CNN-LSTM-Based Obstacle Detection Framework for Drone Technology using Blockchain Security

Abdullah Algashami[1]

[1]Department of Computer Science and Information
College of Science Zulfi, Majmaah University, Saudi Arabia

[1]a.algashami@mu.edu.sa

*Abstract***The integration of Artificial Intelligence (AI) with drones has significantly advanced autonomous navigation and flight safety, specifically for real-time obstacle detection, which is essential for maneuvering through unfamiliar or dynamic environments. This study presents an intelligent drone-based obstacle detection system that combines Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks to enhance both spatial recognition and temporal awareness during flight. The proposed architecture consists of multiple stages, beginning with the drone capturing high-resolution aerial imagery in real time. These images are passed through a structured pipeline that includes data pre-processing, augmentation, and annotation. CNNs are employed to extract robust spatial features from each frame, while LSTMs are used to analyze the temporal sequences of these features, enabling the system to detect and anticipate obstacles based on movement patterns and environmental context over time. To ensure data integrity and security in scenarios involving multiple drones, the system integrates blockchain technology. The proposed approach constructs a decentralized, content-addressable storage framework that ensures tamper-proof logging of mission-critical data and model updates. Experimental evaluations validate the effectiveness of the approach, demonstrating high accuracy in real-time obstacle detection, reduced false positive rates, and improved operational safety for autonomous drone missions across diverse terrains.**

Index Terms **Drone Blockchain Security Artificial Intelligence**

I. Introduction

Recent developments in drone technology have led to notable applications in domains such as precision agriculture, environmental monitoring, and emergency response [1] [2] [3] [4]. Despite widespread adoption, autonomous drones continue to encounter limitations in real-time, high-precision obstacle detection and localization [5]. This capability is critical for effective navigation in dynamic and unstructured environments, where undetected obstacles can result in mission failure or safety hazards [6]. Conspicuously, an enhanced AI-based obstacle detection framework is presented in the current study. The system integrates Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to support spatial and temporal analysis of sequential aerial data [7]. CNNs are applied to extract visual features from high-resolution drone imagery, while LSTM networks process the temporal evolution of these features to improve the prediction and detection of both static and dynamic obstacles. To address data integrity and security requirements in multi-drone operations, the framework incorporates blockchain-based components [8]. A combination of Distributed Hash Tables (DHTs) and the Interplanetary File System (IPFS) is used to establish a decentralized, tamper-resistant storage mechanism for obstacle detection logs and operational data. While existing literature has addressed secure communication and image analysis in UAV systems [9] [10], this work provides a comprehensive system architecture along with a formal mathematical model to support obstacle detection processes. The complete workflow—ranging from data acquisition and AI-driven analysis to blockchain-based validation—is designed to enhance reliability and operational robustness in real-world drone deployments [11] [12].

Key Research Contributions

Based on the aforementioned aspects, the specific contributions of the proposed approach are as follows;

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

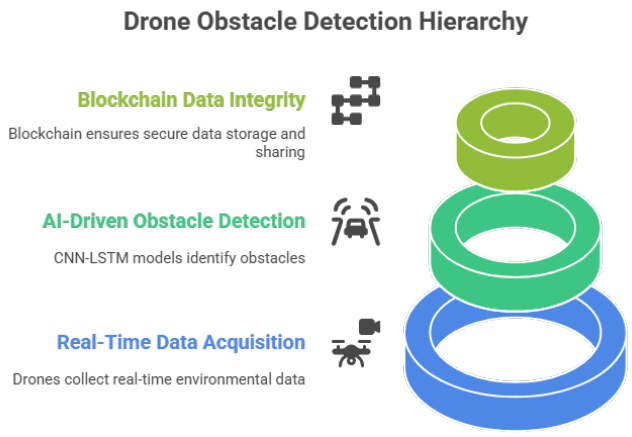

Fig. 1. Conceptual View of Proposed Approach

- **Drone-Based Multi-Layer Obstacle Detection Architecture:** A three-layer architecture is developed, comprising real-time data acquisition by drones, CNN-LSTM-based obstacle detection, and secure data transmission through blockchain protocols.
- **Spatio-Temporal AI Modeling:** Obstacle detection performance is improved using CNNs for spatial feature extraction and LSTM networks for modeling temporal dependencies, enabling the identification of both stationary and moving obstacles.
- **Blockchain-Enabled Data Integrity:** Blockchain technology is employed to support immutable, decentralized storage and sharing of obstacle detection data, ensuring trust and traceability in collaborative drone operations.

