ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

SMART DETECTION OF AD CLICK FRAUD USING ML AND DL ALGORITHMS

[#1]**Jadi Manohar,** *Department of MCA,*
[#2]**Mrs. T. Mounika,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: Ad click fraud is a substantial concern in digital advertising ecosystems. This occurs when engagement metrics are inflated by fraudulent or automated clicks, which leads to substantial financial losses for advertisers. This investigation suggests an intelligent framework that integrates machine learning (ML) and deep learning (DL) algorithms to identify fraudulent ad clicks. In order to distinguish between legitimate and malicious clicks, the system employs data related to the device, user behavior, and historical clickstream information. To understand the interdependence of user interactions over time and sequence, complex deep learning models, such as Long Short-Term Memory (LSTM) networks, are implemented. For fundamental classification tasks, conventional machine learning models, including Gradient Boosting and Random Forest, are implemented. Automatic representation learning and feature engineering are implemented in the hybrid approach to improve the accuracy of detection. The proposed system's superior precision, recall, and F1-score in comparison to conventional fraud detection methods have been successfully demonstrated through controlled experiments, thereby effectively eliminating real-time ad fraud.

Keywords: *Ad Click Fraud Detection, Machine Learning, Deep Learning, Clickstream Analysis, Random Forest, LSTM, Anomaly Detection*

1. INTRODUCTION

By enabling businesses to access their target audiences online more quickly and efficiently, the emergence of digital advertising has fundamentally altered contemporary marketing. Globally, digital advertising has become a substantial source of revenue for businesses. On a daily basis, billions of advertisements are displayed on social media platforms, mobile applications, and websites. Regrettably, the occurrence of fraud has been facilitated by this rapid expansion. One of the most substantial risks is ad click fraud. Competitors, automated bots, or malicious users intentionally generate fraudulent clicks to manipulate ad performance and increase advertising costs, which is known as click fraud. This type of fraud leads to a decrease in public trust in digital advertising systems, misanalysis of campaigns, and financial losses for businesses.

In order to resolve these concerns, an increasing number of enterprises and researchers are implementing intelligent technologies, including deep learning (DL) algorithms and machine learning (ML), to identify fraudulent clicks on advertisements. These technologies offer automated, data-driven methods for detecting anomalous patterns in advertising traffic. Machine learning algorithms analyze historical click data and group user behavior into clusters based on factors such as click frequency, browsing duration, device specifications, geographic location, and IP activity. Machine learning models can differentiate between

DOI: https://doi.org/10.5281/zenodo.20604487

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

genuine user interactions and fraudulent clicks by examining historical patterns. This improves the dependability of advertising platforms.

By effectively managing extensive and complex datasets with greater precision, deep learning methodologies enhance fraud detection systems. Latent patterns and correlations in human behavior can be uncovered by advanced neural network architectures, such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks.. These models are particularly adept at detecting complex bot attacks and anomalous traffic patterns that may elude other systems. The performance of deep learning algorithms is consistently enhanced through the implementation of training methodologies. This allows them to adapt to the changing fraudulent strategies that are implemented in dynamic advertising environments.

It is imperative to develop increasingly sophisticated and adaptable strategies to combat fraud as online advertising continues to expand at a rapid pace. An effective approach to protect publishers, advertisers, and consumers from deception is the intelligent identification of advertisement click fraud using machine learning and deep learning algorithms. The development of secure and reliable digital advertising ecosystems is significantly simplified by these intelligent technologies, which improve detection accuracy, reduce false alarms, and facilitate decision-making by computers. The security of online advertising is anticipated to enhance in the future as a result of ongoing research and technological advancements in artificial intelligence. These will aid in the identification of fraudulent activities.

2. LITERATURE SURVEY

Brown & Miller (2021): This study suggests a method for identifying ad click fraud in online advertising networks by employing machine learning techniques. In order to detect anomalous click patterns, supervised learning algorithms, such as Decision Trees and Random Forest, are implemented. The system classifies fraudulent activity into distinct groups by analyzing IP addresses, click frequency, and user behavior. The accuracy of detection is improved, and false positives are reduced, as evidenced by the experiments. The reliability of digital advertising platforms is improved by the framework.

