Emerging Trends in Digital Transformation
Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-08***

MACHINE LEARNING AND DEEP NEURAL NETWORK BASED APPROACH FOR ONLINE AD CLICK FRAUD DETECTION

[#1]**D. SHIREESHA,** *Dept of CSE,*
[#2]**Dr.D.SRIKANTH REDDY,** *AssistantProfessor, Dept of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: The cost and efficacy of digital advertising are impacted by false clicks. Views that are fake, bot-generated, or of poor quality damage advertisements and cost marketers money. AI in this experiment instantly avoids errors. The proposed system uses machine learning and deep learning to assess session metrics, user activity, and traffic. Features are provided by IP activity, click frequency, device fingerprinting, and temporal trends. Both supervised and unsupervised algorithms are used to detect user fraud. Repeated attacks teach the system. An error occurs when rule-based detection is used. It lowers false positives and streamlines fraud detection. The data flow of a large advertising platform can increase. Trust is developed through transparent and reliable digital advertising networks.
Keywords: *Invalid Click Detection, Click Fraud, Digital Advertising, Artificial Intelligence, Machine Learning, Deep Learning, Anomaly Detection, Fraud Detection*

1. INTRODUCTION

In marketing, search engines, social media, and programmatic networks are the main forces behind digital advertising. PPC and CPM expenses have increased due to the rapid expansion of internet advertising networks. This increase exposes networks, publishers, and advertisers to phony views and fraudulent interactions. Click farms, bots, rival websites, and dishonest individuals produce phony clicks to increase campaign performance or advertising expenses.
Marketers squander funds and information on phony perspectives. Deceptive transactions damage network trust, ROI, and online ad auction bidding. Structured fraudster networks and sophisticated bots avoid human fraud detection, threshold-based algorithms, and IP filtering. Advanced user behavior simulators are used by scammers to evade static detection.
AI is able to recognize fraudulent digital advertising practices with speed. AI models for machine learning and deep learning examine click patterns, activity trends, device fingerprinting, and user session behavior on large websites. AI algorithms might be more adept at identifying fraudulent user behavior since they might discover novel patterns and connections in multivariate data. Because online advertising is constantly changing, these special systems can adjust to new fraud techniques.
It takes supervised, unsupervised, and semi-supervised learning to detect abnormal click activity. Unlabeled abnormalities are found using clustering and anomaly detection techniques. Neural networks, decision trees, and random forests use labeled data to assess interactions. Semi-supervised learning fraud data gaps are filled by labeled and unlabeled interaction recordings. Everywhere, real-time ad pipeline fraud is detected by learning models.

DOI: https://doi.org/10.5281/zenodo.20487333

Feature engineering is necessary for AI-based invalid click detection. Important factors include the depth of the user experience, navigation, past interactions, location, browser and device specifications, click duration, and frequency. While temporal and behavioral data indicate minimal changes in user behavior, network-based features reveal significant fraud. An AI model's features determine how long it lasts and how well it can identify fraudulent trends.

AI works well but presents challenges for digital advertising. Concept drift, model interpretability, data imbalance between authentic and fraudulent clicks, privacy concerns, and real-time processing limitations must all be taken into account when detecting fraud. Aggressive fraudsters find it more difficult to learn since they alter their strategies to evade discovery. To ensure the stability of the digital advertising ecosystem, it is necessary to investigate and enhance AI-powered invalid click detection.

2. DEEP NEURAL NETWORK–BASED APPROACH

In order to identify sophisticated click fraud, deep learning systems can automatically understand complex nonlinear correlations and temporal relationships in large clickstream data. Deep neural networks are perfect for real-time fraud detection in online advertising systems because they can adjust to new fraud techniques. as opposed to models that are superficial or based on rules.

To differentiate users from malware, these algorithms look at click frequency, dwell time, session length, device fingerprinting, IP address patterns, and navigation sequences.