Figure 1 depicts the conceptual view of the proposed approach.

II. Problem Formulation

This work proposes a spatio-temporal object detection framework tailored for drone-based systems, integrating CNNs for spatial feature extraction and LSTM networks for temporal sequence modeling. Drones often operate in dynamic and complex environments, where object detection accuracy is challenged by factors such as varying illumination, environmental noise, and changing terrain structures. Thus, the detection model must deliver high accuracy while remaining computationally efficient and energy-conscious, suitable for deployment on embedded drone platforms. Let a sequence of images $\mathcal{X} = \{X_1, X_2, ..., X_T\}$, where each $X_t \in \mathbb{R}^{H \times W}$, be captured over time T by an onboard drone camera. The goal is to detect a corresponding sequence of object sets $\mathcal{Y}_t = \{y_{t1}, y_{t2}, ..., y_{tm}\}$, with each detection y_{tj} paired with a predicted class probability q_{tj}, indicating object classification across time.

A. Objective Function

The total objective loss $\mathcal{J}_{\text{total}}$ comprises localization, classification, and regularization components:

$$\mathcal{J}_{\text{total}} = \sum_{t=1}^{T}\sum_{j=1}^{m} \mathcal{J}_{\text{loc}}(y_{tj}, \tilde{y}_{tj}) + \mu \sum_{t=1}^{T}\sum_{j=1}^{m} \mathcal{J}_{\text{cls}}(q_{tj}, \tilde{q}_{tj}) + \gamma \mathcal{J}_{\text{reg}}$$

Where:

- $\mathcal{J}_{\text{loc}}$: Localization loss measuring geometric deviation between predicted and ground-truth bounding boxes.
- $\mathcal{J}_{\text{cls}}$: Classification loss penalizing incorrect predictions of object categories.
- $\mathcal{J}_{\text{reg}}$: Regularization term to control model complexity and prevent overfitting.
- μ, γ: Hyperparameters balancing the loss components.

a) Localization Loss:: The localization loss evaluates prediction overlap accuracy:

$$\mathcal{J}_{\text{loc}} = \frac{1}{T \cdot m} \sum_{t=1}^{T}\sum_{j=1}^{m} (1 - \text{IoU}(y_{tj}, \tilde{y}_{tj}))$$

This metric is vital for safe obstacle detection in drone navigation scenarios.

b) Classification Loss:: Cross-entropy loss is used to assess label prediction accuracy:

$$\mathcal{J}_{\text{cls}} = -\sum_{t=1}^{T}\sum_{j=1}^{m} \tilde{q}_{tj} \log(q_{tj})$$

where q_{tj} and $\tilde{q}_{tj}$ denote predicted and true class probabilities, respectively.

c) Regularization:: To reduce overfitting in CNN-LSTM layers, L2 regularization is applied:

$$\mathcal{J}_{\text{reg}} = \frac{\delta}{2} \|\phi\|^2$$

with ϕ representing model parameters and δ the regularization factor.

B. Operational Constraints

The CNN-LSTM-based detection model must meet the following drone deployment constraints:

1) **Real-time Inference:** Low-latency predictions for dynamic obstacle avoidance and trajectory adjustments.
2) **Edge Compatibility:** Lightweight architecture compatible with drone-embedded processors (e.g., Jetson Nano, Coral TPU).
3) **Environmental Robustness:** High generalization across lighting variations, occlusions, and weather.
4) **Energy Efficiency:** Optimal compute-to-power ratio to extend drone flight time.

In summary, the formulated CNN-LSTM-based detection system minimizes $\mathcal{J}_{\text{total}}$ under drone-specific operational constraints, offering accurate, temporally aware object detection for real-world autonomous drone missions.

III. Proposed System Model

The proposed architecture is a modular and multi-layered framework that facilitates real-time obstacle detection in drones by leveraging deep learning and blockchain technologies. It consists of three interdependent layers: the **Drone Data Collection Layer**, the **CNN-LSTM-Based Obstacle Detection Layer**, and the **Blockchain Security Layer**. Each layer performs a specialized role, contributing collectively to robust, secure, and high-precision obstacle identification in dynamic environments.

