International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

Adaptive Attention-Based Hybrid Deep Learning Framework for Click Fraud Detection in Digital Advertising

Ramissetty Triveni[1], Nagul Shareef Shaik[2]

[1]M. Tech, [2]Assistant Professor, Department of Computer Science and Engineering, MVR College of Engineering & Technology (Autonomous), Paritala, India

***Abstract*-- Click fraud has become a significant challenge in online advertising systems, where fraudulent entities generate invalid clicks to manipulate revenue and distort analytics. Traditional detection approaches rely on static data analysis and conventional machine learning models, which are often ineffective in capturing complex behavioral patterns and temporal dependencies in clickstream data.**

In this paper, an adaptive attention-based hybrid deep learning framework is proposed for accurate click fraud detection. The model integrates Convolutional Neural Networks (CNN) for extracting feature relationships and Long Short-Term Memory (LSTM) networks for modeling sequential click behavior. A self-attention mechanism is incorporated to dynamically identify and prioritize the most relevant features across time steps, improving prediction performance.

The system includes preprocessing techniques such as data encoding, normalization, and feature selection to enhance model efficiency. Experimental evaluation using standard metrics such as accuracy, precision, recall, and F1-score demonstrates that the proposed approach outperforms traditional machine learning and baseline deep learning models. The system is further deployed using a web-based framework to enable real-time fraud detection, making it suitable for practical online advertising environments.

***Keywords*-- Click Fraud Detection, Deep Learning, Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Attention Mechanism, Online Advertising, Feature Selection, Behavioral Analysis, Predictive Modeling**

I. Introduction

Online advertising has become a fundamental component of the digital economy, enabling businesses to reach targeted audiences and optimize marketing strategies. However, the rapid growth of digital advertising platforms has also led to the emergence of fraudulent activities, among which click fraud is one of the most critical challenges. Click fraud occurs when invalid clicks are generated on advertisements, either by automated bots or malicious users, with the intention of increasing revenue unfairly or exhausting competitors' advertising budgets. This results in financial losses and unreliable analytical insights for advertisers.

Traditional click fraud detection systems primarily rely on rule-based approaches and classical machine learning models that analyze features such as IP address, device information, and click frequency.

While these methods can detect basic fraudulent patterns, they are limited in their ability to capture complex and evolving user behavior. In real-world scenarios, clickstream data exhibits temporal characteristics, where user actions occur in sequences over time. Ignoring these temporal dependencies often leads to reduced detection accuracy and increased misclassification.

Recent advancements in deep learning have introduced powerful techniques for modeling complex data patterns. Convolutional Neural Networks (CNN) are effective in extracting meaningful feature representations, while Long Short-Term Memory (LSTM) networks are capable of learning sequential dependencies in time-series data. However, standard deep learning models often treat all input features with equal importance, which may limit their ability to focus on critical patterns associated with fraudulent activity.

To address these challenges, this paper proposes an adaptive attention-based hybrid deep learning framework for click fraud detection. The proposed model combines CNN for spatial feature extraction and LSTM for temporal sequence modeling, while integrating a self-attention mechanism to dynamically identify important features across time steps. By capturing both behavioral patterns and feature relevance, the system aims to improve detection accuracy and robustness.

The remainder of this paper is organized as follows. Section II presents the literature review, Section III discusses the problem statement and objectives, Section IV describes the proposed methodology, Section V presents the results and discussion, and Section VI concludes the paper with future research directions..

II. Literature Review

Click fraud detection has been widely studied in the domains of online advertising and cybersecurity due to its significant financial impact. Early approaches to fraud detection primarily relied on rule-based systems and statistical techniques. These methods used predefined rules based on parameters such as IP address frequency, click intervals, and user activity patterns. Although simple to implement, rule-based systems lack adaptability and are ineffective against evolving fraud strategies.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

With the advancement of machine learning, various classification algorithms such as Decision Trees, Support Vector Machines (SVM), Naive Bayes, and Random Forest were introduced to improve fraud detection accuracy. These models are capable of capturing non-linear relationships within data and have shown better performance compared to traditional methods. Among them, ensemble models like Random Forest gained popularity due to their robustness and reduced overfitting. However, most of these approaches operate on static datasets and fail to consider the sequential nature of clickstream data, which limits their effectiveness in real-world scenarios.

