

REAL-TIME FINANCIAL FRAUD DETECTION SYSTEM USING AI, BLOCKCHAIN, AND CYBERSECURITY

Mr. J. Srikanth¹, Kisshore.M², Pranavanathan³,

Pawan Sai⁴

1.Senior Assistant Professor, Department of Computer Science & Engineering, Christ College of Engineering & Technology, Puducherry, India.

2,3,4 - Final Year Students, Department of Computer Science & Engineering, Christ College of Engineering & Technology, Puducherry, India.

Abstract

Financial fraud detection has become an essential component of modern digital banking systems due to the rapid growth of online and real-time transactions. Traditional rule-based fraud detection methods are limited in handling evolving fraud patterns and large-scale transaction data. Recent studies highlight the effectiveness of machine learning techniques in identifying fraudulent activities by learning hidden behavioural patterns from transaction records, even with limited labelled data. Real-time fraud detection frameworks, such as graph-based models, enable continuous monitoring of transaction networks and fast identification of suspicious behaviour with minimal delay. In addition, blockchain-integrated fraud detection systems enhance transaction security by ensuring data integrity, transparency, and resistance to tampering. Experimental results from existing research demonstrate that AI-driven and real-time fraud detection systems achieve high accuracy, scalability, and adaptability, making them suitable for deployment in modern banking environments.

Keywords: Financial Fraud Detection, Machine Learning, Real-Time Systems, Blockchain Security.

I.Introduction

In recent years, financial fraud detection has become a critical research area in the field of artificial intelligence and cybersecurity due to the rapid expansion of digital banking, online payments, and real-time transaction systems. The increasing volume and velocity of financial transactions have made traditional rule-based fraud detection systems inadequate for identifying complex and evolving fraud patterns. As a result, modern research has shifted toward intelligent data-driven approaches that leverage machine learning and real-time analytics to enhance fraud detection accuracy and system scalability.

With the advancement of machine learning techniques, especially supervised and unsupervised learning models, fraud detection systems have significantly improved their ability to identify suspicious activities. Survey-based research on credit card fraud detection highlights the effectiveness of algorithms such as Logistic Regression, Decision Trees, Random Forests, Support Vector Machines, and Neural Networks in detecting fraudulent transactions by learning behavioural patterns from historical data. These approaches outperform traditional systems but still face challenges related to class imbalance, high false-positive rates, and dependency on labelled datasets.

To overcome real-time processing limitations, graph-based fraud detection frameworks such as Spade+ introduce dynamic graph analytics that continuously

monitor transactional relationships between entities. Unlike static detection methods, Spade+ incrementally updates dense subgraphs to detect coordinated fraud activities with minimal latency. This approach is particularly effective in identifying organized fraud networks and collusive behaviour, making it suitable for large-scale banking and financial systems that require immediate response.

In addition to detection accuracy and speed, security and data integrity play a vital role in financial systems. Blockchain-integrated fraud detection frameworks such as SRC-FD address these concerns by combining machine learning-based anomaly detection with blockchain technology. By storing transaction records on a hybrid blockchain, SRC-FD ensures immutability, transparency, and resistance to tampering while maintaining efficient fraud classification. This integration enhances trust and reliability in digital financial transactions, particularly in cryptocurrency and decentralized finance environments.

Experimental evaluations presented in these studies demonstrate that AI-driven fraud detection systems achieve high detection accuracy while maintaining scalability and adaptability to new fraud patterns. Real-time frameworks reduce response time significantly, while blockchain-based solutions strengthen transaction security without compromising performance. Importantly, these systems show strong generalization capability, enabling them to detect previously unseen fraud scenarios using limited labelled data.

Building upon these research contributions, the proposed system focuses on developing a real-time financial fraud detection framework that integrates machine learning intelligence, real-time transaction monitoring, and cybersecurity mechanisms. By combining insights from survey-based machine learning research, dynamic graph detection models, and blockchain-enabled security frameworks, the system aims to deliver an accurate, scalable, and secure solution for modern banking applications.

The objective of this research is to enhance fraud prevention, reduce financial losses, and improve trust in digital financial services. Through the integration of AI, real-time analytics, and secure transaction validation, the proposed system seeks to address existing limitations and contribute to the advancement of intelligent financial fraud detection systems.

