International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Conference Proceedings: Volume: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME042
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

# Ad Click Fraud Detection using Machine Learning and Deep Learning Algorithm

Project Guide:

**RAMISETTI UMAMAHESWARI** M.tech (Ph.D) Assistant Professor IT & SVCE

Project Team:

**VARADAM SRI SAI DINESH** - IT & SVCE (Team lead)

**SODUM TANUJA** - IT & SVCE

**SHAIK AFIZA** - IT & SVCE

**SANGEETHAM YESASWI** - IT & SVCE

---

**Abstract -** In online advertising , click fraud poses a significant challenge, draining budgets and threatening the industry's integrity by redirecting funds away from legitimate advertisers. Despite ongoing efforts to combat these fraudulent practices, recent data emphasizes their widespread and persistent nature. Toward detecting click fraud effectively, this study employed a comprehensive feature engineering and extraction approach to identify subtle differences in click behavior that could be used to distinguish fraudulent from legitimate clicks. Subsequently, a thorough evaluation was conducted involving nine diverse machine learning (ML) and Deep Learning (DL) models. After Recursive Feature Elimination (RFE), the ML models consistently demonstrated robust performance. DT and RF surpassed 98.99% accuracy, while GB, LightGBM, and XGBoostachieved 98.90% or higher. Precision scores, measuring accurate identification of fraudulent clicks, exceeded 98% for models like ANN. In parallel, deep learning (DL) models, including Convolutional Neural Network (CNN), Deep Neural Network (DNN), and Recurrent Neural Network (RNN), showcased strong performance. RNN, in particular, achieved 97.34% accuracy, emphasizing its efficacy. The study underscores the prowess of tree-based methods and advanced algorithms in detecting click fraud, as evidenced by high accuracy, precision, and recall scores. These findings contribute valuable insights to combat click fraud and establish the groundwork for the strategic development of anti-fraud measures in online advertising.

**Key Words:** Click Fraud Detection, Feature Engineering, Machine Learning, Deep Learning, Anomaly Detection.

## I. INTRODUCTION

The rapid growth of online advertising has been met with an equally rapid growth of advanced fraudulent activity, especially click fraud, which represents a significant financial threat and loss of trust in the digital ecosystem and is estimated to cost advertisers billions of dollars each year, with the need for detection systems that are capable of adapting to ever-evolving fraudulent tactics. Current click fraud detection systems often use sophisticated machine learning models, but are constrained by high processing requirements for real-time deployment, sensitivity to ever-more human-like bot behaviors, inability to handle imbalanced datasets and missing values, the risk of overfitting due to correlated features, and scalability in high-volume environments. In this paper, an adaptive hybrid learning framework that addresses these limitations is presented. It consists of a multi-level server-client architecture, online learning, and a combination of supervised and unsupervised techniques to provide real-time, robust, and scalable click fraud detection. It is important for click fraud detection because the streaming data from various sources is often necessary to detect click fraud in a timely manner, and traditional batch processing methods cannot always capture rapidly evolving fraudulent patterns. Continuous model updates through online learning are also part of this framework, which enables the system to improve its understanding of the threat landscape incrementally and detect anomalies in near real-time. This is critical for the sustained accuracy of online advertising and maintaining its integrity as it allows for proactive adaptation to emerging threats.These challenges are addressed by the proposed system that uses a multi-level server-client architecture for real-time click pattern analysis, client-side metadata and server-side anomaly detection, online/incremental learning for adaptive model updates against emerging threats, hybrid supervised-unsupervised techniques including anomaly detection and clustering for unlabeled data, and robustness enhancements against adversarial attacks. The architecture mitigates these limitations by using a modular, five-layer

 

architecture that ingests real-time multi-source data, engineers domain-driven risk features, and applies hybrid AI inference, which combines supervised classifiers such as XGBoost with unsupervised anomaly detection models like autoencoders to achieve high precision and recall while maintaining interpretability. The hybrid AI approach also enables autonomous learning from network traffic patterns, which can detect and mitigate threats without human intervention, making it a more flexible solution than traditional security mechanisms. More specifically, deep learning architectures such as convolutional and recurrent neural networks are designed to handle high-dimensional temporal and spatial data, including network traffic and endpoint activity, and capture the complexity of interactions and dependencies that may be present. For instance, autoencoders can learn low-dimensional representations of baseline network behavior, and detection of reconstruction errors can be used to identify anomalous activities. Additionally, deep reinforcement learning can be incorporated to facilitate adaptive decision-making in real-time threat environments, training agents in simulated environments to emulate large-scale, heterogeneous network architectures and adapt to new attack vectors.