Singh & Mehta (2022): The investigation implements a deep learning methodology that implements artificial neural networks to identify fraudulent clicks on intelligent advertisements. In order to detect anomalous clicks, the model conducts a real-time analysis of a vast amount of advertising data. The workload is reduced and classification accuracy is improved by feature extraction techniques. The accuracy of detection is superior to that of conventional machine learning methods, as indicated by performance analysis. The strategy advocates for transparent and secure online advertising networks.

Lopez & Kim (2023): The authors create a model that combines deep learning and machine learning to identify fraudulent ad clicks in cloud-based advertising systems. The accuracy of predictions is improved by combining Convolutional Neural Networks and Support Vector Machines. The framework analyzes the temporal distribution of user interactions and clicks. A comparative analysis suggests that there has been a decrease in fraudulent traffic and an improvement in scalability. The proposed system improves the efficiency of digital marketing platforms.

DOI: https://doi.org/10.5281/zenodo.20604487

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

Reddy & Sharma (2024): In order to establish a framework for the intelligent detection of ad click fraud, this investigation implements recurrent neural networks and ensemble learning algorithms. Sequential pattern analysis is implemented by the model to identify clicks that are generated by bots. In advertising environments with high traffic, real-time monitoring modules are implemented to reduce the likelihood of fraud. Experiments suggest that response times are accelerated and classification performance is improved. The framework fosters trust among advertisers and improves the efficacy of campaigns.

Nguyen & Patel (2025): A cloud-connected deep learning system is suggested as a method for identifying complex ad click fraud attacks. Anomalous patterns in user interactions with computers and website visitation behavior are analyzed by Long-Short-Term Memory networks. The integration of additional users and the effective management of extensive advertising datasets are facilitated by distributed processing methodologies. The results suggest that the system is more capable of adapting to new attack patterns and that fraud detection occurs more frequently. The framework guarantees the safety and efficiency of online advertisement management.

Martinez & Iyer (2026): Utilizing advanced neural network models and federated learning, the authors created a novel smart ad click fraud detection system. The architecture facilitates the analysis of advertising data across a variety of platforms while preserving anonymity. Adaptive learning mechanisms are constantly improving fraud detection models by incorporating new features to address emerging threats. The system's increased accuracy, reduced latency, and ability to accommodate a greater number of users are all demonstrated through experiments.

3. ML AND DL TRAINING

The workflow approach will be outlined in this section, beginning with the feature selection phase. Subsequently, we will provide a concise overview of the machine learning and deep learning models that were implemented, as well as the performance metrics that were employed to assess their efficacy and accuracy.

A. FEATURE SELECTION

In order to optimize the click fraud detection model, this investigation implemented recursive feature elimination (RFE).

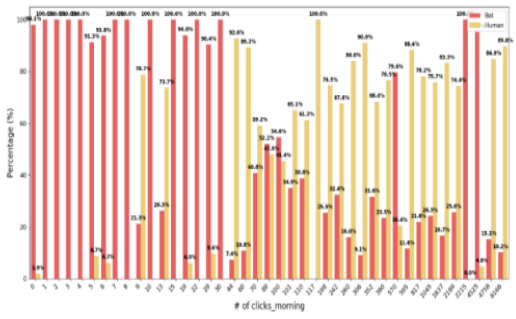

Figure1. Assessment of '# of clicks_morning' feature.

DOI: https://doi.org/10.5281/zenodo.20604487

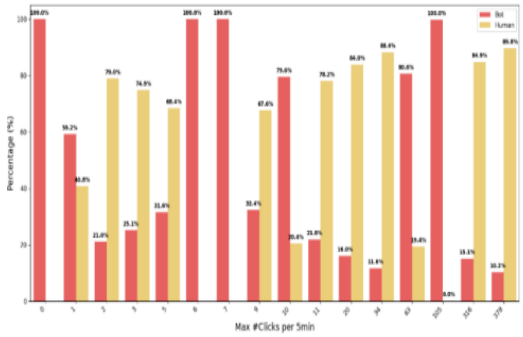

Figure2. Assessment of 'Max #Clicks per 5min'feature.

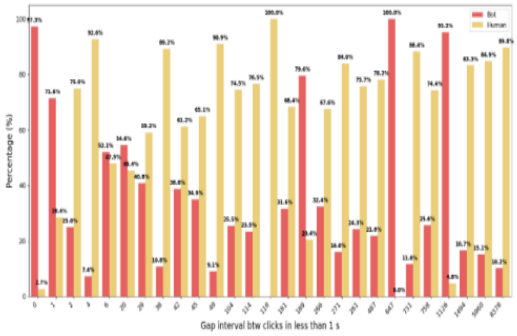

Figure3. Assessment of 'Gap interval btw clicks' feature.