A. Drone Data Collection (DDC) Layer

The DDC Layer is responsible for acquiring time-sequenced visual data from aerial platforms. A network of drones equipped with high-resolution imaging sensors conducts autonomous or semi-autonomous missions. These drones follow predefined flight paths or dynamically adjust trajectories to capture detailed, real-time visual data across operational zones [13].

1) **Image Generation:** Each drone is equipped with multi-sensor payloads, including multispectral or hyperspectral cameras, thermal sensors, LiDAR, and HD video systems. These sensors collect spatial and spectral data across various bands (visible, infrared, thermal), recorded at fixed intervals to maintain continuity in the visual stream. This multi-sensor approach allows for rich environmental representation suitable for advanced analytics.
2) **Image Acquisition and Metadata Integration:** The collected images are transmitted over encrypted channels—using protocols such as AES—to ground control systems or edge computing nodes. Every image frame is tagged with contextual metadata such as GPS coordinates, altitude, timestamp, drone velocity, and orientation (pitch, roll, and yaw). This metadata supports context-aware processing essential for spatio-temporal modeling.

In this layer, drones operate as real-time aerial visual sensors. They generate and transmit continuous image sequences that serve as input to the subsequent deep learning layer. The structured nature of this data stream enables temporal correlation across frames, which is critical for the performance of CNN-LSTM models in detecting both static and dynamic obstacles.

B. CNN-LSTM-Based Obstacle Detection (CBOD) Layer

CBOD Layer serves as the core analytic module of the proposed drone system. It performs real-time obstacle identification by leveraging deep learning models that combine spatial feature extraction through CNNs and temporal sequence modeling using LSTM networks.

1) Theoretical Foundation: **CNNs** are specialized neural networks designed to automatically and adaptively learn spatial hierarchies of features through backpropagation using multiple building blocks such as convolution layers, pooling layers, and fully connected layers [14] [15]. Given an input image $I \in \mathbb{R}^{H\times W\times C}$, a CNN extracts a feature map $F \in \mathbb{R}^{H'\times W'\times D}$ through convolutional kernels:

$$F_{i,j,d} = \sigma\left(\sum_{m,n,c} I_{i+m,j+n,c}\cdot K_{m,n,c,d} + b_d\right)$$

where K is the convolution kernel, b_d is the bias term, and σ is the activation function (typically ReLU).
LSTM networks are a form of Recurrent Neural Networks (RNNs) capable of learning long-term dependencies [16] [17]. LSTM units mitigate the vanishing gradient problem through the use of gated structures. For a sequence of CNN features $\{F_1, F_2, ..., F_T\}$, LSTM computes hidden states h_t using the following update equations:

$$\begin{aligned}
f_t &= \sigma(W_f\cdot[h_{t-1}, F_t] + b_f)\\
i_t &= \sigma(W_i\cdot[h_{t-1}, F_t] + b_i)\\
o_t &= \sigma(W_o\cdot[h_{t-1}, F_t] + b_o)\\
\tilde{c}_t &= \tanh(W_c\cdot[h_{t-1}, F_t] + b_c)\\
c_t &= f_t\odot c_{t-1} + i_t\odot\tilde{c}_t\\
h_t &= o_t\odot\tanh(c_t)
\end{aligned}$$

where σ is the sigmoid activation, $\odot$ denotes element-wise multiplication, and W_*, b_* are learnable parameters.

2) Data Pipeline:

- **Preprocessing:** Raw images I_t are denoised, normalized, and resized:

$$I'_t = \text{Resize}(\text{CLAHE}(G_\sigma * I_t), H', W')$$

- **Augmentation:** Training data is augmented to improve generalization:

$$\tilde{I}_t = \mathcal{A}(I'_t) \quad \text{where } \mathcal{A} \in \{\text{flip, rotate, crop, mosaic, CutMix}\}$$

- **Annotation:** Each image is labeled with a set of bounding boxes and class labels:

$$\mathcal{Y}_t = \{(x_i, y_i, w_i, h_i, c_i)\}_{i=1}^{N_t}$$

3) CNN-LSTM Model Structure: The different components of the CNN-LSTM model are depicted ahead.
Feature Extraction:

$$F_t = \text{CNN}(\tilde{I}_t) \in \mathbb{R}^D$$

Temporal Modeling:

$$h_t = \text{LSTM}(F_1, F_2, ..., F_t)$$

Prediction:

$$\hat{Y}_t = \text{Dense}(h_t) = \{(\hat{x}_i, \hat{y}_i, \hat{w}_i, \hat{h}_i, \hat{c}_i, \hat{p}_i)\}_{i=1}^{\hat{N}_t}$$

