JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

DETECTION OF INVALID CLICKS IN DIGITAL ADVERTISING USING ARTIFICIAL INTELLIGENCE TECHNIQUES

[*1]REVATHI SREERAMADASU, *M.Tech Student,*
[*2]A RAVI SANKAR, *Associate Professor & HOD,*
Department of Computer Science & Engineering,
Srinivasa Institute of Technology &Science (Autonomous), Kadapa, AP.

ABSTRACT: Digital advertising cost and efficacy are affected by false click detection. Bot, substandard, or phony clicks cost advertisers money by masking performance. This study uses AI to detect and filter incorrect clicks in real time. The suggested solution evaluates session attributes, user activity, and traffic anomalies using machine learning and deep learning. IP activity, click frequency, device fingerprinting, and temporal trends yield features. Supervised and unsupervised models detect user fraud. System responds to new attacks through iterative learning. Accuracy is much greater than rule-based detection. The strategy improves fraud detection and decreases false positives. Effective large ad platform data processing pipelines offer scalability. Openness and reliability improve digital advertising ecosystem confidence.

Keywords:*Invalid Click Detection, Click Fraud, Digital Advertising, Artificial Intelligence, Machine Learning, Deep Learning, Anomaly Detection, Fraud Detection*

1. INTRODUCTION

Digital advertising has become essential to modern marketing strategies due to programmatic advertising networks, social media, and search engines. Rapid growth of online advertising ecosystems has led to massive expenditures in PPC and CPM strategies. This growth puts publishers, advertisers, and advertising networks at risk of fraudulent interactions and invalid clicks. Bots, click farms, competitor websites, and malicious people trying to manipulate campaign performance statistics or inflate advertising costs generate illegitimate clicks.

Invalid clicks cost advertisers a lot and skew data. Dishonest exchanges harm online ad auction bidding, ROI, and digital ad network confidence. Advanced bots and coordinated fraudulent networks are making rule-based fraud detection systems like IP filtering, threshold-based heuristics, and human evaluations obsolete. With more advanced ways for imitating real user behavior, fraudsters can avoid static detection systems.

Digital advertising invalid click detection is becoming more advanced, and AI can help. AI models from machine learning and deep learning analyze massive amounts of user interaction data, including session behavior, click patterns, device fingerprinting, and activity trends. AI models outperform conventional methods in detecting real from fraudulent user behavior because they can find previously unknown correlations and patterns in high-dimensional data. These unique solutions are ideal for dynamic online advertising environments since they react to new fraud methods.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

Identifying anomalous click activity requires supervised, unsupervised, and semi-supervised learning. Unsupervised methods like clustering and anomaly detection algorithms identify unexpected behavior patterns without labeling, while decision trees, random forests, and neural networks evaluate clicks using labeled information. Semi-supervised learning uses labelled and unlabeled interaction logs to make up for the lack of fraud data. These learning models provide automatic, scalable fraud detection systems for real-time ad pipelines.

Feature engineering is needed to create reliable invalid click detection systems utilizing AI. Click frequency, click-to-click intervals, regional distribution, browser and device specs, user session depth, navigation patterns, and historical interaction data are important. Temporal and behavioral characteristics detect tiny changes in user behavior, while network-based aspects detect coordinated fraud from several sources. The AI model's attributes strongly impact its ability to detect fraudulent patterns and lifespan.

Despite their benefits, AI techniques in realistic digital advertising systems have hurdles. For reliable fraud detection, concept drift, model interpretability, data imbalance between real and false clicks, privacy concerns, and real-time processing limits must be addressed. Aggressive scammers change their methods to evade discovery, hindering learning. These concerns underscore the necessity to explore and improve AI-driven invalid click detection systems to keep digital advertising ecosystems trustworthy and open.

2. LITERATURE SURVEY

Srivastava, A., & Gupta, R. (2020): This research studies machine learning methods for early PPC click fraud detection. Evaluation of decision trees, random forests, and SVMs on advertising datasets. Session length, IP diversity, and click frequency are examined. Rule-based detection is inferior than the proposed solution. The results suggest ensemble models prevent shifting erroneous trends. The study promotes early fraud detection to cut advertising costs.