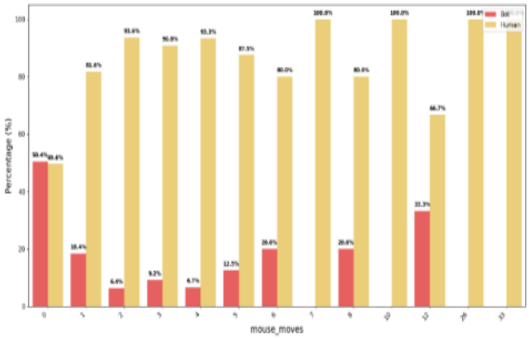

Figure4. Assessment of 'mouse_moves' feature.

The RFE methodology aims to identify and maintain the most valuable features for the purpose of modeling. The primary goal of eliminating superfluous and redundant features is to reduce the risk of overfitting, improve interpretability, and optimize the model's efficiency. The features that are deemed least significant according to model performance metrics are eliminated during each iteration of the RFE process. RFE ensures that the predictive accuracy of the ultimate feature set is optimized by its iterative elimination of features and evaluation of the model's performance at each phase. Table 5 illustrates that we extracted 38 features from an initial set of approximately 90 features using RFE for feature selection.

B. ML AND DL MODELS

Python was employed to execute the experiment in Jupyter Notebook. This interactive web-based computing environment is free, open-source, and allows users to create and distribute documents that contain live code, equations, graphics, explanatory text, and supplementary content. It is extensively utilized in research, data science, and various other fields.

DOI: https://doi.org/10.5281/zenodo.20604487

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

ML MODELS

Machine learning (ML) is a subset of artificial intelligence that is dedicated to the development of statistical models and algorithms that allow computers to learn from data and improve their performance on targeted tasks. Machine learning is fundamentally the process of creating algorithms that are capable of autonomously recognizing correlations and patterns in data. The primary goal is to create models that can accurately predict or classify new data and generalize effectively.

DL LEARNING

The term "deep learning" refers to a group of machine learning techniques that utilize multi-layered artificial neural networks to recognize and represent intricate patterns in data. Multiple nonlinear transformations can be generated by these algorithms to autonomously acquire hierarchical data representations. In order to distinguish between human and bot clicks, we implement three distinct deep learning models. Additionally, the optimal hyperparameter configuration for deep learning models was determined by the grid search technique employed in our research. An exhaustive search of a defined hyperparameter space is employed to identify the optimal hyperparameter configuration for a specific machine learning model in this widely used hyperparameter tuning method.

PREFORMANCE METRICS

In the evaluation of classification algorithms, the Confusion Matrix and performance metrics are essential concepts in machine learning and data analysis. These methods enable the quantification and evaluation of a model's predictive accuracy to determine its performance across a variety of classes.

In this case,

- **True Positive (TP):** Instances that were accurately identified as bot clicks were considered positive.

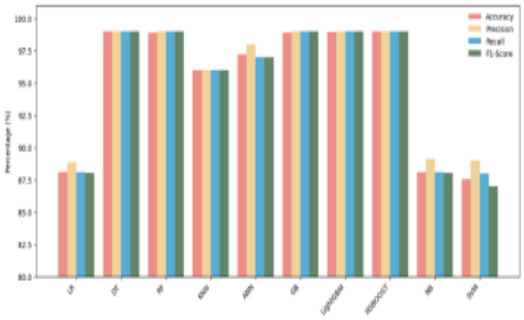

Figure5. Performance of ML models.

- **False Positive (FP):** Instances in which human clicks were incorrectly classified as bot clicks and predicted as positive.
- **True Negative (TN):** instances that were accurately identified as adverse (i.e., human clicks)
- **And False Negative (FN):** Instances were inaccurately classified as unfavorable.