To overcome the limitations of static models, deep learning techniques have been explored for click fraud detection. Artificial Neural Networks (ANN) provided improved feature representation capabilities but lacked the ability to model temporal dependencies explicitly. Recurrent Neural Networks (RNN), particularly Long Short-Term Memory (LSTM) networks, were later introduced to address this issue. LSTM models are well-suited for analyzing sequential data and have demonstrated improved performance in detecting time-dependent fraud patterns. Despite their advantages, standard LSTM models treat all input features equally and do not dynamically identify the most relevant features.

Recent research has focused on integrating attention mechanisms into deep learning models to enhance performance. The attention mechanism enables models to assign weights to input features based on their importance, allowing the system to focus on critical patterns in the data. This approach has been successfully applied in various domains such as natural language processing and financial prediction, and its application in fraud detection has shown promising results.

In addition to model improvements, data preprocessing techniques such as feature selection and normalization play a crucial role in improving model performance. Techniques like Recursive Feature Elimination (RFE) help in identifying the most relevant features, while normalization ensures stable training of deep learning models.

Despite these advancements, many existing systems do not effectively combine spatial feature extraction, temporal modeling, and feature importance within a unified framework. There remains a need for an integrated approach that can capture complex behavioral patterns in clickstream data while improving detection accuracy and robustness.

III. Problem Statement And Objectives

A. Problem Statement

Existing click fraud detection methods primarily rely on static feature analysis and conventional machine learning models, which are insufficient for capturing sequential patterns in user behavior. In practical scenarios, fraudulent activities often occur in the form of repeated or time-dependent click patterns that cannot be effectively detected using traditional approaches.

Another major limitation is that most models treat all input features equally, without considering their relative importance in detecting fraud. This results in reduced model efficiency and lower prediction accuracy. Additionally, click fraud datasets are often imbalanced, where genuine clicks significantly outnumber fraudulent ones, leading to biased model performance and increased misclassification of fraudulent instances.

Due to these challenges, current systems struggle to provide accurate and reliable click fraud detection, especially in dynamic and large-scale advertising environments. Therefore, there is a need for an advanced approach that can model temporal behavior, identify important features, and improve classification performance.

B. Objectives

The primary objective of this research is to develop an intelligent and robust click fraud detection system using hybrid deep learning techniques.

The specific objectives are as follows:

- To model clickstream data as sequential behavior rather than static records
- To utilize Convolutional Neural Networks (CNN) for extracting feature relationships
- To apply Long Short-Term Memory (LSTM) networks for capturing temporal dependencies
- To integrate a self-attention mechanism for identifying important features
- To improve fraud detection accuracy and reduce misclassification
- To develop a system capable of real-time prediction using a web-based framework

IV. Proposed Methodology

A. Dataset and Input Representation

The proposed system is implemented as a practical deep learning-based framework integrated with a web application for real-time click fraud detection.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

The system follows a structured execution flow starting from data input to final prediction output. It combines preprocessing techniques, hybrid deep learning architecture, and deployment using a Flask-based interface.

A. System Execution Workflow

The system operates through a sequential execution process:

1. User provides click-related input through the web interface
2. Input data is received by the Flask backend
3. Data preprocessing is applied to convert input into model format
4. Feature selection is performed using a trained RFE model
5. Processed data is reshaped for model input
6. Data is passed through CNN layers for feature extraction
7. Extracted features are processed by the LSTM layer
8. Attention mechanism assigns importance to features
9. Final prediction is generated by the model
10. Output is displayed to the user

This workflow ensures efficient and real-time fraud detection.

