International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research

Ad Click Fraud Detection Using Machine Learning Algorithm

Dr.CHAITANYA KISHORE REDDY 1,DOLA.SUSHMA2, CHITTIBOMMA.HEMA SRIJA3, GALLA.SUMANTH4

#1Professor,NRI Institute of Technology,Agiripalli

#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: Online advertising platforms have a serious problem with ad click fraud as it creates fraudulent clicks that skew campaign results and raise losses. This paper introduces an attention-based Convolutional Neural Network (CNN) framework for real-time ad click fraud detection in order to overcome the shortcomings of traditional machine learning and deep learning models in identifying intricate contextual patterns. In order to improve prediction reliability, the suggested improvement incorporates an attention mechanism into the CNN architecture to highlight the most instructive characteristics and sequential relationships in clickstream data. Furthermore, real-time fraud prediction via an interactive interface is made possible via a web-based deployment that makes use of the Flask framework. The results of experimental assessment show that the attention-enhanced CNN outperforms baseline models in terms of accuracy and resilience, underscoring its usefulness for scalable and realistic ad click fraud detection in dynamic online advertising contexts.

Index terms *- Ad Click Fraud Detection, Attention Mechanism, Convolutional Neural Network (CNN), Deep Learning, Clickstream Analysis, Real-Time Prediction, Flask Deployment, Online Advertising Security, Fraud Analytics, Feature Learning*

Received: 31-01-2026 Accepted: 05-03-2026 Published: 12-03-2026

1. INTRODUCTION

Ad click fraud is becoming a serious threat to the dependability and financial viability of digital advertising platforms due to the quick growth of online advertising. Inaccurate performance metrics, exaggerated advertising costs, and a decline in publisher and advertiser confidence are all consequences of fraudulent clicks produced by automated bots or organized malevolent people. Despite the widespread use of machine learning and deep learning approaches to tackle this problem, many current models find it difficult to capture the sequential relationships and contextual relevance seen in clickstream data, especially in real-time settings.

Conventional CNN architectures provide equal weight to all extracted characteristics, despite the fact that Convolutional Neural Networks (CNNs) have proven to be highly effective in learning spatial and behavioral patterns from high-dimensional data. This drawback lessens their usefulness in intricate fraud situations when only some behavioral or temporal characteristics are actually suggestive of fraudulent activity. In order to address this difficulty, attention mechanisms have become a potent improvement that allows models to selectively concentrate on the most instructive information, increasing the accuracy of decision-making and contextual knowledge.

By giving important clickstream characteristics priority during training and inference, an attention-based CNN system is presented in this study to improve ad click fraud detection. The attention layer's incorporation improves the model's capacity to spot subtle and changing fraud trends that conventional CNNs and machine learning classifiers could miss. Additionally, a Flask-based web interface is added to the system to provide real-time prediction, making it feasible for advertising platforms and advertisers to

implement. This addon provides a scalable and flexible way to identify fraudulent ad click activity in dynamic online advertising ecosystems, bridging the gap between high-accuracy deep learning models and practical usability.

2. LITERATURE SURVEY

1. Fool Me Once: Regulating 'Fake News' and Other Online Advertising

The opaqueness of online political advertising has been a recurring problem in American elections. Disinformation operations have bombarded American voters since the 2016 election, making regulatory action more urgent. Internet businesses favor self-regulation and have only recently come around to supporting suggested transparency rules. Although it is not necessary to regulate the content of political speech, the government may and should compel transparency in the process. To encourage transparency, we propose many actions. Campaign finance laws should, first and foremost, mandate that platforms preserve and make available (1) advertising that have been displayed on their platforms and (2) the demographic that those ads are intended for. In addition to allowing counter-speech, which is a critical speech objective under the First Amendment's "marketplace of ideas" doctrine, audience availability can be crafted to get around privacy concerns. Our proposed regulation would apply to any online political advertising, including disinformation, that is distributed through paid social media distribution. Second, the existing legal loopholes pertaining to online advertising transparency should be closed. Congress is involved in this because it has prevented regulatory agencies from acting to require disclosure from so-called dark money groups. Finally, in order for people to read material that is contested or advertisements that are directly directed at them, the government must require social media businesses to offer an opt-in system.