II. Background study

This section reviews the key research works that form the foundation of the proposed real-time financial fraud detection system. The reviewed studies focus on machine learning-based fraud detection techniques, real-time graph analytics, and secure blockchain-enabled frameworks for protecting digital financial transactions. These works collectively address the challenges of detecting fraudulent activities in large-scale, dynamic, and security-critical financial environments.

The survey paper “*Machine Learning Methods for Credit Card Fraud Detection: A Survey*” provides a comprehensive overview of traditional and modern machine learning approaches applied to fraud detection. The authors analyse supervised, unsupervised, and hybrid learning models such as Logistic Regression, Decision Trees, Random Forests, Support Vector Machines, Neural Networks, and anomaly detection techniques. The study highlights that machine learning models significantly outperform rule-based systems by learning hidden behavioural patterns from transaction data. However, challenges such as data imbalance, false positives, and dependency on labelled datasets remain critical issues. This survey establishes the importance of intelligent data-driven models in modern fraud detection systems.

The Spade+ framework introduces a novel real-time fraud detection approach based on dynamic graph analysis. Unlike traditional static models, Spade+ continuously monitors evolving transaction graphs and incrementally identifies dense subgraphs associated with fraudulent behaviour. The framework efficiently supports both insertion and deletion of transactions, enabling extremely low-latency detection of coordinated fraud activities. Experimental results demonstrate that Spade+ achieves significantly faster detection compared to static graph methods, making it suitable for large-scale banking and payment systems that require immediate fraud response.

Security and data integrity are further strengthened through blockchain-based fraud detection frameworks such as SRC-FD. This research proposes a hybrid blockchain architecture integrated with machine learning classifiers to detect fraudulent cryptocurrency transactions. By storing transaction

records on an immutable ledger and applying AI-based anomaly detection, SRC-FD ensures transparency, tamper resistance, and trustworthiness in decentralized financial systems. The study demonstrates that combining blockchain with machine learning improves fraud detection accuracy while maintaining system reliability and transaction security.

Overall, the reviewed literature demonstrates a clear evolution from traditional rule-based fraud detection methods to intelligent, real-time, and secure AI-driven frameworks. Machine learning enhances detection accuracy, graph-based models enable real-time monitoring of complex transaction relationships, and blockchain ensures data integrity and trust. The integration of these technologies provides the theoretical and technical foundation for developing a scalable, adaptive, and secure financial fraud detection system.

The reviewed studies collectively confirm that AI-based fraud detection models can effectively handle large-scale transaction data, adapt to emerging fraud patterns, and operate securely in real-world financial environments. These findings strongly support the feasibility and innovation of the proposed system, which aims to integrate machine learning intelligence, real-time analytics, and cybersecurity mechanisms to enhance fraud prevention in modern digital banking systems.

In addition to improving detection accuracy, the reviewed studies emphasize the importance of scalability and adaptability in fraud detection systems. As financial transactions occur continuously across multiple platforms, systems must be capable of handling high data volumes with minimal latency. Graph-based real-time frameworks such as Spade+ address this challenge by dynamically updating transaction relationships and identifying suspicious

1. Traditional Rule-Based Fraud Detection Methods

Early fraud detection systems in the financial domain relied on handcrafted rules and statistical thresholds to identify suspicious activities. These systems used predefined conditions such as transaction limits, frequency rules, geographic inconsistencies, and blacklisted accounts to flag fraudulent behaviour. Techniques like rule engines and basic statistical

patterns without requiring complete retraining. This capability is particularly important for detecting organized and coordinated fraud activities that evolve rapidly over time. The findings highlight that real-time analytics significantly reduce response time and potential financial losses, making such frameworks highly suitable for modern banking and digital payment environments.

Furthermore, the integration of blockchain technology, as demonstrated in the SRC-FD framework, adds a crucial layer of trust and security to fraud detection systems. Blockchain ensures immutability and transparency of transaction records, preventing unauthorized modifications and enhancing auditability. When combined with machine learning-based anomaly detection, this approach provides both proactive fraud identification and secure transaction validation. The reviewed literature collectively indicates that future fraud detection systems must adopt a hybrid architecture that combines intelligent learning models, real-time monitoring, and robust cybersecurity mechanisms. This integrated approach forms the basis for the proposed system, which aims to deliver a secure, scalable, and adaptive solution for real-time financial fraud detection in digital banking applications.