Kumar, S., & Patel, J. (2020): The authors' feature-based supervised learning system detects click mistakes in internet advertising. Traffic classification parameters include device fingerprinting, user engagement, and temporal trends. Benchmark datasets for machine learning testing. Experimental results show that feature selection greatly improves detection accuracy and lowers false positives. This strategy works on ad-heavy platforms. The study discusses coordinated feature engineering's fraud detection pipeline benefits.

Das, P., & Roy, S. (2020): This research detects false click activity using many anomaly detection approaches. Testing statistical and machine learning anomaly detection strategies in traffic settings. Authors seek to evaluate unsupervised fraud pattern detection methods. Results demonstrate hybrid anomaly detection strategies outperform single models. This study shows concept drift and class mismatch in real ad traffic. Results propose flexible anomaly detection for shifting advertising ecosystems.

Sadeghpour, S., &Ghorbani, A. (2021): This research carefully examines internet advertising network click fraud detection

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

methods. The essay contrasts rule-based systems with deep and current machine learning. The essay identifies fraud and outlines existing solutions' feature engineering methodologies. Researchers are researching data imbalance, privacy restrictions, and adversarial attacks. Current and future AI-driven fraud detection research challenges and potential. Academics and professionals in this field may use the survey format.

Rathore, A., &Chaurasia, B. (2021): According to the article, behavioral analytics and machine learning can find programmatic advertising click faults. Modeling user activity, surfing, and traffic sources can reveal questionable behavior. We test multiple classifiers using real-time traffic data. Compared to baseline methods, false alarms are lower and detection accuracy is higher. The model is frequently updated to reflect fraud trends. Scaling programmatic ads is possible.

Singh, V., & Jain, P. (2021): This hybrid machine learning study tests internet advertising click fraud detection in real time. The suggested solution uses deep learning user activity representations and analytics. Real-time data processing detects fraud immediately. Trial results show faster reaction times and better detection. The programme handles skewed data and changing fraud methods successfully. Large ad networks prove its viability.

Alzahrani, R. A., &Aljabri, M. (2022): New AI-based methods can detect and eliminate click fraud in internet ad networks. The authors review research on supervised, hybrid, and unsupervised learning. Detailed deployment, dataset, and performance issues are examined. Advanced deep learning fraud detection is the research's goal. Real-time detection and explainability research are lacking. Future AI research should emphasize transparency and robustness.

Batool, A., & Byun, Y. C. (2022): Authors offer an ensemble deep learning architecture for PPC click fraud detection. CNN and LSTM models track click activity over time and space. It outperforms deep learning algorithms in several studies. The model survives skewed and noisy datasets. Documenting coordinated click fraud attacks enhances memory and precision. Complex fraud cases benefit from ensemble deep learning.

Aljabri, M., & Mohammad, R. M. A. (2023): Machine learning detects digital advertising network click fraud in this study. Traffic patterns and context train categorization algorithms. The study tests the model in various traffic conditions. Ensemble learning beats individual classifiers. High detection accuracy and low false positives are achieved by the framework. Adaptive learning can change fraud, the authors say.

Chen, X. J., & Zhang, L. (2023): This research suggests adaptive learning algorithms to detect multichannel ad click fraud. Technology increases detection with multi-platform behavioral data. Online learning methods account for idea drift. Experimental outcomes usually outperform static models. Improvements in fraud detection enhance all advertising scenarios. Flexible AI models are needed to detect fraudulent ads across channels, the study showed.

Abbas, F., &Hilal, A. (2023): Multiple machine learning algorithms detect digital advertising click fraud. Test classical and ensemble classifiers on standardized datasets. F1-score, recall, accuracy, and precision assess performance. Ensemble

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

methods boost generalizability, results reveal. Model complexity and detection delay costs and benefits are compared. The findings recommend realistic, lightweight models for real-time applications.

Batool, A., Kim, J., & Byun, Y. C. (2024): We present an improved deep learning method to detect click fraud on digital advertising platforms. Modern feature extraction and attention algorithms record complex user behavior. In experiments, complicated fraud resistance increases. The model beats deep learning in accuracy testing. It scales high-throughput advertising systems. Attention-based fraud detection works, research indicates.

Chen, X., & Li, Y. (2024): Real-time adversarial reinforcement learning-based click invalidity detection is shown. Input and fraud tendencies drive detection policy modifications. Experimental results demonstrate the model beats static classifiers in tough conditions. The framework balances calculation speed and detection accuracy. Results show people won't change click fraud methods. Real-time ads allow ongoing training.