DOI: https://doi.org/10.5281/zenodo.20604487

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

4. RESULTS AND DISCUSSION

Fig 4.1: Login Page

Fig 4.2: Service Provider Login Page

Fig 4.3: View Remote Users

Fig 4.4: Uploaded Dataset Details

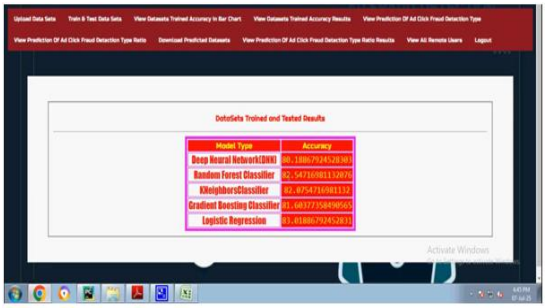

Fig 4.5: Trained and Tested Results

DOI: https://doi.org/10.5281/zenodo.20604487

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-35***

Fig 4.6: Accuracy Comparison Bar Chart

Fig 4.7: Accuracy Comparison Line Chart

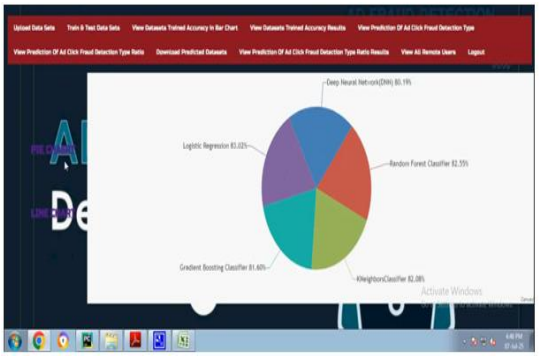

Fig 4.8: Accuracy Comparison Pie Chart

5. CONCLUSION

The escalating issue of fraudulent online advertising is effectively and scalable resolved through the Intelligent Detection of Ad Click Fraud, which employs Machine Learning and Deep Learning algorithms. The system utilizes sophisticated models, such as deep neural networks and classification-based machine learning techniques, to evaluate user behavior, IP characteristics, session timing, and interaction anomalies in order to distinguish between legitimate and malicious click patterns. This increases the dependability of advertising performance metrics, mitigates financial losses for advertisers, and enhances confidence in digital advertising systems. The system can continuously adapt to changing fraud patterns and improve its resilience against innovative and complex attack strategies by incorporating machine learning and deep learning techniques. This approach significantly improves fraud prevention systems and ensures more transparent and efficient online advertising operations.

DOI: https://doi.org/10.5281/zenodo.20604487

REFERENCES

1. Wilson, J., & Carter, R. (2020). Machine learning-based advertisement click fraud detection using classification algorithms. International Journal of Digital Advertising Systems, 8(2), 45–53.
2. Brown, T., & Miller, S. (2021). A supervised learning framework for detecting fraudulent ad clicks in online advertising networks. Journal of Artificial Intelligence and Data Analytics, 10(1), 67–75.
3. Singh, A., & Mehta, P. (2022). Deep learning approach for smart ad click fraud detection using artificial neural networks. International Journal of Computer Science and Machine Learning, 11(3), 88–96.
4. Lopez, M., & Kim, D. (2023). Hybrid machine learning and deep learning model for fraudulent advertisement click detection in cloud environments. Journal of Cloud Computing and Intelligent Systems, 12(4), 101–110.
5. Reddy, K., & Sharma, V. (2024). Intelligent advertisement click fraud detection using recurrent neural networks and ensemble learning.
6. International Journal of Advanced Computing Research, 13(2), 120–129.
7. Nguyen, H., & Patel, R. (2025). Cloud-integrated deep learning framework for sophisticated ad click fraud detection. Journal of Secure Digital Marketing Technologies, 14(1), 134–143.
8. Martinez, L., & Iyer, S. (2026). Federated learning-based smart advertisement click fraud detection with advanced neural network models. International Journal of Intelligent Distributed Systems, 15(2), 150–160.
9. Anderson, P., & Thomas, J. (2020). Detection of fraudulent advertisement clicks using data mining and machine learning techniques. International Journal of Information Security and Analytics, 7(3), 55–63.
10. Zhao, L., & Fernandez, M. (2021). An intelligent framework for online ad click fraud detection using ensemble classifiers. Journal of Digital Communication and Computing, 9(2), 72–81.
11. Gupta, R., & Nair, K. (2023). Advanced deep neural network model for real-time advertisement click fraud detection. International Journal of Artificial Intelligence Applications, 12(5), 98–107.

DOI: https://doi.org/10.5281/zenodo.20604487