach USD 35 billion by 2026, highlights their growing part in financial and innovative headways [2].

Advances in lightweight materials, such as carbon-fiber composites, and modern onboard innovations, counting GPS and remote communication, have improved drones' productivity and integration into the Web of Things (IoT). This movement has given rise to the Web of Rambles (IoD), a organized system empowering UAV collaboration in airspace zones overseen by Zone Benefit Suppliers (ZSPs). Whereas IoD encourages real-time checking and adaptable arrangements, it moreover raises noteworthy security

Pranav Shivanand Patil; Prasanna Prasad Shenoy; Pavan YDG; Prajwal Prakash Shetti; Sai Gagan Sirigeri; Shobha T, (2025), Intelligent Drone Systems for Confidential Data Gathering. *International Journal of Innovative Science and Research Technology*, 10(1), 731-736. https://doi.org/10.5281/zenodo.14724977

concerns, such as information capture attempts, spoofing, and framework vulnerabilities due to centralized designs [6,7].

Traditional cryptographic strategies are regularly illogical for UAVs due to their vitality and computational confinements. Tending to these challenges requires lightweight, decentralized security conventions custom-made to the IoD. This paper proposes a novel component that combines productive cryptographic conventions with decentralized capacity to improve information keenness and strength, approved through security investigation and execution testing [12].

The quick development of IoD moreover presents administrative and operational challenges. Guaranteeing secure and productive ramble operations requires coordination among partners, counting policymakers, flying specialists, and innovation suppliers. Creating standardized systems for airspace administration, communication conventions, and security compliance is basic to cultivating economical development in the IoD biological system. Rising advances like blockchain, AI, and progressed edge computing frameworks are central to empowering secure and independent operations in this advancing landscape.

Moreover, IoD applications are progressively joined with societal and natural contemplations. In agribusiness, IoD empowers accuracy cultivating hones, optimizing asset utilize and diminishing natural affect. Essentially, in urban situations, IoD-supported ramble systems offer arrangements for activity observing, contamination mapping, and quick crisis reaction. Be that as it may, tending to challenges related to security, moral utilize, and open acknowledgment is fundamental to opening the full potential of IoD advances in these domains.

Edge computing is progressively basic for IoD operations, empowering UAVs to prepare information locally or through adjacent edge hubs or maybe than depending on cloud framework. This approach diminishes idleness, bolsters real-time decision-making, and upgrades independence, making it imperative for time-sensitive applications like calamity reaction and reconnaissance. Edge computing moreover coordinating AI-driven analytics, empowering in-flight irregularity location, protest acknowledgment, and natural mapping [6,8].

II. LITERATURE REVIEW

A. Progressions in UAV Information Collection

The Unmanned Ethereal Vehicles have revolutionized the collection of data over changed spaces, wedding progressed AI with security propels to overhaul their viability and faithful unwavering quality. Afterward, this advanced significantly in enhancing the capacity for autonomous operation by UAVs, real-time handling of data, and adaptation to dynamic circumstances. Major progresses have included:

- AI-driven choice making: Through AI models, UAVs would be able to decide their flight pathing and task prioritization or adapt to diverse environmental changes for improved operational efficiency.
- Real-time risk detection: Allowing the UAVs to detect anomalies and respond to threats using machine learning techniques, such as in cases of signal interference or even physical tampering.
- Information Security through Blockchain: Blockchain ensures that data transmission is secure and tamper-proof. It subsequently addresses the issue of data authenticity and integrity [?].

B. Challenges in AI-Driven UAV Systems

Although some enhancements have been carried out, the nature of their autonomous operation, coupled with the difference in operational contexts, complicates securing the AI-powered UAV systems. Certain of the problems likely to emanate include:

- Cybersecurity Risks: The tendency of GPS to spoof signals, stick signals, or simply a hack introduces other vulnerable possibilities in tampering with the information and the missions of UAVs.
- Asset Limitations: Low battery life and limited computational power make the execution of robust security mechanisms such as encryption and real-time monitoring nearly impossible.
- Information Security: Most frequently, the utilization of UAVs deals with sensitive zones; consequently, unauthorized access and misuse of information gathered from such flying objects is always a concern.

C. Gaps in Current Research

While there is significant improvement in AI and security for UAVs, a number of gaps still exist with respect to the unique challenges of AI-driven information collection frameworks:

- Real-time Danger Detection: Among several other emerging UAV-specific threats, GPS spoofing and signal jamming cannot be addressed using traditional passive or signature-based methods. It has been identified that AI-driven models hold a greater potential for anomaly detection; however, further adaptation is required to handle high speeds in flight coupled with limited networking characteristics. Real-time risk detection capability will improve once UAV-specific dataset advancements and AI adaptation are achieved.