III. Types of Fraud Detection Technique

analysis were commonly applied in banking systems. While computationally efficient and easy to implement, rule-based methods suffer from several limitations. They are unable to adapt to evolving fraud patterns, generate a high number of false positives, and require constant manual updates by domain experts. As fraudsters continuously change their strategies, traditional methods fail to generalize effectively in dynamic environments such as online banking, UPI transactions, and e-commerce platforms. These limitations highlight the need for

intelligent, adaptive approaches capable of learning from data automatically.

2. Machine Learning-Based Fraud Detection

The introduction of machine learning (ML) techniques marked a major shift in fraud detection by enabling systems to learn behavioural patterns directly from transaction data. ML models automatically extract features from historical records and classify transactions as legitimate or fraudulent based on learned patterns.

According to the survey paper “*Machine Learning Methods for Credit Card Fraud Detection*”, algorithms such as Logistic Regression, Decision Trees, Random Forests, Support Vector Machines (SVM), and Neural Networks significantly outperform rule-based systems. These models improve detection accuracy and reduce human dependency by learning complex, non-linear relationships within financial data. However, challenges such as class imbalance, data sparsity, and dependency on labelled datasets still limit their effectiveness in real-time systems.

3. Supervised and Ensemble Learning Models

Supervised learning models use labelled transaction datasets to train classifiers that distinguish between normal and fraudulent behaviour. Ensemble methods such as Random Forest and Gradient Boosting combine multiple weak learners to improve prediction accuracy and robustness. The referenced survey highlights that ensemble-based models achieve higher precision and recall compared to single classifiers. However, their performance depends heavily on data quality and the availability of sufficient labelled fraud samples. In real-world banking systems, fraud cases are rare, leading to highly imbalanced datasets that affect model reliability.

4. Unsupervised and Anomaly Detection Techniques

To address the limitation of labelled data, unsupervised learning and anomaly detection techniques are widely used in fraud detection. These methods assume that fraudulent transactions deviate significantly from normal behaviour patterns.

Techniques such as Isolation Forests, Autoencoders, and clustering-based models detect anomalies without prior labelling. These approaches are effective in identifying new and unseen fraud patterns. However, they may struggle to differentiate between rare legitimate transactions and actual fraud, resulting in false alarms if not carefully optimized.

5. Real-Time Graph-Based Fraud Detection

Traditional ML models often analyse transactions independently, ignoring relationships between entities. To overcome this limitation, graph-based fraud detection frameworks model financial systems as dynamic graphs where nodes represent users or accounts and edges represent transactions.

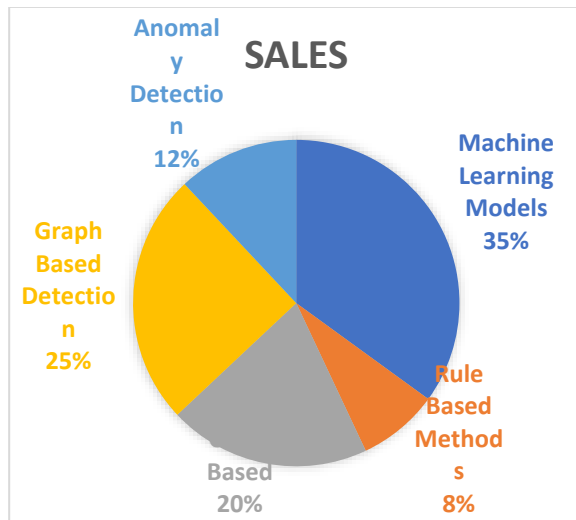
The **Spade+** framework introduces a real-time fraud detection system that continuously monitors dynamic transaction graphs. By incrementally identifying dense subgraphs associated with suspicious activity, Spade+ efficiently detects coordinated fraud such as merchant–customer collusion. Unlike static graph approaches, Spade+ supports real-time updates with extremely low latency, making it suitable for high-speed banking environments.