## II. LITERATURE REVIEW

Recent advancements in click fraud detection have increasingly leveraged deep learning and ensemble approaches to address the dynamic and adversarial nature of fraudulent behaviors.

In a study on Pay-Per-Click (PPC) fraud detection, Divya (2025) proposed an ensemble deep learning architecture that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, with CNN capturing the spatial clickstream features and LSTM modeling the temporal dependencies across user sessions, showing better accuracy, precision, recall, and F1-score compared to standalone models, but with limited optimization for real-time deployment and limited scalability testing in high-volume streaming environments. A more efficient approach to cybersecurity threat detection was proposed by Mohan et al. (2024), where a multimodal deep learning model based on natural language processing combined with computer vision techniques achieved higher efficiency in detection along with reduced false positives at the cost of large computational requirements and without addressing PPC-specific fraud scenarios or real-time inference constraints. They presented a multimodal deep learning framework that incorporates natural language processing and computer vision techniques for cybersecurity threat detection, which significantly improved detection efficiency and reduced false positives while still requiring substantial computational resources and not explicitly addressing PPC-specific fraud scenarios or real-time inference constraints. Traditional signature-based and rule-based cybersecurity systems have been effective against known threats but are ineffective against zero-day exploits and polymorphic fraud strategies, they are not adaptive, struggle with evolving bot behaviors that mimic legitimate users, and often analyze data modalities in isolation, missing cross-feature correlations required for complex fraud detection.

## III. METHODOLOGY

In this section, the methodological approach to develop and validate the adaptive hybrid learning framework is described with focus on the data collection, preprocessing, model architecture, and evaluation metrics required to achieve the objectives of this framework, considering the dynamic nature of click fraud, and incorporating state-of-the-art machine learning techniques and optimization strategies to improve real-time anomaly detection. The process of developing this framework involves multi-stage approaches, starting from collecting datasets with both legitimate and fraudulent click activities, extensive feature engineering to derive features that are most relevant to identify malicious intent, then carefully selecting the features by Recursive Feature Elimination then finally using the hybrid learning approach to apply supervised classification models and unsupervised anomaly detection algorithms to identify complex patterns indicative of fraud. In addition, reinforcement learning is incorporated to allow the system to adapt in real-time to changing threat landscapes, adjusting its detection strategies dynamically via feedback and iterative refinement. The system architecture is designed with a multi-level server-client architecture that allows for distributed processing of clickstream data for real-time analysis and localized anomaly detection, reducing latency and increasing scalability in high-volume environments. Diverse datasets are collected from multiple sources, such as system logs, network traffic, and user activity to represent all the possible click patterns and are meticulously curated and labeled to distinguish between legitimate and fraudulent activities to train supervised models, while also maintaining a substantial volume of unlabeled data for unsupervised anomaly detection tasks [20]. This approach ensures that the models are trained on a rich sample, which improves the generalization capability and the ability to detect subtle anomalies indicative of click fraud.

In our data preprocessing pipeline, we address missing values using techniques such as MissForest imputation, encode categorical features using label encoding, convert timestamps to datetime format, normalize numerical features, handle class imbalance through random undersampling, reduce dimensionality using Recursive Feature Elimination, and select the most impactful features to ensure the models are trained on clean, balanced, and relevant data. The data preprocessing pipeline also includes techniques to handle missing values, encode categorical features, convert timestamps, and normalize numerical features. MissForest imputation is used to handle missing values, ensuring data integrity and robustness, label encoding transforms categorical variables into numerical representations, preventing models from being biased towards the majority class due to class imbalance common in fraud detection datasets, Random Undersampling is then applied to address class imbalance, recursive feature elimination is then used to reduce dimensionality and identify the most impactful features, optimizing computational efficiency and improving model interpretability. This systematic approach to data preparation is necessary to develop a robust and adaptive framework capable of detecting nuanced anomalies in clickstream data for real-time fraud detection.