III. RELATED WORK

AI-driven approaches for securing unmanned aerial vehicles (UAVs) focus on risk discovery mechanization and protection against cyber threats. The remote communication channels of UAVs remain vulnerable to interference and tampering, requiring advanced security measures. While cryptographic techniques such as RSA and AES offer robust security, their resource-intensive nature makes them unsuitable for resource-constrained UAVs. As a result, lightweight cryptographic protocols tailored for such scenarios are widely recommended [26].

Moreover, the Internet of Drones (IoD) system has highlighted challenges such as limited data capacity, security

issues, and centralized control, prompting the adoption of blockchain technology to enable decentralized and tamper-resistant storage solutions, thereby ensuring enhanced data integrity and resilience. Blockchain-based security mechanisms have shown potential in improving UAV data security. For instance, a blockchain-based access control system using elliptic curve cryptography and the Ripple protocol consensus algorithm (RPCA) provides reliable mutual authentication but results in high computational costs. Another blockchain-based approach integrates deep learning for miner node selection, improving data reliability while facing challenges related to energy consumption in smart city applications [24].

Decentralized consensus protocols have been introduced to organize drones into geographical sub-groups, improving inter-group communication. However, such solutions remain vulnerable to physical attacks, where compromising a single drone could jeopardize the entire network. Further research explores UAV integration with 5G and blockchain, addressing challenges in securing cyber-physical systems. A proposed model uses drones as mobile network access points, leveraging blockchain to secure collected data against malicious tampering, while also enabling credit-based charging systems. Despite their promise, blockchain-based solutions often face trade-offs between security and performance [26].

To alleviate these issues, novel methods leveraging physical unclonable functions and chaotic cryptographic systems are being proposed, offering improved security and computational efficiency tailored to IoD scenarios. Machine learning approaches have significantly advanced UAV security algorithms. Techniques like isolation forests and one-class support vector machines (OC-SVM) are widely used for anomaly detection in UAV sensor data. These methods are efficient in outlier detection; thus, any potential threat or malfunction of a system may be detected much earlier than in other cases [22].

Further, other works have pointed to deep learning approaches, such as LSTM networks for real-time anomaly detection and CNNs in the case of image-based risk analysis. In later works, real-time address detection algorithms like YOLO are claimed to improve performance related to UAVs. Such models would then empower drones to perform real-time obstacle detection, detection of objects, and potential intrusions. Going forward, operational effectiveness in perception and security scenarios is bound to increase.

IV. SECURITY CHALLENGES OF DATA COLLECTION

A. Information Confidentiality

Data privacy is quintessential in rambles' operations for applications such as reconnaissance, environmental monitoring, and even military intelligence. Confidentiality ensures that unauthorized parties cannot access, view, or intercept data in collection either during transmission or storage. Still, rambles usually operate in uncontrolled environments, with data being forwarded over unsecured networks to be prone to interception. Critical data, for instance, in the form of video footage, environmental readings, etc., becomes exposed, whereby security breaches are a possibility or can lead to failed missions [1].

Traditional methods of encryption are effective in securing data, but they require high processing power and battery life, which is quite demanding for rambles. Development of lightweight cryptographic algorithms that can secure data in transit while minimizing resource utilization is in process. Dynamic AI-based encryption methods are emerging but need further testing. They change the level of encryption based on the sensitivity of the data and risk assessment [6].

Example: In urban monitoring, rambles employed for the analysis of traffic or crime can collect identifiable license plates or faces. If intercepted, this could facilitate unauthorized surveillance or criminal misuse; robust encryption protocols will be required [6].

B. Integrity and Authenticity Risks

Data integrity and authenticity are paramount in ensuring that the data collected by drones is accurate and reliable. Integrity ensures that data is not altered without authorization, while authenticity refers to the source of the data. In the absence of integrity and authenticity, malicious actors may intercept data and manipulate it to affect critical decisions [4].

AI-based tamper-detection technologies are able to provide solutions by detecting abnormal situations constantly. Some systems track every manipulation of information and immediately send it as an alarm to operators' screens. There is a constant need for advancements in the tamperdetection algorithms so that their response to regular variations in real data diminishes the number of false positives.

Example: Wildlife conservation involves rambles collecting data on the population of various species. Such alteration may result in distorted figures in terms of the population and would impact further conservation accordingly. AI-based tools increase the security by highlighting any suspicious modification.