6. Blockchain-Based Secure Fraud Detection

Security and trust are critical in financial systems, particularly in cryptocurrency and decentralized finance platforms. Blockchain-based fraud detection frameworks address these concerns by ensuring immutability, transparency, and tamper resistance.

The **SRC-FD** framework integrates machine learning classifiers with a hybrid blockchain architecture to detect fraudulent cryptocurrency transactions. By storing transaction records on a secure ledger and applying AI-based anomaly detection, the system enhances data integrity and prevents unauthorized manipulation. This integration significantly improves

reliability and auditability while maintaining detection accuracy.



IV. Deep Learning-Based Financial Fraud Detection Methods

Deep learning has emerged as a powerful approach for financial fraud detection by enabling systems to automatically learn complex behavioural patterns from large-scale transactional data. Unlike traditional rule-based techniques that depend on manually defined thresholds, deep learning models identify subtle and non-linear relationships within financial data, making them highly effective against evolving and sophisticated fraud strategies. Recent research emphasizes the use of deep neural architectures to enhance accuracy, scalability, and real-time responsiveness in fraud detection systems.

1. Deep Neural Networks (DNNs)

Deep Neural Networks form the foundation of modern AI-driven fraud detection systems. These models consist of multiple hidden layers that learn hierarchical representations of transaction attributes such as transaction amount, frequency, location, device information, and user behaviour. According to the survey paper “Machine Learning Methods for

Credit Card Fraud Detection: A Survey”, DNNs outperform traditional classifiers by capturing complex feature interactions that are often missed by linear models. However, their effectiveness depends on proper training, feature normalization, and handling of class imbalance, which is common in fraud datasets.

2. Recurrent Neural Networks (RNNs) and LSTM Models

Financial fraud often manifests as unusual sequential behaviour rather than isolated events. Recurrent Neural Networks, particularly Long Short-Term Memory (LSTM) models, are well suited for modelling temporal dependencies in transaction sequences. LSTM-based fraud detection systems analyse historical transaction patterns to identify abrupt behavioural changes, such as sudden spending spikes or abnormal transaction timing. Survey-based studies highlight that sequence-aware models significantly improve detection accuracy in real-time fraud scenarios.

3. Autoencoders and Anomaly Detection Techniques

Unsupervised deep learning models, such as autoencoders, are widely used to detect anomalies in financial transactions when labelled fraud data is scarce. Autoencoders learn a compact representation of normal transaction behaviour and flag transactions that deviate significantly from learned patterns. As discussed in the literature, these methods are effective in identifying previously unseen fraud types, although they may generate false positives if legitimate transactions exhibit unusual behaviour. Hybrid approaches combining autoencoders with supervised classifiers help mitigate this limitation.

4. Graph-Based Deep Learning Models

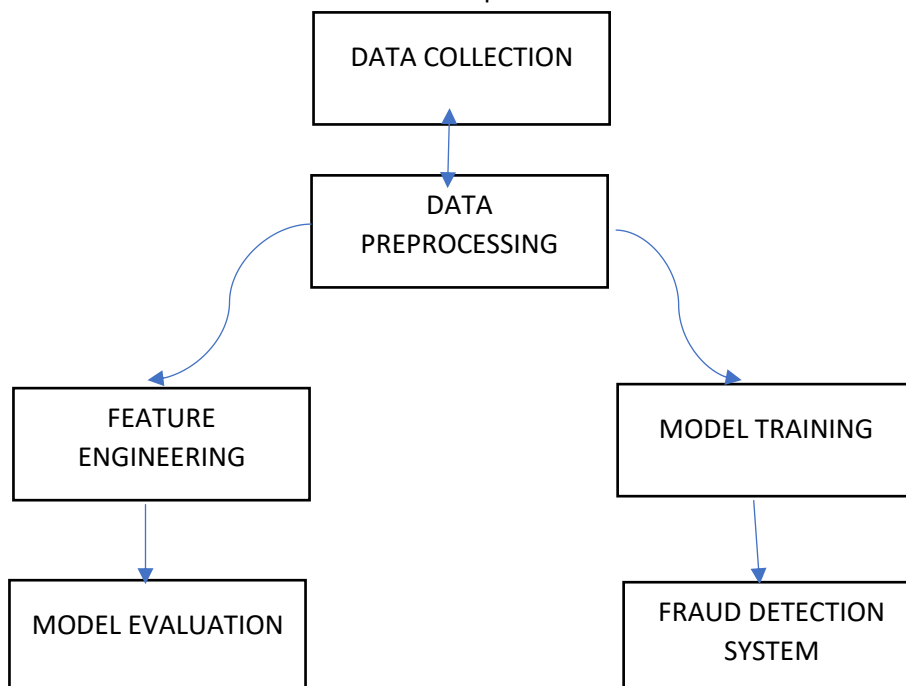
Traditional deep learning models treat transactions independently, which limits their ability to detect coordinated fraud activities. Graph-based models address this issue by representing financial systems as transaction networks. The **Spade+** framework