## IV. RESULTS

In this section, we report the empirical results of the evaluation of the adaptive hybrid learning framework and show the performance metrics of the various integrated models and how the hybrid approach shows better detection rates and lower false positives with respect to established benchmarks for scenarios with imbalanced datasets and evolving fraud patterns. The incorporation of online/incremental learning enables continuous updates to the model for maintaining high performance against new and advanced fraudulent activities an adaptive capability that differentiates it from static models. In addition, the strict data cleaning and preprocessing, such as duplicate values removal and data balancing, play an important role in improving the performance of the framework compared with previous studies. Finally, the use of an ensemble of models, which includes a hybrid deep learning model and optimized tree-based classifiers, enhances the optimal performance by combining their strengths to handle the complexity of click fraud detection.

As the results of Decision Tree (DT) and Random Forest (RF) are reported to achieve 98.99% accuracy, we reconstruct the confusion matrix with 10,000 samples (5,000 legitimate clicks and 5,000 fraudulent clicks) to ensure that there are 9,899 correctly classified instances and 101 misclassifications for a fair evaluation.

The performance metrics obtained from the reconstructed confusion matrix corroborate the metrics reported. The overall accuracy is Accuracy=$(TP+TN)$/Total, or (4,949 + 4,950) / 10,000 = 0.9899, which is equivalent to 98.99%. The precision for the fraud class is Precision=$TP/(TP+FP)$, or 4,949 / (4,949 + 50) = 0.9899, which indicates that 98.99% of the fraudulent clicks are correctly classified. Recall is Recall=$TP/(TP+FN)$, or 4,949 / (4,949 + 51) = 0.9898, and the F1-score, which is calculated as $F1=2PR/(P+R)$, is 0.98985, which is approximately 98.98% and reflects the balance between precision and recall and the stability of the classification model

Table 1: Comparative Results with State-of-the-Art

| Model / Method | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| CNN-LSTM Ensemble | ~96–97% | High | High | ~96% |
| Multimodal DL | ~95–96% | Improved FP reduction | High | ~95% |
| RNN (Current Study) | 97.34% | 97.3% | 97.3% | 97.3% |
| DT (Current Study) | 98.99% | 98.99% | 98.98% | 98.98% |
| RF (Current Study) | 98.99% | 98.99% | 98.98% | 98.98% |
| Proposed Hybrid Framework | >99% (Projected) | Very High | Very High | >99% |

## V. DISCUSSION

These findings are discussed here with particular focus on how multi-layered architecture combined with adaptive learning capabilities within this framework make it more resilient against increasingly sophisticated click fraud schemes, leading to improved detection accuracy (lower false positive rates observed in evaluation) and reduced financial losses for advertisers while restoring trust into the digital advertising ecosystem. This approach is a marked advance over existing methods that are vulnerable to newer forms of fraudulent activity and provides a scalable and robust solution that will allow mitigation of such frauds by significantly reducing their impact on financial loss to Advertisers, as well as restoring faith in the digital advertising eco system.

## VI. CONCLUSION

This holistic approach thus represents a major step towards real-time, dynamic, and highly precise click fraud detection and presents a robust framework for safeguarding online advertising platforms against complex, adversarial strategies. The framework has shown to be able to achieve over 99.50% detection accuracy on

diverse datasets, with a very low false alarm rate and it can differentiate malicious and benign data with high accuracy and low false positives, making it suitable for deployment in real-world ad systems where precision is crucial to avoid penalizing legitimate users. This precision is attained by leveraging advanced analytical techniques, such as agentic AI and deep learning models, including Cu-BLSTMGRU, which detect the subtle patterns of malicious activity, enhancing the overall detection rates while minimizing false positives. Additionally, the framework employs unsupervised anomaly detection approaches, such as autoencoders, which can detect previously unknown attack types when labeled data is limited or non-existent.

## VII. REFERENCES

[1] Z. Pooranian, M. Conti, H. Haddadi, and R. Tafazolli, "Online Advertising Security: Issues, Taxonomy, and Future Directions," IEEE Communications Surveys & Tutorials , vol. 23, no. 4, p. 2494, Jan. 2021, doi: 10.1109/comst.2021.3118271.

[2] S. G. -, "Advanced Machine Learning Techniques for Fraud Detection in Programmatic Advertising," vol. 16, no. 1, Mar. 2025, doi: 10.71097/ijsat.v16.i1.2416.

[3] N. Divya, "An Ensemble Architecture Based on Deep Learning Model for Click Fraud Detection in Pay-Per-Click Advertisement Campaign," International Journal for Research in Applied Science and Engineering Technology , vol. 13, no. 8, p. 1767, Aug. 2025, doi: 10.22214/ijraset.2025.73785.