Artificial Neural Networks (ANN): Fraud can be detected by deep learning models such as ANNs and MLPs. It has hidden layers, input, and output. Complex nonlinear correlations between click frequency, session duration, IP address consistency, device fingerprint, and regional trends can be learned by the model thanks to hidden layers. ReLU and Sigmoid activation functions facilitate the acquisition of nonlinear fraud strategies. Use backpropagation and gradient descent to enhance classification. Artificial neural networks are suitable for a number of labeled datasets. Real-time fraud risk assessment is common.

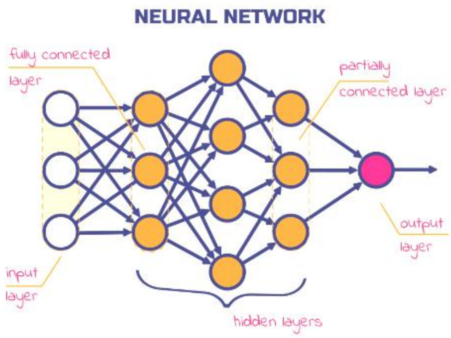

Fig. 1: Neural Network Architecture

Recurrent Neural Networks (RNN): The actions of models are linked to sequential data by RNNs. RNNs, in contrast to other types of neural networks, try to hide previous time steps. Users are assigned sessions that are time-based. It is possible for RNNs to identify click fraud by analyzing the click sequence, the length of the click, and the navigation of the session. When bots browse, they do it in peculiar ways and at peculiar times. It is possible for RNNs to detect dishonesty when user interactions are timed and sequenced in a specific order.

DOI: https://doi.org/10.5281/zenodo.20487333

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-08***

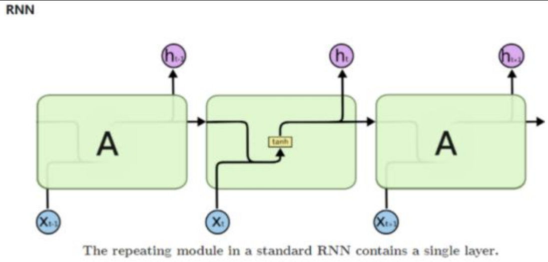

Fig. 2: Recurrent Neural Network (RNN) Architecture

Long Short-Term Memory (LSTM): Long-term dependence and gradient diminishing are handled by sophisticated RNNs like LSTM. Information flow is regulated over time using LSTM memory cells and input, output, and forget gates. By identifying coordinated malware click sequences over time or sessions, LSTMs are able to identify click fraud. The deceit of a delayed attacker is identified. Long-term contextual monitoring aids LSTMs in identifying intricate and ever-changing fraudulent advertising.

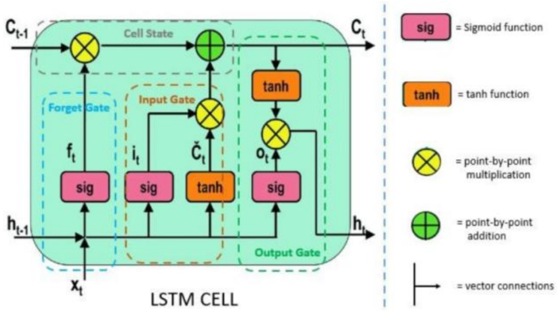

Fig. 3: Long Short-Term Memory (LSTM) Cell Architecture

Autoencoders: Deep autoencoders learn on their own. The primary objective is to identify click fraud. The decoder reconstructs the lower-dimensional latent form from which the encoder writes the data. By using shared data for training, it replicates click behavior. False inputs cause the system to become alerted by increasing reconstruction error. In unlabeled data, autoencoders identify novel fraud trends.