4) Loss Function and Optimization: The training objective includes both localization and classification loss terms: **Localization Loss (Smooth L1):**

$$\mathcal{L}_{\text{loc}} = \sum_{i=1}^{N} \text{SmoothL1}(\hat{b}_i - b_i)$$

Classification Loss (Cross Entropy):

$$\mathcal{L}_{\text{cls}} = -\sum_{i=1}^{N} \sum_{j=1}^{|\mathcal{C}|} y_{ij} \log(\hat{y}_{ij})$$

Total Loss:

$$\mathcal{L}_{\text{total}} = \lambda_1 \mathcal{L}_{\text{loc}} + \lambda_2 \mathcal{L}_{\text{cls}}$$

Optimization algorithms such as SGD, Adam, or RMSprop are applied, with learning rate scheduling and early stopping for convergence control. Evaluation metrics include:

- Mean Average Precision (mAP)
- Intersection over Union (IoU)
- Precision-Recall (PR) curves

5) Detection Output and Reporting: Once inference is complete, the system outputs structured detection results per frame:

$$\text{Report}_t = \{\text{Class}, \text{Confidence}, (x, y, w, h), \text{IoU}, \text{Time}, \text{DroneID}\}$$

These reports include:

- Detected object classes with confidence levels
- Bounding boxes or segmentation masks
- Positional metadata and drone identifiers
- Statistical summaries (e.g., number of objects, average confidence, false positive/negative rates)

This layer forms the system's decision engine, converting raw visual inputs into actionable insights for drone navigation in cluttered, uncertain, or dynamic environments. The integration of CNN and LSTM provides spatio-temporal awareness crucial for real-time obstacle avoidance.

6) Functional Workflow: CBOD layer is deployed on high-performance computing (HPC) platforms such as GPUs, TPUs, or FPGA accelerators. It can operate in cloud environments or at the edge, offering low-latency processing suitable for real-time applications. The functional components of this layer are outlined as follows:

1) **Data Preprocessing**
   Raw images obtained from drone sensors are first preprocessed to enhance quality and consistency. Noise is suppressed using filters (e.g., Gaussian or median), and contrast or color normalization is performed. In cases involving multispectral data, spectral bands may be selectively fused to emphasize features critical for obstacle detection.
2) **Image Rescaling**
   Preprocessed images are resized to match the required input dimensions of the model (e.g., 300×300, 512×512, or 1024×1024 pixels). Rescaling is performed using interpolation techniques such as bilinear or bicubic methods to preserve essential spatial features.
3) **Data Augmentation**
   To improve model generalization and mitigate overfitting, a variety of augmentation techniques are applied. These include geometric transformations (cropping, rotation, flipping) and photometric adjustments (e.g., brightness control). Advanced augmentation strategies such as CutMix and Mosaic are also used to further diversify the training dataset.
4) **Image Annotation**
   Each image is labeled with relevant information, including bounding boxes, keypoints, or segmentation masks. This labeling process may be semi-supervised to manage large-scale datasets. Frameworks such as YOLO, SSD, and Mask R-CNN are employed to define obstacle classes and regions of interest.
5) **Model Training and Evaluation**
   The deep learning model, combining CNN for spatial feature extraction and LSTM for temporal sequence modeling, is trained using domain-specific aerial datasets. The training process utilizes the backpropagation algorithm and optimizers such as SGD, Adam, or RMSprop. Evaluation metrics, including mean Average Precision (mAP), Intersection over Union (IoU), and Precision-Recall (PR) curves, guide the tuning of hyperparameters. To avoid overfitting, regularization techniques like dropout, batch normalization, and early stopping are applied.
6) **Obstacle Detection Reports**
   After training and deployment, the system generates comprehensive detection reports. These include obstacle classification results, confidence scores, location coordinates, and optional visual representations (e.g., bounding boxes or segmentation overlays). Summary statistics such as object counts, average confidence levels, and false positive/negative rates are also presented in tabular form.