C. Transmission and Storage Vulnerabilities

Drones rely on wireless channels such as Wi-Fi, LTE, and satellite links for data transmission. These make the drone prone to some cyber-attacks: eavesdropping, jamming, man-in-the-middle attack, which are more threatening when rambles operate over either public or remote networks with minimum security infrastructure. Local storage also presents certain risks, in that captured rambles will lead to unauthorized data extraction [14].

Stored data is encrypted with lightweight encryption techniques to maintain a proper balance between processing and storage constraints on drones. Artificial intelligence-based anomaly detection systems are under test, monitoring rambles on data access and flagging unauthorized attempts. [7].

Example: Rambles collect critical data on infrastructure damage and the location of survivors during disaster response. Cyberattacks on either channels of communication or storage could compromise such data and put communities in jeopardy. Adaptive firewalls and anomaly detection systems provide real-time defenses.

D. Access Control and Authorization

Access control mechanisms prevent unauthorized control of rambles and their data. Uncontrolled access can result in data theft, system tampering, or drone hijacking, especially in high-security applications like border monitoring and emergency zones. Biometric and behavioral authentication systems, including facial recognition and voice identification, powered by AI, improve access control. Real-time monitoring identifies unusual activities and initiates security protocols accordingly. Multi-layered approaches based on biometrics and adaptive AI monitoring show potential but need optimization against the resource limitations of drones [4].

Example: Rambles in military operations gather sensitive information about the movement of enemies. If unauthorized access is made, it might lead to compromising missions. AI-enabled access control limits data access to verified personnel, reducing the risk of leaks.

E. Threat Detection and Response

Drones face cyber threats like GPS spoofing, malware injections, and signal jamming, which can manipulate flight paths or disrupt data collection. AI-based threat detection tools are critical for identifying anomalies in telemetry data, flight paths, and communication patterns. These tools utilize machine learning to distinguish normal variations from potential attacks, enabling operators to take defensive actions. However, real-time detection remains challenging due to the computational limitations of drones, requiring optimized monitoring to maintain operational efficiency [12].

For example, drones on border patrol are vulnerable to GPS spoofing that redirects them to unauthorized areas. AI-powered systems can detect such anomalies, alert the control station, and initiate corrective measures. Advances in these systems enhance response times, allowing drones to adapt and counter cyber threats effectively.

V. METHODOLOGY

A. AI Techniques for Securing Data Collection

- Lightweight Encryption Methods: UAV systems require encryption techniques optimized for resource constraints. SIMON and ALW-AES are lightweight ciphers tailored to UAVs. SIMON offers robust security with minimal computational overhead, while ALW-AES modifies AES to reduce rounds, improving energy efficiency and speed without compromising security [14].

B. Machine Learning-Based Anomaly Detection

- Long Short-Term Memory (LSTM) Networks: LSTM networks analyze time-series data, detecting deviations in telemetry. Their ability to learn temporal dependencies helps address spoofing attacks and system malfunctions [9].
- Convolutional Neural Networks (CNNs): CNNs process UAV-captured images to detect threats like unauthorized objects. Their real-time analysis enhances surveillance by autonomously identifying security risks [6].

C. Deep Learning for Object Recognition and Data Validation

- YOLO for Real-Time Object Detection: The YOLO demonstrate is able to distinguish objects quick and precisely utilizing grid-based picture investigation, hence making the UAV framework effectively track an question amid the handle of reconnaissance.
- Autoencoders for Anomaly Detection: Autoencoders make compact representations from typical information and identify irregularities based on the reproduction mistake. This approach guarantees dependable information for UAVs indeed in complex, high-dimensional streams.

D. Tools and Frameworks

- TensorFlow and PyTorch: These are the most critical stages for the improvement and sending of machine learning models, counting CNNs and LSTMs. Their utilize of GPU increasing speed altogether moves forward preparing and sending proficiency.
- OpenCV: OpenCV gives picture preparing and successfully blends with models such as YOLO for superior question acknowledgment capabilities. This makes it exceptionally vital in the improvement of vision-based security highlights for UAV frameworks.

E. Specific Algorithms for Security and Data Processing

- Henon Map for Encryption: The Henon outline applies chaos hypothesis to produce unusual keys for encryption. This will make strides the security of data, especially beneath exceptionally unfavorable or unfriendly conditions.
- Isolation Forest (iForest): Isolation Forest's real-time anomaly detection capabilities ensure UAV operational safety by identifying potential threats or failures [24].

VI. CASE STUDIES ON AI IN UAV APPLICATIONS

A. Case study 1: AI in Surveillance Drones

Surveillance rambles improve security by covering huge regions and conveying real-time information. AI handles challenges such as information protection amid capacity and transmission. Machine learning models empower peculiarity discovery, hail unauthorized get to, and scramble touchy records. Versatile encryption guarantees basic information, like film from high-risk zones, gets more grounded protection[12].