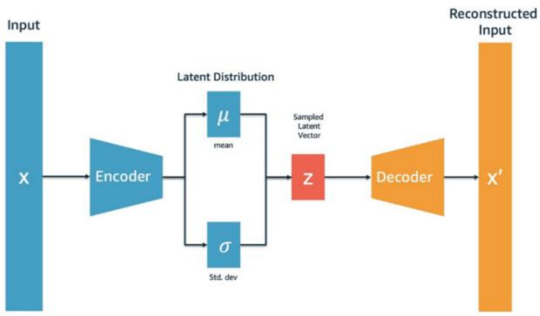

Fig. 4: Variational Autoencoder (VAE) Architecture

Graph Neural Networks (GNN): Relationship data is examined by deep learning GNNs. Click fraud nodes include people, gadgets, accounts, and IP addresses. Graph edges are the result of shared properties. These structures are used by GNNs to identify coordinated fraud networks and botnets. Abnormal accounts, infrastructure utilization, and hidden fraud are discovered. GNNs are able to identify massive, coordinated click fraud thanks to structured links.

DOI: https://doi.org/10.5281/zenodo.20487333

Volume-2, Issue-2, April-June 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I2-08

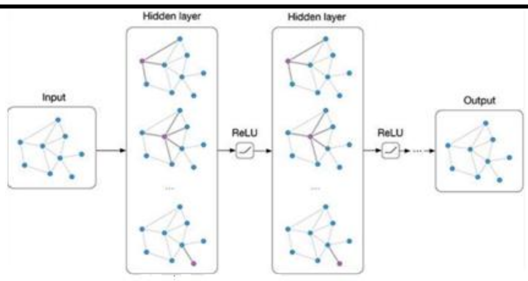

Fig. 5: Graph Neural Network (GNN) Architecture with ReLU Activation Layers

3. LITERATURE SURVEY

Srivastava, A., & Gupta, R. (2020): Machine learning is employed to early identify PPC click fraud in this investigation. Decision trees, random forests, and SVMs are employed to evaluate advertising datasets. The evaluation is conducted with respect to the session length, IP diversity, and interactions. The proposed technique surpasses rule-based detection. Data indicates that ensemble models mitigate spurious trends. The paper recommends the early detection of deception in order to reduce advertising expenditures.

Kumar, S., & Patel, J. (2020): The online ad click issues are detected by their feature-based supervised learning method. In the classification of traffic, device fingerprinting, user involvement, and temporal patterns are all considered. Datasets for validating machine learning models. Experimental results indicate that the accuracy of detection is improved and the number of false positives is decreased through the use of feature selection. This strategy is well-suited to platforms that are heavily reliant on advertisements. The report examines the advantages of the coordinated feature engineering fraud detection pipeline.

Das, P., & Roy, S. (2020): In this investigation, spurious click activity is detected by numerous anomaly detection systems. Evaluate traffic anomaly statistical and machine learning methodologies. Unsupervised fraud pattern identification will be evaluated by the authors. The results indicate that hybrid anomaly detection systems outperform singular models. Idea drift and class disparity are identified in advertising traffic. The results indicate that anomaly detection can be adapted to changing advertising conditions.

Sadeghpour, S., & Ghorbani, A. (2021): This research conducts a comprehensive examination of the detection of click fraud in internet advertising networks. Rule-based systems are contrasted with contemporary machine learning. According to the essay, feature engineering is employed in fraud prevention solutions. Data imbalance, privacy, and external attacks are investigated by researchers. Issues and prospects in research on AI-driven fraud detection. Surveys are applicable to both academics and professionals.

Rathore, A., & Chaurasia, B. (2021): The research asserts that programmatic advertising click faults can be identified through the use of behavioral analytics and machine learning. Modeling internet use, behavior, and traffic sources in an inappropriate manner. Real-time traffic data is employed to evaluate numerous classifiers. Our detection accuracy exceeds the baseline, and our false alarm rate is reduced. The model is periodically updated to monitor fraud. It is feasible to expand programmatic advertisements.