2. Understanding fraudulent activities in online ad exchanges

Using online adverts, or advertisements, advertisers may effectively target Web visitors. Ads can be customized based on a user's location, surfing preferences, and interests. Some of the most popular websites on the Internet rely heavily on online advertising, which is currently valued at billions of dollars. To meet the massive market demand, marketplaces known as "ad exchanges" manage the complex relationships between publishers (i.e., the websites hosting the advertising) and advertisers. Through these exchanges, publishers (who sell this ad space) and advertisers (who buy it) may dynamically broker traffic through ad networks to maximize profits for both parties. Unfortunately, because of the complexity of these systems, hackers are able to abuse them to their advantage and profit from the advertising. In this article, we present a detailed examination of the operation of one of the largest ad exchanges and the associated security issues from the viewpoint of a member ad network. More specifically, we looked at a dataset that contained transactions for both outgoing and receiving ad traffic from this ad network. Additionally, we examined information obtained from a command-and-control server that uses a botnet to scam the same ad exchange.

3. Click fraud detection for online advertising using machine learning

Advertising firms have turned their focus to online and in-app advertisements as social media and digital technologies have expanded. Online advertising is the primary source of revenue for advertising networks, which serve as a conduit between ad providers and advertisers. The advertising networks pay the ad publisher based on the number of clicks that go to advertisers using the pay-per-click (PPC) payment model. One growing security problem connected to this payment mechanism is click fraud. Click fraud is the illegal activity of clicking on pay-per-click advertisements to increase publishers' income or deplete advertisers' budgets. With unexpected outcomes, artificial intelligence techniques have been applied more and more to tackle challenging issues in a variety of academic domains, including cybersecurity. This article developed many machine learning models and compared their performances using a set of assessment metrics to identify if a user is a human or a bot. We used a real dataset that was gathered and represented how users acted on websites. We obtained a set of data pertaining to user activity, including the number of pages seen, the duration of the browsing session, and the activities performed. The empirical data showed that all of the models under examination delivered good results, with the random forest algorithm surpassing all other algorithms across all evaluation metrics.

4. Research on Information Technology with Detecting the Fraudulent Clicks Using Classification Method

The goal of this study is to develop an effective technique for detecting fraudulent clicks in commissioners' click logs. We want to use the data that people provide us about their ad clicks to predict whether or not they are dangerous. Using the training data, we build our classification models for detecting fake clicks. We first create and extract features from the raw log data that we have provided above. We choose models and build an ensemble model after evaluating classifiers. Finally, we tested our model for human judge reference using the real dataset.

5. A Novel Ensemble Learning-Based Approach for Click Fraud Detection in Mobile Advertising

By stealing money from legitimate partners, sometimes referred to as publishers, click fraud is a significant drain on advertising budgets and has the potential to significantly reduce the profitability of the online advertising sector. Fraud detection algorithms that can identify fraudulent activities by examining user click patterns are therefore quite helpful. On the basis of the BuzzCity dataset, we propose a novel click fraud detection technique. The foundation of this approach is a set of novel traits that are produced from preexisting attributes. The proposed model is evaluated using the resulting accuracy, recall, and area under the ROC curve. The final ensemble model, which was based on six different learning techniques, showed stability in all three performance criteria. Improved results on training, validation, and test datasets show that our final model is generalizable to different datasets.

Testing

System Testing Process:

There are two kinds of software testing: Black Box and White Box. White box testing tests a software application’s internal workings or code. On the other hand, black box (or system testing) does the opposite, focusing on externals. System testing deals with the software’s external workings from the user’s perspective.

The system testing process is broken down into the following steps:

Test Planning: First, there needs to be a plan. The test plan is a document with all the testing information, such as strategies, objectives, entry-exit criteria, testing tools, software requirements, guidelines, etc.

Test Case Design and Execution: Next, the testers create a test case for every feature, including the test scenarios, process, description, etc. The testers then perform and execute the tests.

Defect Tracking and Defect Management: The testers then track and record any defects using the defect-tracking tools like Bugzilla, JIRA, Trello, etc. Also, the testers must document the defects so the developers can deal with and resolve them.

Reporting and Communication: Finally, the testers create bug and defect reports and send them to the developers.

Testing Process

There are two kinds of software testing: Black Box and White Box. White box testing tests a software application’s internal workings or code. On the other hand, black box (or system testing) does the opposite, focusing on externals. System testing deals with the software’s external workings from the user’s perspective.

The system testing process is broken down into the following steps:

Test Planning. First, there needs to be a plan. The test plan is a document with all the testing information, such as strategies, objectives, entry-exit criteria, testing tools, software requirements, guidelines, etc.