- Impact and Challenges: AI decreases human mediation, quickens risk location, and improves open security. In any case, computational requests for real-time encryption and preparation require optimized models. Straightforward

information approaches offer assistance addressing security concerns.

- Example: A 2020 ponder by Wu et al. illustrated AI's viability in moving forward question discovery, which empowered speedier wrongdoing avoidance and secured delicate video bolsters from cyberattacks.

B. Case study 2: AI for Natural Monitoring

AI-equipped rambles collect natural information, counting discussion and water quality, deforestation rates, and species checking, while minimizing environmental disturbance. Real-time sifting and energetic encryption optimize information transmission, adjusting security with vitality efficiency[6].

- Impact and Challenges: Environmental rambles secure huge datasets in inaccessible ranges. Key challenges incorporate keeping up information security in the midst of arrange limitations and overseeing scrambled information without exhausting battery life.

- Example: A 2021 think tank by Singh et al. showcased AI-powered rambles observing deforestation in the Amazon. Scrambled pictures of imperiled species avoided information abuse, helping preservation efforts.

C. Case study 3: Military and Defense Applications

AI-driven military rambles perform insights, reconnaissance, and surveillance (ISR) operations, guaranteeing mission security with real-time encryption, counting quantum-safe strategies. These capabilities secure classified information from interception[21].

- Impact and Challenges: AI improves ISR proficiency whereas guaranteeing mission-critical information remains secure. In any case, actualizing progressed encryption in resource-constrained rambles remains a challenge.

VII. CONCLUSION AND FUTURE WORK

This paper presents an in-depth examination of AI's part in making strides data security for ramble operations over ranges such as observation, natural observing, and defense. Through versatile encryption, energetic inconsistency discovery, and progressed danger evaluation models, AI has altogether fortified the capacity of rambles to safely collect, transmit, and oversee information in genuine time [25].

By empowering rambles to identify unauthorized get to endeavors and alter encryption levels agreeing to the affectability of the information, AI presents a proactive layer of security that meets the complex security requests of progressed ramble applications. One of the key discoveries of this ponder is the adequacy of AI-driven data security measures, especially in circumstances where routine information security apparatuses drop brief. Rambles prepared with AI can react independently to changing security dangers, keeping up information astuteness and anticipating unauthorized interferences endeavors. The flexibility of these AI arrangements moreover emphasizes their potential for broad selection over different divisions, where vigorous and secure information taking care of is critical [26].

❖ *Future Inquire about Directions*

- Optimizing Vitality Productivity and Control Management: Enhancing vitality proficiency is a basic center for future AI-driven rambles. The computational concentrated of AI algorithms—especially those for real-time encryption and profound peculiarity detection—places noteworthy strain on drones' restricted control supplies, frequently restricting operational timeframes. Future investigate can center on lightweight, low-power AI models optimized particularly for ramble equipment. Furthermore, progressions in vitality administration frameworks that utilize renewable vitality sources, such as sun based charging, might amplify drones' battery life, empowering longer and more complex missions without compromising information security [29].
- Refining Peculiarity Discovery for Complex Threats: While current peculiarity discovery models successfully distinguish standard cyber dangers, foes are ceaselessly creating progressed techniques to breach frameworks. Future AI inquire about ought to, hence, prioritize more versatile and self-learning inconsistency location models, able of distinguishing indeed inconspicuous and developing dangers in genuine time. By refining the machine learning calculations utilized for inconsistency location, analysts can upgrade drones' flexibility against cyberattacks, such as sticking or spoofing endeavors, which are especially predominant in delicate zones like military and defense. Furthermore, consolidating components of ill-disposed machine learning may offer assistance fortify these models against assaults that look for to control or misdirect AI systems [30].
- Blockchain Integration for Information Transparency: Blockchain innovation offers a promising road for upgrading information judgment and straightforwardness in ramble operations. Blockchain's tamper-proof record capabilities can serve as a supplementary integration for applications where information realness and traceability are fundamental, such as law authorization, border security, and natural observing. Blockchain innovation, be that as it may, can be resource-intensive, so future inquire about ought to investigate strategies to streamline blockchain forms for compatibility with the vitality limitations of AI-powered rambles [31].

REFERENCES

[1]. C. Feng, K. Yu, A. Bashir, Y. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," *IEEE Network*, vol. 35, no. 1, pp. 130–137, 2021.