Figure 2 presents the functional workflow of the proposed CBOD layer.

C. Blockchain-Based Security (BBS) Layer

BBS Layer functions as the trust and integrity module of the proposed system, ensuring that all obstacle detection data remains immutable, verifiable, and securely accessible. By integrating decentralized ledger technologies, this layer facilitates secure transmission, accountability, and tamper-proof storage of detection reports across all participating entities.

1) System Architecture and Components:

- **User Access Control:** Multiple stakeholders interact with the blockchain layer, including drone operators, safety officers, data analysts, and regulatory bodies. Each participant is assigned a cryptographic

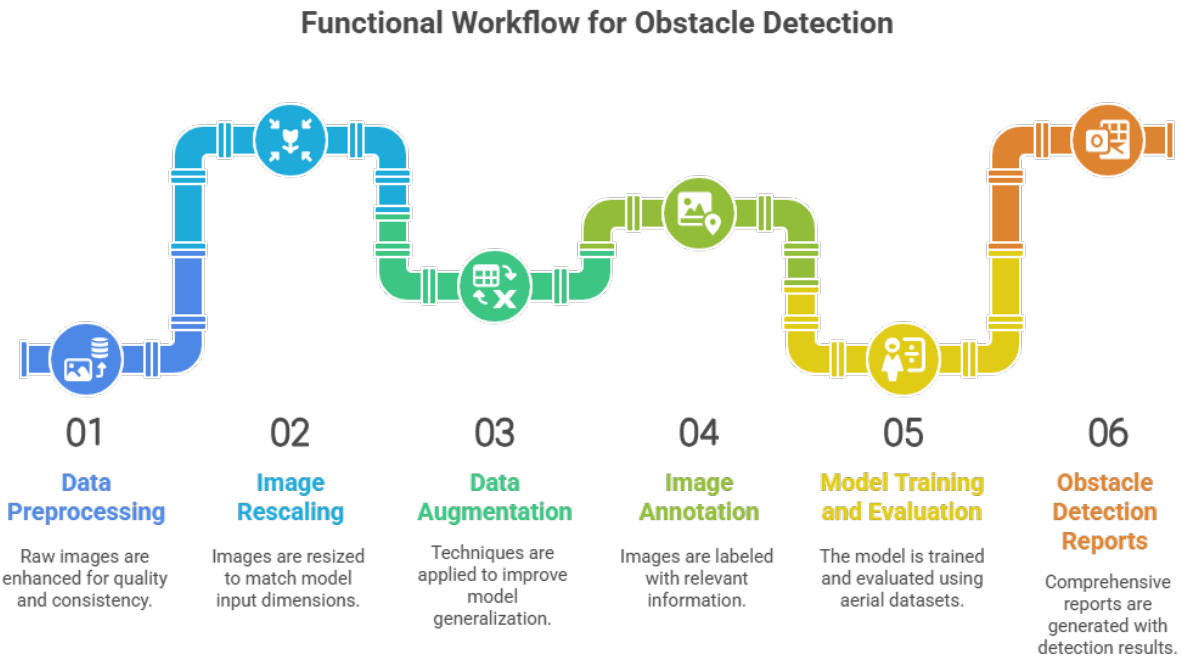

Fig. 2. CNN-LSTM Proposed Model: Functional Workflow

identity using a public-private key pair, enabling authentication and access control. Depending on predefined access roles, users may have read-only or write permissions within the blockchain network.

- **Blockchain Network Configuration :** The system may utilize either permissioned platforms, such as Hyperledger, or permissionless public chains like Ethereum. The choice depends on operational requirements regarding scalability, transparency, and governance.
- **Tamper-Proof Record Logging:** Obstacle detection outputs generated by the CNN-LSTM layer are hashed and recorded on the blockchain. Each report includes metadata such as a timestamp, the uploader's public key, and a pointer to the previous block. The hashed content ensures immutability and allows traceability of all stored events.
- **Distributed Hash Table (DHT):** Detection reports are indexed using a DHT mechanism. This peer-to-peer structure distributes storage across multiple nodes, eliminating single points of failure and enhancing resilience and redundancy.
- **InterPlanetary File System (IPFS) Integration:** The raw detection data, often large, is stored off-chain using IPFS. Only cryptographic hash pointers referencing IPFS nodes are recorded on the blockchain. This hybrid architecture combines IPFS's scalability with blockchain's immutability, enabling efficient access to large-scale data while maintaining robust security.