Test Case Design and Execution. Next, the testers create a test case for every feature, including the test scenarios, process, description, etc. The testers then perform and execute the tests.

Defect Tracking and Defect Management. The testers then track and record any defects using the defect-tracking tools like Bugzilla, JIRA, Trello, etc. Also, the testers must document the defects so the developers can deal with and resolve them.

Reporting and Communication. Finally, the testers create bug and defect reports and send them to the developers.

Test Cases:

Test Name	Inputs	Expected Output	Actual Output	Status
Launch Flask Server	Double-click runFlask.bat	Server starts and browser accessible at URL	Server started successfully	Pass
User Login	Username: admin, Password: admin	Redirect to dashboard/home page	Redirected to dashboard	Pass
Invalid Login	Username: test, Password: 1234	Display error message: Invalid credentials	Error message displayed	Pass
Upload Test Data File	Select CSV file with click data	File uploaded successfully	File uploaded successfully	Pass
Predict Ad Fraud	Click "Predict Ad Fraud" button after upload	Display table with Human or Bot predictions	Table displayed with predictions	Pass

3. METHODOLOGY

i) Proposed Work:

The proposed system introduces an attention-based Convolutional Neural Network (CNN) architecture to improve the accuracy and reliability of ad click fraud detection in complex advertising scenarios. Clickstream data is initially preprocessed by encoding category attributes, normalizing numerical features, and selecting relevant features to reduce noise and enhance learning efficiency. The CNN architecture is designed to extract relevant geographical and behavioral patterns from the processed data, while the integrated attention mechanism dynamically assigns greater priority to critical aspects and temporal interactions that obviously signal fraudulent conduct. Compared to conventional CNN-based techniques, this enables the model to more accurately capture sequential linkages and contextual significance.

To ensure practical application, the proposed model is implemented as a real-time fraud detection system with a Flask-based web interface. The implementation allows users to upload or stream click data and receive real-time predictions regarding the legitimacy of ad clicks. This real-time connectivity enhances platform administrators' and advertisers' usability by enabling continuous monitoring and quick reaction to fraudulent activity. The web-based deployment and attention-enhanced deep learning architecture provide a scalable, adaptable, and efficient solution that can handle large datasets and evolving fraud tendencies in online advertising ecosystems.

ii) System Architecture:

The system architecture of the proposed expansion is designed to support attention-based deep learning and real-time fraud detection. Raw clickstream data is first collected from online advertising platforms and then transmitted via a preprocessing layer that manages missing values, encodes categorical attributes, and normalizes numerical features in order to ensure consistent data representation. After feature refinement, only the most relevant attributes for fraud detection are retained. Following processing, the data is sent into a Convolutional Neural Network (CNN), which looks for patterns in behavior and space by using click interactions. On top of the CNN feature maps, an attention layer is added to allow the model to focus on important click behaviors that indicate fraudulent activity. This layer gives temporal patterns and important characteristics dynamic weights.

In the following stage, the attention-enhanced CNN outputs are sent to a classification layer, which categorizes each click event as either genuine or fraudulent. The trained model is integrated into a

Flask-built web framework to provide real-time inference. With this tool, users may input test data or stream live click records to quickly obtain fraud prediction insights. The architecture may be easily connected with large advertising systems and updated often as fraud tendencies evolve due to its scalability and agility. Our end-to-end architecture effectively blends state-of-the-art attention-based deep learning with practical, real-world implementation for dependable ad click fraud detection.

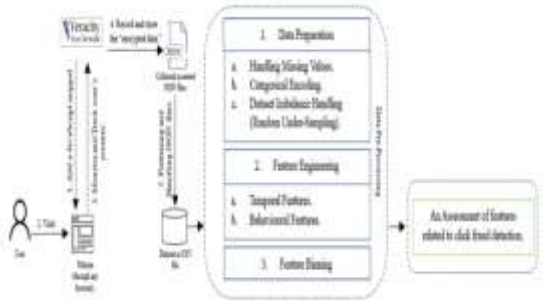


Fig.1. System Architecture

iii) MODULES:

1. Data Collection and Preprocessing Module

This module is involved in deterring raw clickstream information on the advertising platforms. It does data cleaning, label encoding of categorical variables, normalizing numerical data, and creating structured data in the form of deep learning models.