[2]. J. Pozner, "A Comprehensive List of Commercial Drone Use Cases," 2020. [Online]. Available: https://www.dronegenuity.com/commercial-drone-use-cases-comprehensive-list.

[3]. A. Lemert, M. Meyer, R. Mills, J. Paine, and A. Wong, "Drone Policy Overview," *Purdue Policy Research Institute Policy Briefs*, vol. 4, no. 1, p. 5, 2018.
[4]. C. Pu, A. Wall, K. Choo, I. Ahmed, and S. Lim, "A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment," *IEEE Internet of Things Journal*, pp. 1–1, 2022.
[5]. A. Gameros, "The Use of Composite Materials in Unmanned Aerial Vehicles," [Online]. Available: https://www.azom.com/article.aspx?ArticleID=12234.
[6]. S. Zaidi, M. Atiquzzaman, and C. Calafate, "Internet of Flying Things (IoFT): A Survey," *Computer Communications*, vol. 165, pp. 53–74, 2021.
[7]. C. Pu and L. Carpenter, "Psched: A Priority-Based Service Scheduling Scheme for the Internet of Drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4230–4239, 2021.
[8]. C. Pu and P. Zhu, "Defending against Flooding Attacks in the Internet of Drones Environment," in *Proc. IEEE GLOBECOM*, 2021, pp. 1–6.
[9]. J. Zhang and Y. Zhang, "A Method for UAV Reconnaissance and Surveillance in Complex Environments," in *Proc. IEEE ICCAR*, 2020, pp. 482–485.
[10]. C. Pu and P. Zhu, "Mitigating Routing Misbehavior in the Internet of Drones Environment," in *Proc. IEEE VTC2022-Spring*, 2022, pp. 1–6.
[11]. C. Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System," in *Proc. IEEE LANMAN*, 2020, pp. 1–6.
[12]. J. Yaacoub and O. Salman, "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.
[13]. W. Stallings, *Cryptography and Network Security - Principles and Practices*, 8th Edition. Pearson, 2020.
[14]. M. Ozmen and A. Yavuz, "Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones," in *Proc. IEEE MILCOM*, 2018, pp. 1–6.
[15]. Y. Li and C. Pu, "Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack," in *Proc. IEEE CSE*, 2020, pp. 92–97.
[16]. C. Li, L. Guan, J. Lin, B. Luo, Q. Cai, J. Jing, and J. Wang, "Mimosa: Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1196–1213, 2021.
[17]. Automated Validation of Internet Security Protocols and Applications. [Online]. Available: http://www.avispa-project.org/.
[18]. The Scyther Tool. [Online]. Available: https://people.cispa.io/cas.cremers/scyther/ index.html.
[19]. Laptop Computers. [Online]. Available: https://www.hp.com/us-en/shop/cat/laptops.
[20]. Latte Panda. [Online]. Available: https://www.lattepanda.com/.
[21]. S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A New Secure Data Dissemination Model in Internet of Drones," in *Proc. IEEE ICC*, 2019, pp. 1–6.
[22]. B. Bera, D. Chattaraj, and A. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Computer Communications*, vol. 153, pp. 229– 249, 2020.
[23]. D. Schwartz, N. Youngs, A. Britto et al., "The Ripple Protocol Consensus Algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151, 2014.
[24]. M. Singh, G. Aujla, and R. Bali, "A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4404–4413, 2021.
[25]. D. Wang, L. Yuan, L. Pang, Q. Xu, and Y. He, "Age of Information-Inspired Data Collection and Secure Upload Assisted by the Unmanned Aerial Vehicle and Reconfigurable Intelligent Surface in Maritime Wireless Sensor Networks," *Journal/Conference Name*, vol. XX, no. YY, pp. ZZ–ZZ, Year.
[26]. C. Pu, A. Wall, I. Ahmed, and K.-K. R. Choo, "SecureIoD: A Secure Data Collection and Storage Mechanism for Internet of Drones," in *Proceedings of the 23rd IEEE International Conference on Mobile Data Management (MDM)*, 2022.
[27]. X. Xu, H. Zhao, H. Yao, and S. Wang, "A Blockchain-enabled Energy Efficient Data Collection System for UAV-assisted IoT," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2431–2443, 2021.
[28]. P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518–538, 2020.
[29]. G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight Mutual Authentication Protocol for V2G Using Physical Unclonable Function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020.
[30]. M. Henon, "A Two-Dimensional Mapping with A Strange Attractor," Springer, 1976.
[31]. B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.
[32]. Dronebuster, accessed on: June 07, 2020. [Online]. Available: http://flexforce.us/ product/dronebuster/.