2) Security and Resilience Features: BBS safeguards system data through the following mechanisms:

1) **Immutability:** Once stored, data cannot be altered, ensuring trustworthy system logs.
2) **Accountability:** All system actions are traceable to user identities via digital signatures.
3) **Fault Tolerance:** Decentralized file distribution via IPFS and DHT mitigates risks from network failures.
4) **Scalability:** Off-chain storage of large files avoids blockchain bloat while retaining high availability.

BBS layer enforces cryptographic integrity and distributed access, forming the backbone of secure obstacle data management within the multi-drone ecosystem. The synergy of blockchain, DHT, and IPFS guarantees that all obstacle detection reports are verifiable, tamper-resistant, and consistently retrievable.

IV. Experimental Evaluation

This section presents the performance analysis of the proposed drone-based obstacle detection framework that integrates a CNN-LSTM architecture with blockchain-based security. Multiple experiments were conducted to validate the system's performance across three key dimensions: computational efficiency, detection accuracy, and security assurance.

A. Gas Consumption Efficiency

Figure 3 compares the gas consumption (in ETH) for storing obstacle detection events between the proposed

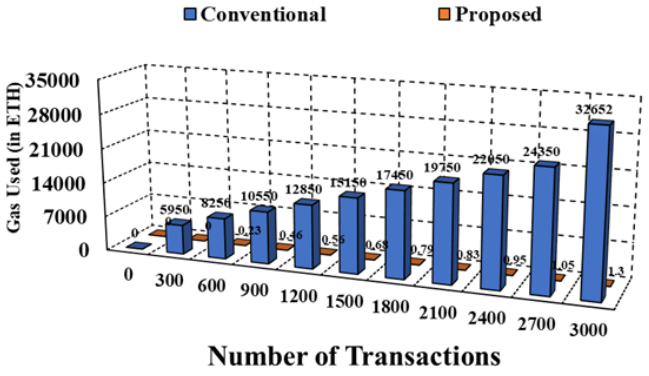

Fig. 3. Gas Consumption Efficiency

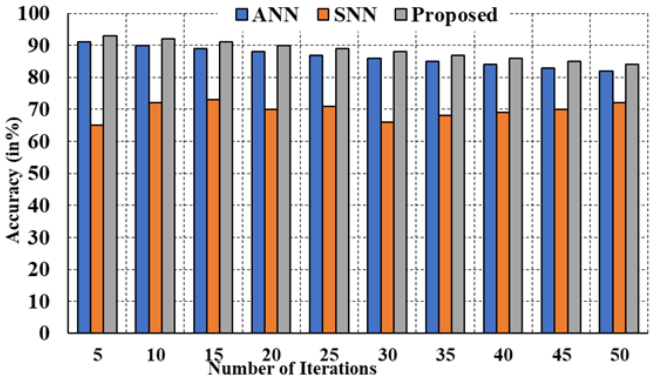

Fig. 4. Obstacle Detection Precision

blockchain-based storage mechanism and a conventional approach. The proposed system demonstrates superior scalability, incurring zero gas cost for up to 300 transactions and only 1.3 ETH at 3000 transactions. Conversely, the traditional model starts at 5950 ETH for 300 transactions and sharply increases to over 32,000 ETH at 3000 transactions. These findings confirm the cost-effectiveness of the method, particularly under high transaction volumes.

B. Obstacle Detection Precision Across Models

Figure 4 presents a comparative analysis of obstacle detection accuracy across training epochs for three neural network models: Artificial Neural Network (ANN), Spiking Neural Network (SNN), and the proposed CNN-LSTM-based architecture. The proposed model achieves a peak detection precision of 94.6% after 50 training epochs and maintains consistent performance throughout, demonstrating robust generalization across test scenarios. The ANN follows closely, stabilizing at around 91.2%, indicating reliable yet slightly inferior spatial-temporal modeling capacity. In contrast, the SNN shows significant variability, with accuracy fluctuating between 65% and 74%, and an average of 70.1%, underscoring its reduced effectiveness in high-speed UAV operations requiring real-time vision processing. These results confirm that the proposed CNN-LSTM framework offers superior obstacle recognition capabilities in dynamic aerial environments by efficiently capturing both spatial and sequential visual features, outperforming conventional ANN and SNN models in terms of precision.