Singh, V., & Jain, P. (2021): Real-time internet ad click fraud is identified in this hybrid machine learning study. Deep learning is employed to analyze user activity in the proposed

DOI: https://doi.org/10.5281/zenodo.20487333

system. Fraud is promptly identified through real-time data processing. The trials demonstrated improved detection and quicker reaction times. The program continues to function despite the presence of evolving fraud methods and inconsistent data. Large advertising networks illustrate.

Alzahrani, R. A., & Aljabri, M. (2022): AI has the capacity to identify and prevent click deception on online ad networks. Research on supervised, hybrid, and unsupervised learning is examined. We evaluate efficacy, dataset, and deployment concerns. To enhance the detection of fraud through deep learning. The field of real-time detection and explainability is currently lacking in research. In the future, artificial intelligence research should be transparent and resilient.

Batool, A., & Byun, Y. C. (2022): A potent deep learning approach is presented for the detection of PPC click fraud. CNNs and LSTMs monitor actions in relation to time and location. Research indicates that it surpasses deep learning. The model is capable of analyzing data that is distorted or noisy. Recall and accuracy are enhanced by acknowledging coordinated click fraud assaults. Complex fraud is mitigated by ensemble deep learning.

Aljabri, M., & Mohammad, R. M. A. (2023): In this investigation, click fraud on digital advertising networks is identified through machine learning. Grouping algorithms are taught by traffic patterns and context. The model is scrutinized in a variety of traffic scenarios in the study. Single classifiers are inferior to ensemble learning. The framework precisely identifies objects with minimal false positives. Adaptive learning has the potential to alter the nature of fraud, as per the authors.

Chen, X. J., & Zhang, L. (2023): Adaptive learning is suggested in this study for the detection of multichannel ad click deception. Multi-platform behavioral data enhances detection capabilities. The concept of idea drift is taken into account in online learning strategies. Static models are frequently outperformed by experimental results. Fraud detection is advantageous to all forms of advertising. The study determined that adaptable AI models are required to identify all-channel phony advertisements.

Abbas, F., & Hilal, A. (2023): Digital ad click fraud can be identified using a variety of machine learning methods. Utilize shared data to evaluate classical and ensemble classifiers. Performance is evaluated by the F1-score, recall, accuracy, and precision. Ensemble methods enhance generalizability, as indicated by the results. We investigate the advantages and disadvantages of model complexity and detection latency. The results indicate that models that are lightweight and precise are the most suitable for real-time use.

Batool, A., Kim, J., & Byun, Y. C. (2024): We demonstrate an improved deep learning algorithm for the detection of click deception on digital advertising platforms. Complex user behavior is monitored by contemporary feature extraction and attention algorithms. Advanced fraud defenses are fortified by experiments. In accuracy testing, the model surpasses deep learning. Produces advertising solutions that attract significant traffic. Research indicates that attention-based fraud detection is effective.

Chen, X., & Li, Y. (2024): Real-time adversarial reinforcement learning identifies incorrect inputs. Changes in detection policy are contingent upon input and deception. The model outperforms static classifiers in challenging settings, as demonstrated by experimental results.

DOI: https://doi.org/10.5281/zenodo.20487333

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-08***

The architecture strikes an equilibrium between precision and speed. The results indicate that click fraud will persist. Practice with real-time advertisements.

Smith, T. J., & Zhao, Q. (2025): We conducted research on the detection of click fraud using both traditional machine learning and deep learning. We evaluate a huge number of classifiers on extensive online advertising datasets. The results indicate that deep learning algorithms are more effective at detecting intricate fraud. The process of establishing machine learning models is more efficient and straightforward. The investigation evaluates the cost and efficacy of computers. The results assist in the selection of the most effective real-world advertising model.

Oliveira, F., & Silva, M. (2025): Programmatic ad network fake hits are identified by AI-powered deep learning. The model is monitored in terms of the time, location, and manner in which users employ it. Based on my experience, it is both durable and precise, even in the presence of excessive noise. Automated fraud strategies are subject to change as architecture evolves. Advertisers conserve funds through the implementation of early fraud detection. This research demonstrates that deep learning is effective in data-intensive programmatic advertising.