B. Backend Processing

The backend is implemented using Flask and handles all application-level operations. User inputs are collected through HTML forms and include attributes such as IP address, device type, click time, and user activity details. The backend processes the input data and prepares it for model execution.

The trained deep learning model is loaded into the system using TensorFlow/Keras. Input data is converted into the required numerical format and passed through the preprocessing pipeline before being sent to the model for prediction.

C. Data Preprocessing

The input data is preprocessed to ensure compatibility with the model. Categorical features are converted into numerical values using label encoding. Missing values are handled using appropriate statistical methods. Feature scaling is applied using normalization to ensure that all values are within a fixed range, improving model stability and performance.

D. Feature Selection

Recursive Feature Elimination (RFE) is used to select the most relevant features for fraud detection. The method removes less important features based on model importance scores and retains only significant attributes. This reduces dimensionality and improves prediction accuracy.

E. CNN-Based Feature Extraction

The preprocessed data is passed through a Convolutional Neural Network (CNN), which extracts important feature patterns using convolution operations. The CNN layer generates feature maps that capture relationships between input attributes. Activation functions are applied to introduce non-linearity and improve model learning capability.

F. LSTM-Based Temporal Analysis

The output from the CNN layer is passed to the LSTM network. The LSTM model captures temporal dependencies in clickstream data by analyzing sequential patterns. It learns user behavior over time, enabling detection of abnormal click patterns.

G. Attention Mechanism

An attention layer is applied to the LSTM output to assign weights to different features and time steps. This mechanism allows the model to focus on the most relevant information, improving prediction accuracy and model performance.

H. Model Training and Prediction

The model is trained using the binary cross-entropy loss function and optimized using the Adam optimizer. During prediction, the trained model processes input data and produces output using a sigmoid activation function. The final output is classified as:

- 0 → Genuine Click
- 1 → Fraudulent Click

I. Deployment

The trained model is integrated into a Flask-based web application. The system allows users to input data and receive predictions in real time. The output is displayed through the web interface, making the system suitable for practical use in online advertising platforms.

V. Results And Discussion

A. Experimental Setup

The proposed click fraud detection system is implemented using Python with libraries including NumPy, Pandas, Scikit-learn, and TensorFlow/Keras. The user interface is developed using Flask, enabling real-time interaction with the model.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

The dataset is preprocessed using encoding, normalization, and feature selection techniques. The processed data is divided into training and testing sets using an 80:20 ratio. The hybrid CNN–LSTM model with an attention mechanism is trained on the dataset, and its performance is compared with traditional machine learning models such as Naive Bayes and Random Forest, as well as standalone deep learning models.

B. Evaluation Metrics

The performance of the system is evaluated using standard classification metrics:

- *Accuracy:* Measures overall prediction correctness
- *Precision:* Indicates reliability of fraud predictions
- *Recall:* Measures ability to detect fraudulent clicks
- *F1-Score:* Provides balance between precision and recall

These metrics are important for evaluating performance on imbalanced datasets.

C. Performance Comparison

The proposed model is compared with baseline models, and the results are shown below.

Table 1: Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score
Naive Bayes	85%	0.83	0.80	0.81
Random Forest	90%	0.89	0.88	0.88
CNN	92%	0.91	0.90	0.90
CNN–LSTM + Attention	**96%**	**0.95**	**0.94**	**0.94**

The results show that the hybrid model achieves the highest accuracy and better overall performance compared to other models.

D. Confusion Matrix Analysis

The confusion matrix is used to analyze classification performance in detail.

Table 2: Confusion Matrix

	Predicted Genuine	Predicted Fraud
Actual Genuine	500	20
Actual Fraud	15	300

The results indicate that the model correctly classifies most of the instances, with a low number of false positives and false negatives.

E. System Output Analysis

The system is tested using real-time inputs through the Flask interface.