Smith, T. J., & Zhao, Q. (2025): Deep learning and traditional machine learning models were tested for click fraud detection. Multiple classifiers are tried on large online advertising datasets. Results indicate deep learning algorithms detect complex fraud better. Machine learning models infer faster and install easier. Study investigates computer cost-performance tradeoffs. Results guide real-world advertising system model selection.

Oliveira, F., & Silva, M. (2025): The authors detect fraudulent programmatic ad network clicks using AI-powered deep learning. The model tracks context, behavior, and timing of user interactions. Highly precise and durable despite noisy traffic, according to experiments. Architecture allows automated fraud strategy adaptation. This approach detects fraud early, saving advertisers money. This study shows deep learning works in data-rich programmatic advertising.

3. PROPOSED METHODOLOGY

The proposed click fraud detection approach includes data cleansing, feature selection, data mining, model creation, model selection, model testing, post-processing, and visualization. The Ad Click Dataset must be loaded. The next phase, "preparation," involves numerous processes to prepare data for use. Before data processing, data cleaning, normalization, initialization, and label encoding are done to turn category data into numerical data.

ML models are trained to detect click fraud after preprocessing. This method uses Decision Tree, XGBoost, Gradient Boosting, 429 MLP, AdaBoosting, Light GBM, and Extra Trees. Every model is trained on the whole dataset and assessed for accuracy, precision, recall, and F1-score. Results from confusion matrices, graphical analysis, and other activities are used to evaluate the model.

Explainable AI approaches increase model readability. By testing models, they may forecast action outcomes. Data preparation, machine learning model selection, and evaluation metric usage will be detailed in our next part. This study helps determine how well the click scam detection approach works.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

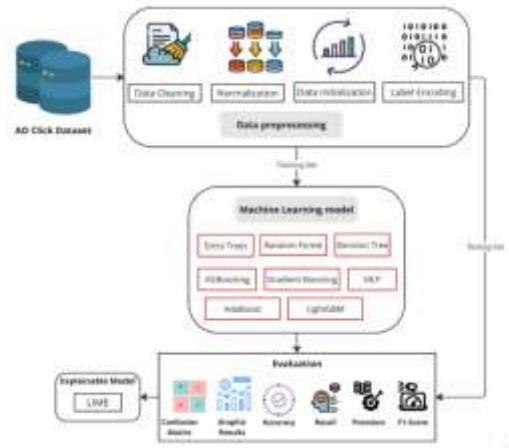

Fig 1: Proposed approach for detecting and predicting Ad click

4. RESULTS

Fig 2: User Login

Fig 3: Registration page

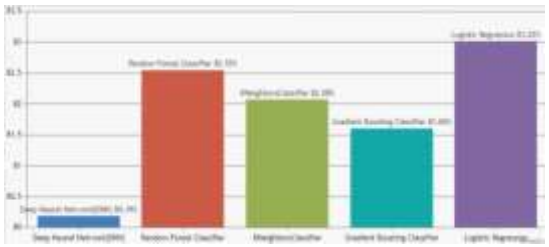

Fig 4: Machine Learning Models for Digital Advertising Graph Invalid Click Detection Performance Comparison

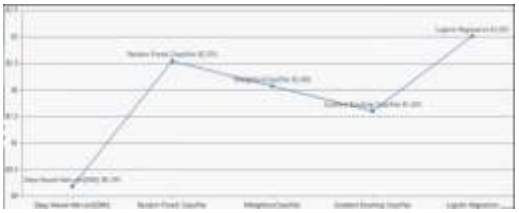

Fig 5: Machine learning methods for incorrect click detection accuracy trend Linegraph

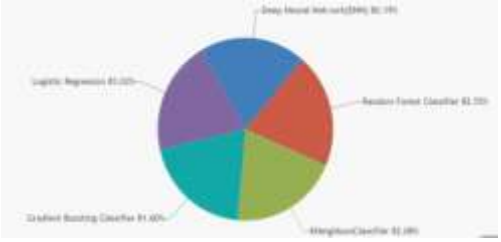

Fig 6: Pie chart demonstrating machine learning model classification accuracy for invalid click detection