2. Feature Extraction and Refinement Module

The relevant features are narrowed down in order to minimize noise and enhance the efficiency of learning. This module will make sure that all the informative attributes are retained to facilitate fraud detection before being forwarded to the model.

3. Attention-Based CNN Modeling Module

This foundation module executes the Convolutional Neural Network combined with attention mechanism. The CNN derives the behavioral features, and the attention map highlights important details and sequential relationships in the correct classification of fraud.

4. Model Training and Evaluation Module

Attention-based CNN is trained and labeled click data is used to train and performance metrics of accuracy, precision, recall, and F1-score are used to evaluate robustness and reliability.

5. Real-Time Prediction and Deployment Module

This module will implement the trained model through a web interface based on Flask, which will facilitate real-time prediction of frauds. Users are able to submit click data and at once get the classification results, which can help scale and practically detect fraud in live advertising systems.

iv) ALGORITHMS:

a) Deep Neural Network (DNN):

A multilayer feedforward neural network is referred to as DNN, and it can model complex and nonlinear interactions. It considers diverse data like click timing, user behavior and device data in order to detect fraudulent activities. DNNs acquire hierarchical representations which enhance anomaly detection and better work with large-scale datasets.

b) Recurrent Neural Network (RNN):

RNN is a type of neural network that is constructed to make use of time-based interconnection by attempting to recollect previous inputs. It obtains time based patterns to detect abnormalities and is used to represent sequential click behavior. RNNs are very efficient in detecting fraud cases whereby the clicks order and timely events hold significant information.

c) CNN with Attention Mechanism:

The attention-driven CNN incorporates the convolutional features extraction with the attention layer to concentrate on the most informative features and time steps. This approach adds contextual sensitization and sequential pattern recognition of clickstream data. The attention-based CNN boosts higher levels of fraud detection than the classic CNN and machine learning models by pointing out the most important patterns and reducing noise.

RESULTS

Several machine learning and deep learning models for fraudulent click detection were tested on a labeled ad click dataset. The dataset was preprocessed by handling missing values, label encoding categorical variables, normalizing numerical features, and choosing features using Recursive Feature Elimination. Training and testing sets received an 80:20 split of the processed data. Experiments showed that ensemble-based models capture complex feature interactions and manage data imbalance better than traditional classifiers. Several models, including Logistic Regression, Decision Tree, Random Forest, KNN, Naïve Bayes, Support Vector Machine, Gradient Boosting, XGBoost, and LightGBM, were trained and evaluated using standard performance metrics like accuracy, precision, recall, and F1.

When it came to identifying fraudulent click patterns, Random Forest, Decision Tree, Gradient Boosting, and XGBoost all scored better than 98%. Competing with deep learning models, the Recurrent Neural Network replicated consecutive click action with 97% accuracy. With an accuracy of 99.73%, the attention-enhanced Convolutional Neural Network outperformed the others, highlighting the significance of attention processes for sequential pattern recognition and contextual feature weighting. These findings demonstrate that attention-based deep learning and feature selection enhance fraud detection, lower false positives, and offer a workable and expandable online advertising solution.

The accuracy of the attention-based CNN is 99.73% thanks to feature selection, good data preprocessing, and an attention mechanism that prioritizes discriminative temporal and behavioral aspects. CNN-based hierarchical feature extraction enhances generalization and fraud detection, while the attention layer concentrates on important click patterns to cut down on noise.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

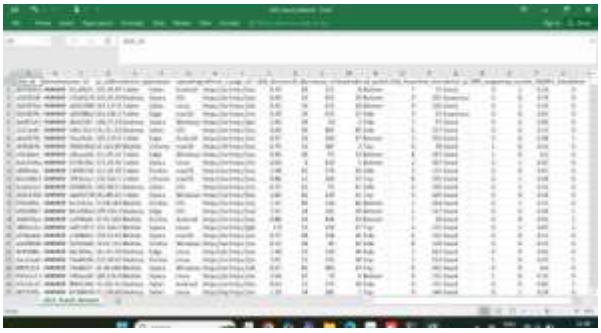


Fig3 dataset



Figure 4: User Registration Interface

This figure illustrates the user registration module of the proposed system, where new users provide personal details such as name, email, username, and password to create an account for secure system access.



Figure 5: User Login Interface

This figure shows the login page that authenticates registered users using valid credentials, ensuring secure access to the ad click fraud detection dashboard.