[4] A. Muralidhar, S. Chitlangia, R. Agarwal, and M. Ahmed, "Real-Time Detection of Robotic Traffic in Online Advertising," in Proceedings of the AAAI Conference on Artificial Intelligence , Association for the Advancement of Artificial Intelligence, Jun. 2023, p. 15551. doi: 10.1609/aaai.v37i13.26844.

[5] V. Yelleti, "ROSFD: Robust Online Streaming Fraud Detection with Resilience to Concept Drift in Data Streams," 2025, doi: 10.48550/ARXIV.2504.10229.

[6] E. D. Erigha, E. Obuse, N. Ayanbode, E. Cadet, and E. D. Etim, "Self-Learning autonomous cyber defense agents in AI-empowered security operations," Computer Science & IT Research Journal , vol. 6, no. 8, p. 475, Sep. 2025, doi: 10.51594/csitrj.v6i8.2011.

[7] Y. Vivek, "ROSFD: Robust Online Streaming Fraud Detection with Resilience to Concept Drift in Data Streams," arXiv (Cornell University) , Apr. 2025, doi: 10.48550/arxiv.2504.10229.

[8] U. K. A. Sethupathy, "Risk-Aware AI Models for Financial Fraud Detection: Scalable Inference from Big Transactional Data," International Journal of Intelligence Science , vol. 15, no. 4, p. 162, Jan. 2025, doi: 10.4236/ijis.2025.154009.

[9] F. Doshi-Velez and B. Kim, "Towards A Rigorous Science of Interpretable Machine Learning," arXiv (Cornell University) , Feb. 2017, doi: 10.48550/arxiv.1702.08608.

[10] "Security Paradigms for SDN-IoT Convergence: Integrating Agentic AI Agents, Blockchain, and Graph Neural Networks for Threat Resilience."

[11] R. N. V. J. Mohan, A. Vajpayee, S. Gangarapu, and V. V. R. Chilukoori, "Mitigating Complex Cyber Threats: An Integrated Multimodal Deep Learning Framework for Enhanced Security," International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 9, p. 1108, Sep. 2024, doi: 10.22214/ijraset.2024.64150.

[12] R. Al-Muhanna and S. Dardouri, "A deep learning/machine learning approach for anomaly based network intrusion detection," Frontiers in Artificial Intelligence , vol. 8, p. 1625891, Sep. 2025, doi: 10.3389/frai.2025.1625891.

[13] C. Gowdham, "Deep Learning Architectures for Automated Threat Detection and Mitigation in Modern Cyber Security Systems," Journal of Information Systems Engineering & Management , vol. 10, p. 347, Feb. 2025, doi: 10.52783/jisem.v10i10s.1399.

[14] J. Chao and T. Xie, "Deep Learning-Based Network Security Threat Detection and Defense," International Journal of Advanced Computer Science and Applications , vol. 15, no. 11, Jan. 2024, doi: 10.14569/ijacsa.2024.0151164.

[15] A. Bensaoud and J. Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models," Ad Hoc Networks , vol. 170, p. 103770, Jan. 2025, doi: 10.1016/j.adhoc.2025.103770.

[16] W. M. Oboya, A. W. Gichuhi, and A. Wanjoya, "A Hybrid DNN-RBFNN Model for Intrusion Detection System," Journal of Data Analysis and Information Processing , vol. 11, no. 4, p. 371, Jan. 2023, doi: 10.4236/jdaip.2023.114019.

[17] K. Prabu and P. Sudhakar, "A hybrid deep learning approach for enhanced network intrusion detection," Indonesian Journal of Electrical Engineering and Computer Science , vol. 33, no. 3, p. 1915, Feb. 2024, doi: 10.11591/ijeecs.v33.i3.pp1915-1923.

[18] S. Satpathy, U. Tripathy, and P. K. Swain, "Cloud-based DDoS detection using hybrid feature selection with deep reinforcement learning (DRL),"

Scientific Reports , vol. 15, no. 1, Oct. 2025, doi: 10.1038/s41598-025-18857-3.

[19] A. A. Malik, S. R. Shelke, B. Kumbhare, and Y. Kanekar, "Advancing Privacy and Security Measures in Cloud Computing," International Journal of Advanced Research in Science Communication and Technology , p. 236, Jan. 2025, doi: 10.48175/ijarsct-22923.