4. RESULTS

Fig 4.1: User Login

Fig 4.2: Registration page

DOI: https://doi.org/10.5281/zenodo.20487333

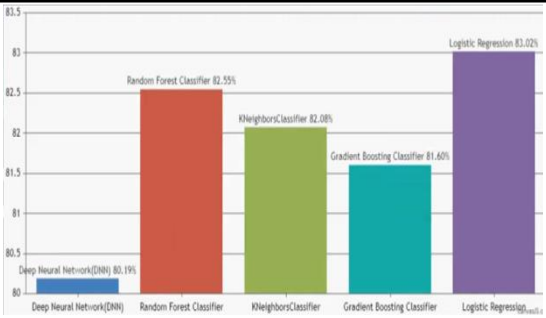

Fig 4.3: Digital Advertising Graph Invalid Click Detection Machine Learning Models

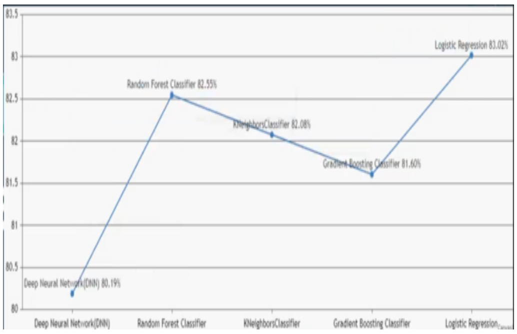

Fig 4.4: Misclick detection trend in machine learning accuracy in a line graph

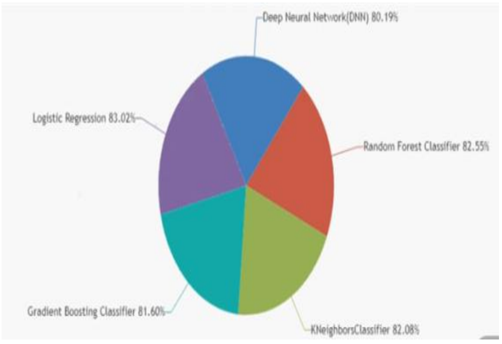

Fig 4.5: Misclassified pie chart machine learning model click detection.

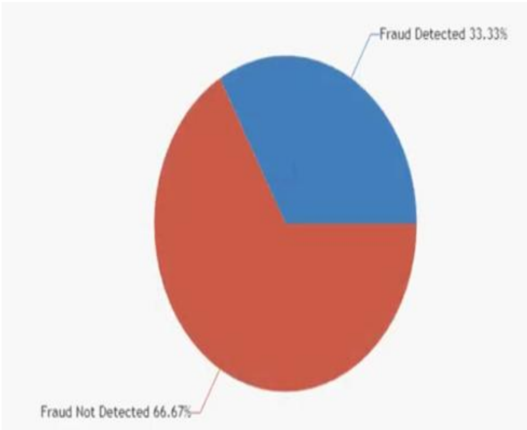

Fig 4.6: Pie chart of detected vs. non-detected invalid clicks

5. CONCLUSION

Artificial intelligence-based click monitoring is essential as click fraud and fraudulent traffic become increasingly complicated. Unlike rule-based techniques, AI-driven models can uncover complex and dynamic fraud trends. Deep learning and machine learning use behavioral, contextual, and temporal data to reduce false positives. Real-time analytics

DOI: https://doi.org/10.5281/zenodo.20487333

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-08***

improve campaign reliability and reduce advertising losses by enabling quick action. Hybrid and ensemble models inhibit hostile and purposeful deception. Explainable AI model decisions increase trust. Data asymmetry, idea dispersion, and privacy limit detection systems despite advances. Online learning and model modification are needed to combat new fraud methods. High-throughput ad systems need powerful processors and potential. Named dataset quality affects model flexibility and efficacy.

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.

DOI: https://doi.org/10.5281/zenodo.20487333