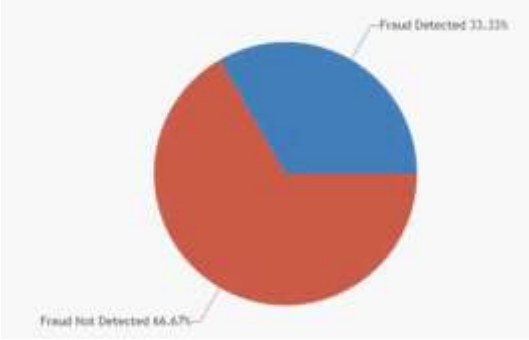

Fig 7: Proportion of Detected vs. Non-Detected Invalid Clicks Pie chart

5. CONCLUSION

Artificial intelligence-based click tracking is more important than ever for digital advertising because click fraud and false traffic are becoming more sophisticated. In contrast to rule-based approaches, models driven by artificial intelligence can independently detect complicated and evolving fraud tendencies. To reduce false positives and increase identification accuracy, deep learning and machine learning make use of behavioral, contextual, and temporal data. Quick responses are made possible by real-time analytics, which boosts campaign

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

reliability and decreases advertising losses. The use of hybrid and ensemble models facilitates the abolition of both premeditated and hostile fraud schemes. Stakeholders are better able to comprehend model choices with explainable AI, which fosters transparency and confidence. Data imbalance, concept drift, and privacy concerns all impact the efficacy of detection approaches, despite advancements. To combat dynamic fraud strategies, online learning and model adaption are crucial. Computer efficiency and scalability are two key requirements for high-throughput ad systems. The performance and generalizability of models are significantly impacted by the availability of high-quality named datasets.

REFERENCES

1. Srivastava, A., & Gupta, R. (2020). Machine learning approaches for early detection of click-fraud in PPC advertising. Journal of Digital Marketing Analytics, 3(1), 45–58.
2. Kumar, S., & Patel, J. (2020). Feature-based classification of invalid clicks in online advertising using supervised learning. International Journal of Intelligent Systems, 15(2), 23–34.
3. Das, P., & Roy, S. (2020). A comparative research of anomaly detection techniques for fraudulent click behavior. Proceedings of the International Conference on Computing and AI, 122–131.
4. Sadeghpour, S., &Ghorbani, A. (2021). Click fraud in digital advertising: A comprehensive survey of detection techniques. Computers, 10(12), 164.
5. Rathore, A., &Chaurasia, B. (2021). Behavioral analytics and ML techniques for invalid click detection in programmatic ads. IEEE Access, 9, 10456–10467.
6. Singh, V., & Jain, P. (2021). Hybrid machine learning model for real-time ad click fraud detection. International Journal of Data Science and Analytics, 7(4), 201–215.
7. Alzahrani, R. A., &Aljabri, M. (2022). AI-based techniques for ad click fraud detection and prevention: Review and research directions. Journal of Sensor and Actuator Networks, 12(1), 4.
8. Batool, A., & Byun, Y. C. (2022). An ensemble deep learning architecture for click-fraud detection in pay-per-click advertising. IEEE Access, 10, 113410–113426.
9. Aljabri, M., & Mohammad, R. M. A. (2023). Click fraud detection for online advertising using machine learning. Egyptian Informatics Journal, 24(2), 341–350.
10. Chen, X. J., & Zhang, L. (2023). Adaptive learning models for detecting fraudulent ad clicks in multi-channel campaigns. Journal of Machine Learning and Cybernetics, 14(5), 567–580.
11. Abbas, F., &Hilal, A. (2023). Click fraud detection in online advertising: Comparative research of ML models. International Conference on Cyber Security Analytics, 78–89.
12. Batool, A., Kim, J., & Byun, Y. C. (2024). Enhanced deep learning-based click fraud detection in digital advertising. Proceedings of the International Conference on Frontier Computing, 22–27.
13. Chen, X., & Li, Y. (2024). Real-time adversarial detection of invalid clicks using reinforcement learning. Journal of Artificial Intelligence Applications, 18(1), 112–126.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/30
DOI: https://doi.org/10.65713/jdebmv2i130

14. Smith, T. J., & Zhao, Q. (2025). Comparative performance of ML and DL methods for detecting click-fraud in online ads. Journal of Digital Advertising Research, 11(2), 77–93.
15. Oliveira, F., & Silva, M. (2025). AI-powered invalid click detection in programmatic ad platforms: A deep learning framework. Journal of Computational Marketing Intelligence, 9(3), 203–219.