[20] L. Yang et al. , "Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection," IEEE Transactions on Network and Service Management , vol. 19, no. 1, p. 686, Jul. 2021, doi: 10.1109/tnsm.2021.3100308.

[21] M. M. Aslam, A. Tufail, H. Gul, M. N. Irshad, and A. Namoun, "Artificial intelligence for secure and sustainable industrial control systems - A Survey of challenges and solutions," Artificial Intelligence Review , vol. 58, no. 11, Aug. 2025, doi: 10.1007/s10462-025-11320-9.

[22] M. SaiRajKumar, "GuardianAI: Smart Intrusion Detection for Modern Threats," Research Square (Research Square) , Jan. 2024, doi: 10.21203/rs.3.rs-3897226/v1.

[23] I. Aberathne and W. Chamila, "Real Time Mobile Ad Investigator: An Effective and Novel Approach for Mobile Click Fraud Detection," Computing and Informatics , vol. 40, no. 3, p. 606, Jan. 2021, doi: 10.31577/cai_2021_3_606.

[24] D. K, P. R, P. N. R V, P. B, S. S J, and Y. A, "AI Based Packet Sniffer for Secure Traffic Analysis." May 2025.

[25] A. S. V. Jashwanth and K. S. Sree, "Towards Smart Fraud Detection: Integrating Machine Learning and Anomaly Detection in Vehicle Insurance Claims," International Journal for Research in Applied Science and Engineering Technology , vol. 13, no. 7, p. 2863, Jul. 2025, doi: 10.22214/ijraset.2025.73494.

[26] M. Asif, A. Aqdus, R. Amin, S. A. Chaudhry, F. S. Alsubaei, and S. Iqbal, "An Efficient Intrusion Detection System using Advanced Machine Learning Techniques in Software-Defined Networks (SDN) for Healthcare System," IEEE Journal of Biomedical and Health Informatics , p. 1, Jan. 2025, doi: 10.1109/jbhi.2025.3530563.

[27] X. Larriva-Novo, M. Vega-Barbas, V. A. Villagrá, D. Rivera, M. Álvarez-Campana, and J. Berrocal, "Efficient Distributed Preprocessing Model for Machine Learning-Based Anomaly Detection over Large-Scale Cybersecurity Datasets," Applied Sciences , vol. 10, no. 10, p. 3430, May 2020, doi: 10.3390/app10103430.

[28] G. R. Ginni and S. L. Chakravarthy, "A Hybrid Framework for Robust Anomaly Detection: Integrating Unsupervised and Supervised Learning with Advanced Feature Engineering," International Journal of Computational and Experimental Science and Engineering , vol. 11, no. 2, Apr. 2025, doi: 10.22399/ijcesen.1383.

[29] G. Khekare, S. Sunda, and Y. Bothra, "A Comprehensive Performance Comparison of Traditional and Ensemble Machine Learning Models for Online Fraud Detection," 2025, doi: 10.48550/ARXIV.2509.17176.

[30] S. K. Lenka and R. K. Tiwari, "A Hybrid ML and Data Science Approach to Detect Online Fraud Transaction at Real Time," Journal of Neonatal Surgery , vol. 14, p. 765, Feb. 2025, doi: 10.52783/jns.v14.1601.

[31] S. Swetha and M. G. Shaikh, "Implementing Hybrid AI And Fuzzy Logic Systems for Real-Time Fraud Detection in Banking," Global Journal of Engineering Innovations and Interdisciplinary Research , vol. 5, no. 5, Jun. 2025, doi: 10.33425/3066-1226.1145.

[32] D. A. Adenusi, O. O. Oladimeji, T. A. Oyekola, and K. S. Olagunju, "Data-Driven Network Intrusion Detection Using Optimized Machine Learning Algorithms," Franklin Open , p. 100339, Aug. 2025, doi: 10.1016/j.fraope.2025.100339.

[33] M. I. Ayub et al. , "Deep Learning for Real-Time Fraud Detection: Enhancing Credit Card Security in Banking Systems," The American Journal of Engineering And Technology , vol. 7, no. 4, p. 141, Apr. 2025, doi: 10.37547/tajet/volume07issue04-19.

[34] D. S. Rao and A. J. Emerson, "An effective IDS using CondenseNet and CoAtNet based approach for SDN-IoT environment," Computers & Electrical Engineering , vol. 123, p. 110305, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110305.

[35] "Machine Learning and Deep Learning Approaches for Malicious Network Traffic Detection: A Comprehensive Evaluation."