Table 3: System Output Behavior

Input Condition	Output
Normal click pattern	Genuine
Repeated clicks in short time	Fraud
Unusual activity pattern	Fraud
Valid user behavior	Genuine

The system successfully identifies fraudulent and genuine clicks based on input behavior.

F. Discussion

The experimental results demonstrate that the proposed hybrid CNN–LSTM model with attention mechanism significantly improves click fraud detection performance. The CNN layer effectively extracts feature relationships, while the LSTM model captures temporal patterns in click behavior. The attention mechanism further enhances performance by focusing on important features.

Compared to traditional machine learning models, the proposed system shows higher accuracy and better generalization. The integration of preprocessing techniques such as feature selection also contributes to improved efficiency.

The system performs well in real-time scenarios and provides reliable predictions through the web interface. However, the current implementation is based on a static dataset and can be further improved by incorporating real-time streaming data.

VI. Conclusion

This paper presents an attention-enhanced hybrid CNN–LSTM model for click fraud detection in online advertising systems. The proposed approach addresses the limitations of traditional methods by combining spatial feature extraction, temporal sequence modeling, and feature importance evaluation within a unified framework.

The CNN component effectively captures relationships among input features, while the LSTM network models sequential click behavior to identify time-dependent fraud patterns. The integration of a self-attention mechanism further improves performance by enabling the model to focus on the most relevant features. In addition, preprocessing techniques such as encoding, normalization, and feature selection contribute to improved model efficiency and accuracy.

Experimental results demonstrate that the proposed model outperforms conventional machine learning and baseline deep learning approaches in terms of accuracy, precision, recall, and F1-score. The system also shows reliable performance in real-time scenarios when deployed using a Flask-based web interface.

Overall, the proposed framework provides an effective and scalable solution for detecting fraudulent click activities, making it suitable for practical implementation in modern online advertising platforms.

VII. Future Scope

The proposed click fraud detection system can be further enhanced to improve its performance and applicability in real-world environments. One important extension is the integration of real-time streaming data from advertising platforms, which would enable continuous monitoring and dynamic fraud detection instead of relying on static datasets.

The model can also be improved by incorporating advanced deep learning architectures such as transformer-based models, which are capable of capturing long-range dependencies more effectively than traditional LSTM networks. In addition, applying explainable AI techniques can enhance model interpretability by providing insights into the features influencing fraud detection decisions.

Future work may also focus on deploying the system on cloud platforms to support large-scale data processing and improve scalability. Integration with real advertising APIs and analytics systems can further enhance practical usability. Moreover, incorporating adaptive learning mechanisms can allow the model to update itself based on new fraud patterns, ensuring better performance over time.

Overall, these enhancements can transform the current system into a more robust, scalable, and intelligent solution for real-time click fraud detection in evolving online advertising environments.

REFERENCES

[1] A. Metwally, D. Agrawal, and A. El Abbadi, "Detection of Fraudulent Clicks in Pay-Per-Click Advertising," *ACM Transactions on Information Systems*, vol. 25, no. 2, pp. 1–35, 2007.

[2] C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.

[3] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[4] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[5] A. Vaswani et al., "Attention Is All You Need," in *Proceedings of the Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

[6] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[7] I. Guyon and A. Elisseeff, "An Introduction to Variable and Feature Selection," *Journal of Machine Learning Research*, vol. 3, pp. 1157–1182, 2003.

[8] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[9] M. Abadi et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," 2016.

[10] J. Brownlee, "Deep Learning for Time Series Forecasting," Machine Learning Mastery, 2020.

[11] K. Dave, V. Varma, and V. Prasad, "An Efficient Approach for Click Fraud Detection Using Machine Learning Techniques," *International Journal of Computer Applications*, vol. 182, no. 31, pp. 1–6, 2019.

[12] S. Kitts, B. Freed, and M. Vrieze, "Click Fraud Detection and Prevention," *IEEE Security & Privacy*, vol. 4, no. 3, pp. 66–68, 2006.