C. Security Goal Performance Analysis

The proposed model is compared for the effectiveness of Blockchain, IPFS, and the proposed framework across six key security metrics: Data Integrity, Data Availability, Data Confidentiality, Data Privacy, System Availability, and Non-repudiation.

- **Blockchain** maintains uniform but limited security support across all goals, with an average of 2 nodes.
- **IPFS** shows moderate strength, especially in availability and integrity.
- **Proposed Framework** consistently outperforms both, achieving 6–8 nodes across metrics, peaking in data availability and maintaining superiority in all categories.

D. Stability Analysis

Beyond conventional accuracy metrics, assessing the **stability** of the proposed CNN-LSTM-based obstacle detection framework is essential to ensure operational reliability. Drones frequently operate under dynamic environmental conditions—such as fluctuating illumination, motion blur, or sensor noise—necessitating that the detection system remain robust to varying input characteristics. To quantify this robustness, the *Mean Absolute Shift (MAS)* metric is utilized. MAS measures the average deviation between the predicted and ground truth values under different operational settings, and is defined as:

$$\text{MAS} = \frac{1}{m}\sum_{j=1}^{m}|\hat{y}_j - y_j|$$

Where $\hat{y}_j$ denotes the predicted output (e.g., bounding box position or confidence score) and y_j is the corresponding ground truth value for the j^{th} frame. A **higher MAS value** indicates enhanced tolerance to input variability, reflecting superior system stability, whereas a **lower MAS value** implies increased sensitivity to real-time disturbances. Figure 5 illustrates the MAS values obtained from experimental trials across various UAV flight scenarios, including low-light, urban, and high-altitude conditions. The proposed CNN-LSTM architecture yielded an **average MAS of approximately 0.74**, with recorded values ranging from **0.52 to 0.79**. These findings confirm the system's capacity to deliver consistent outputs under dynamically shifting visual inputs. This observed stability is critical in real-time drone navigation and obstacle avoidance, where even minor misdetections may compromise safety or mission objectives. The high MAS values reinforce the CNN-LSTM

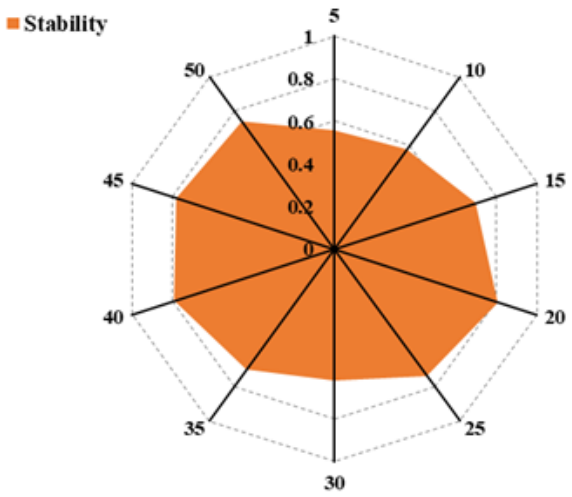

Fig. 5. Stability Analysis

model's effectiveness in maintaining detection reliability and continuity across diverse environmental conditions. In conclusion, the MAS-based evaluation complements conventional performance metrics, confirming that the proposed architecture is not only accurate but also robust and deployment-ready for real-time drone-based vision tasks in unpredictable environments.

V. Conclusion

This paper presents an AI-enhanced obstacle detection architecture that improves the operational reliability and efficiency of drones. The proposed system employs deep learning techniques of CNNs combined with LSTM networks to enable accurate and real-time identification of obstacles in complex and dynamic environments. This functionality supports timely navigation decisions and reduces the risk of collisions during autonomous flight missions. To ensure data integrity and secure communication, the architecture integrates blockchain technology. This addition enables decentralized, tamper-resistant logging and sharing of obstacle detection data among multiple UAVs. Such a framework is particularly effective in multi-agent systems used for applications like search and rescue, precision agriculture, and distributed surveillance, where consistent and verifiable data exchange is critical. The integration of deep learning for perception and blockchain for secure data management provides a scalable and robust foundation for advanced UAV systems. This architecture aligns with the principles of Industry 5.0 by promoting autonomy, security, and interoperability in drone deployments across various industrial domains.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Competing Interests

The authors declare no conflict of interest in this area.