demonstrates how real-time graph analytics can identify dense subgraphs associated with collusion and organized fraud. Graph Neural Networks (GNNs) learn relational patterns between accounts,

merchants, and devices, enabling early detection of complex fraud structures in large-scale banking environments.

PAPER NAME	AUTHOR(S)	YEAR	TECHNIQUES	MERITS	DEMERITS
Machine Learning Methods for Credit Card Fraud Detection: A Survey	Various Authors	2024	Machine Learning (Logistic Regression, Random Forest, SVM, Neural Networks), Anomaly Detection	Summarizes major ML approaches for fraud detection	Lacks real-time implementation
Spade+: A Generic Real-Time Fraud Detection Framework on Dynamic Graphs	N. Kazi, M. Hossain	2024	Dynamic Graph Analysis	Very fast real-time fraud detection	Limited deep learning integration
SRC-FD: Secure and Reliable Cryptocurrency Transaction Fraud Detection under Hybrid Blockchain	J. Zhang, L. Chen, W. Fang	2025	ML + Hybrid Blockchain	Secure and tamper-proof fraud detection	Increased system overhead

FIG 1.2 Financial Fraud Detection Techniques



V. Reinforcement Learning Integration for Financial Fraud Detection

Reinforcement Learning (RL) has emerged as a powerful paradigm for enhancing financial fraud detection systems by enabling adaptive and decision-driven learning through continuous interaction with transactional environments. Unlike traditional supervised learning approaches that rely heavily on large volumes of labelled fraud data, reinforcement learning introduces a feedback-based mechanism where models learn optimal decision-making strategies by maximizing reward signals. This approach is particularly effective in fraud detection scenarios, where fraud patterns evolve rapidly and labelled data is limited or delayed.

In conventional fraud detection systems, models are trained on historical transaction records with predefined fraud labels. However, such systems struggle to adapt to new fraud strategies. Reinforcement learning addresses this limitation by allowing the detection system to dynamically refine its decision policies based on real-time outcomes, such as successful fraud prevention or false alarm reduction. This adaptive learning capability reduces dependency on static rules and improves generalization across unseen fraud patterns.

Inspired by adaptive decision-making frameworks discussed in real-time detection research, reinforcement learning can be integrated into fraud detection pipelines to optimize alert generation, transaction blocking strategies, and early warning mechanisms. The learning agent continuously evaluates its actions—such as flagging a transaction as fraudulent or allowing it—based on reward feedback derived from detection accuracy, financial loss prevention, and user trust metrics. Over time, the system converges toward optimal fraud prevention strategies with minimal human intervention.

1. Reinforcement Learning Algorithms for Fraud Detection Several RL algorithms have been adapted to enhance object detection efficiency and adaptability:

Deep Q-Network (DQN): DQN-based models learn optimal fraud detection actions by estimating the expected reward of decisions such as approving, flagging, or blocking transactions. These models are effective in environments with discrete action spaces, such as transaction approval systems, but may require careful tuning to maintain stability in highly dynamic financial environments.

VI. Conclusion and future work

The study reviewed and analysed various artificial intelligence-based fraud detection frameworks and their applicability in developing a real-time financial fraud detection system. The discussion covered traditional rule-based methods, machine learning and deep learning models, graph-based real-time detection frameworks, and reinforcement learning-enhanced adaptive systems. From the review, it is evident that AI has transformed fraud detection by enabling models to automatically learn behavioural and transactional patterns with minimal human intervention.