Declaration of Generative AI and AI-assisted technologies

During the preparation of this work, the author(s) used Monica.AI in order to improve English Quality and Grammarly to correct grammatical mistakes. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

[1] R. Guebsi, S. Mami, and K. Chokmani, "Drones in precision agriculture: A comprehensive review of applications, technologies, and challenges," *Drones*, vol. 8, no. 11, p. 686, 2024.

[2] M. Aarif KO, A. Alam, and Y. Hotak, "Smart sensor technologies shaping the future of precision agriculture: Recent advances and future outlooks," *Journal of Sensors*, vol. 2025, no. 1, p. 2460098, 2025.

[3] L. A. Shakir, S. Kurnaz, and A. Alkhayyat, "Improve thermal sensing drones for emergency response: A comprehensive control system approach," *Arabian Journal for Science and Engineering*, pp. 1–25, 2025.

[4] J. Akram, W. Hussain, R. H. Jhaveri, R. S. Rathore, and A. Anaissi, "Dynamic gnn-based multimodal anomaly detection for spatial crowdsourcing drone services," *Digital Communications and Networks*, 2025.

[5] M. R. Rezaee, N. A. W. A. Hamid, M. Hussin, and Z. A. Zukarnain, "Comprehensive review of drones collision avoidance schemes: Challenges and open issues," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 7, pp. 6397–6426, 2024.

[6] A. S. Alamoush and A. I. Ölçer, "Maritime autonomous surface ships: Architecture for autonomous navigation systems.," *Journal of Marine Science & Engineering*, vol. 13, no. 1, 2025.

[7] Z. Guo, D. Cai, Z. Jin, T. Xu, and F. Yu, "Research on unmanned aerial vehicle (uav) rice field weed sensing image segmentation method based on cnn-transformer," *Computers and Electronics in Agriculture*, vol. 229, p. 109719, 2025.

[8] K. A. Tychola, K. Voulgaridis, and T. Lagkas, "Beyond flight: Enhancing the internet of drones with blockchain technologies," *Drones*, vol. 8, no. 6, p. 219, 2024.

[9] F. Wan, M. B. Yaseen, M. B. Riaz, A. Shafiq, A. Thakur, and M. O. Rahman, "Advancements and challenges in uav-based communication networks: A comprehensive scholarly analysis," *Results in Engineering*, vol. 24, p. 103271, 2024.

[10] O. Ceviz, S. Sen, and P. Sadioglu, "A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions," *IEEE Communications Surveys & Tutorials*, 2024.

[11] A. Jain, S. Barke, M. Garg, A. Gupta, B. Narwal, A. K. Mohapatra, D. K. Sharma, and G. Srivastava, "A walkthrough of blockchain-based internet of drones architectures," *IEEE Internet of Things Journal*, 2024.

[12] R. Aldossri, A. Aljughaiman, and A. Albuali, "Advancing drone operations through lightweight blockchain and fog computing integration: A systematic review," *Drones*, vol. 8, no. 4, p. 153, 2024.

[13] G. Bhat, M. Dudhedia, R. Panchal, Y. Shirke, N. Angane, S. Khonde, S. Khedkar, J. Pansare, S. Bere, R. Wahul, *et al.*, "Autonomous drones and their influence on standardization of rules and regulations for operating–a brief overview," *Results in Control and Optimization*, vol. 14, p. 100401, 2024.

[14] L. Li, M. Xu, S. Chen, and B. Mu, "An adaptive feature fusion framework of cnn and gnn for histopathology images classification," *Computers and Electrical Engineering*, vol. 123, p. 110186, 2025.

[15] I. D. Mienye and T. G. Swart, "Deep autoencoder neural networks: A comprehensive review and new perspectives," *Archives of computational methods in engineering*, pp. 1–20, 2025.

[16] I. D. Mienye, T. G. Swart, and G. Obaido, "Recurrent neural networks: A comprehensive review of architectures, variants, and applications," *Information*, vol. 15, no. 9, p. 517, 2024.

[17] A. Barjasteh, S. H. Ghafouri, and M. Hashemi, "A hybrid model based on discrete wavelet transform (dwt) and bidirectional recurrent neural networks for wind speed prediction," *Engineering Applications of Artificial Intelligence*, vol. 127, p. 107340, 2024.