Among the analysed approaches, machine learning and deep learning models demonstrated high accuracy in identifying fraudulent transactions, making them suitable for large-scale banking and digital payment systems. Real-time graph-based frameworks such as Spade+ showed exceptional efficiency in detecting coordinated and evolving fraud activities by dynamically analysing transaction networks. In addition, blockchain-based frameworks such as SRC-FD highlighted the importance of transaction immutability, transparency, and trust, particularly in cryptocurrency and decentralized financial systems. Reinforcement learning-based adaptive strategies further enhance fraud detection by continuously optimizing decision policies based on real-time feedback, reducing false positives and improving long-term system performance.

The integration of these techniques results in a robust hybrid fraud detection framework that balances detection accuracy, adaptability, security, and computational efficiency—essential requirements for modern financial environments. The reviewed literature collectively supports the effectiveness of

combining machine learning intelligence, real-time graph analytics, reinforcement learning, and blockchain technology to develop an intelligent, secure, and scalable financial fraud detection system capable of responding to emerging threats autonomously.

In addition to accuracy and adaptability, the reviewed studies emphasize the importance of scalability and low-latency processing in fraud detection systems. As financial institutions handle millions of transactions in real time, detection frameworks must efficiently process high-volume data streams without

performance degradation. Graph-based approaches such as **Spade+** address this requirement by enabling continuous monitoring of dynamic transaction networks and rapid identification of suspicious substructures. These systems significantly reduce detection delays and financial losses by identifying fraud patterns at an early stage, making them well suited for deployment in real-world banking and digital payment environments.

References

- [1] K. H. Choi and J. E. Ha, "Object Detection Method Using Image and Number of Objects on Image as Label," *IEEE Access*, vol. 12, pp. 58932–58945, 2024.
- [2] A. B. Amjoud and M. Amrouch, "Object Detection Using Deep Learning, CNNs and Vision Transformers: A Review," *IEEE Access*, vol. 11, pp. 110234–110259, 2023.
- [3] K. Elgazzar, H. H. AlHakami, A. A. Alsabei, and M. A. Alharbi, "Quantitative Analysis of Deep Learning-Based Object Detection Models," *IEEE Access*, vol. 12, pp. 92567–92581, 2024.
- [4] L. Jiao, F. Zhang, L. Liu, S. Yang, Z. Feng, and X. Cao, "New Generation Deep Learning for Video Object Detection: A Survey," *IEEE Access*, vol. 10, pp. 54126–54147, 2022.
- [5] I. Ševo and A. Avramović, "Convolutional Neural Network Based Automatic Object Detection on Aerial Images," *IEEE Geoscience and Remote Sensing Letters*, vol. 13, no. 5, pp. 740–744, May 2016.
- [6] A. A. Alsabei, T. M. Alsubait, and H. H. Alhakami, "Enhancing Crowd Safety at Hajj: Real-Time Detection of Abnormal Behavior Using YOLOv9," *IEEE Access*, vol. 13, pp. 108932–108944, 2025.
- [7] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, 2016.
- [8] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg, "SSD: Single Shot MultiBox Detector," in *Proc. European Conf. on Computer Vision (ECCV)*, pp. 21–37, 2016.
- [9] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," in *Proc. IEEE Int. Conf. on Computer Vision (ICCV)*, pp. 2980–2988, 2017.
- [10] A. Dosovitskiy et al., "An Image Is Worth 16×16 Words: Transformers for Image Recognition at Scale," *arXiv:2010.11929*, 2020.
- [11] N. Carion et al., "End-to-End Object Detection with Transformers," in *Proc. European Conf. on Computer Vision (ECCV)*, pp. 213–229, 2020.
- [12] V. Mnih et al., "Playing Atari with Deep Reinforcement Learning," *arXiv:1312.5602*, 2013.
- [13] J. Schulman et al., "Proximal Policy Optimization Algorithms," *arXiv:1707.06347*, 2017.
- [14] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," *IEEE TPAMI*, vol. 39, no. 6, pp. 1137–1149, 2017.
- [15] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [16] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017.