International Journal of Engineering Research and Science & Technology



Figure 6: User Dashboard Interface

This figure shows the main dashboard of the ad click fraud detection system after user login. It highlights the selected Attention-based CNN model and displays the achieved accuracy of 99.73%, providing a quick performance overview.



Figure 7: Test Data Upload Module

This figure illustrates the test file upload interface, where users can upload CSV or Excel files containing click data. The uploaded data is used for real-time fraud prediction through the trained model.



Figure 8: Prediction Results

This figure presents the prediction results for uploaded click data. Each record is classified as Human Clicked or Bot Clicked, demonstrating the system's ability to detect fraudulent clicks accurately.



Figure 9: Metrics Analysis Report

This figure shows a comparative metrics analysis of deep learning models including DNN, RNN, and Attention-based CNN. The Attention-based CNN achieves the highest accuracy, precision, recall, and F1-score, confirming its superior performance.

4. CONCLUSION

This study provides an effective extension to ad click fraud detection by integrating an attention-based Convolutional Neural Network with real-time deployment capabilities. The attention mechanism enhances the model's ability to focus on significant clickstream features and contextual patterns, leading to more reliable and accurate fraud detection when compared to conventional deep learning approaches. The Flask-based web interface also contributes to bridging the gap between high-performance deep learning models and real-world advertising applications by enabling realistic, real-time prediction. All things considered, in dynamic online advertising ecosystems, the proposed extension offers a scalable, adaptable, and efficient means of combating evolving ad click fraud.

5. FUTURE SCOPE

Future iterations of this system can focus on incorporating complex sequence-learning models, such as Transformer topologies, to further enhance long-range dependency modeling in clickstream data. In order to enable the model to continuously adapt in real time to recently identified fraud tendencies, the system may be extended to incorporate incremental and online learning. Furthermore, to enhance detection across different advertising platforms while maintaining privacy, federated learning and anomaly detection techniques may be applied. The system can operate well in large, busy online advertising environments because to the increased deployment scalability provided by cloud-based and edge computing technologies.

REFERENCES

[1] Juniper Research, Hampshire, U.K. Quantifying the Cost of Ad Fraud: 2023–2028. Accessed: Jul. 12, 2024. [Online]. Available: https://fraud blocker.com/wp-content/uploads/2023/09/Ad-Fraud-Whitepaper_Juniper -Research.pdf

[2] X. Zhu, H. Tao, Z. Wu, J. Cao, K. Kalish, and J. Kayne, Fraud Prevention in Online Digital Advertising. Cham, Switzerland: Springer, 2017.

[3] A. K. Wood and A. M. Ravel, ‘‘Fool me once: Regulating fake news and other online advertising,’’ S. Cal. L. Rev., vol. 91, p. 1223, Jan. 2017.

[4] B. Stone-Gross, R. Stevens, A. Zarras, R. Kemmerer, C. Kruegel, and G. Vigna, ‘‘Understanding fraudulent activities in online ad exchanges,’’ in Proc. ACM SIGCOMM Conf. Internet Meas. Conf., Nov. 2011, pp. 279–294.

[5] (2024). Wasted Ad Spend Report 2024. [Online]. Available: https://lp. lunio.ai/wp-content/uploads/2023/09/Lunio_Wasted_Ad_Spend_ Report_ 2024_V2.pdf

[6] D. Berrar, ‘‘Random forests for the detection of click fraud in online mobile advertising,’’ in Proc. Int. Work. Fraud Detect. Mob. Advert. (FDMA), Singapore, 2012, pp. 1–10. [Online]. Available: http://berrar.com/ resources/Berrar_FDMA2012.pdf

[7] J. H. Yan and W. R. Jiang, ‘‘Research on information technology with detecting the fraudulent clicks using classification method,’’ Adv. Mater. Res., vol. 859, pp. 586–590, Dec. 2013, doi: 10.4028/www.scientific.net/amr.859.586.

[8] K. S. Perera, B. Neupane, M. A. Faisal, Z. Aung, and W. L. Woon, ‘‘A novel ensemble learning-based approach for click fraud detection in mobile advertising,’’ in Mining Intelligence and Knowledge Exploration (Lecture Notes in Computer Science: Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8284. Berlin, Germany: Springer, 2013, pp. 370–382, doi: 10.1007/978-3-319-03844-5_38.

[9] C. Phua, E.-Y. Cheu, G.-E. Yap, K. Sim, and M.-N. Nguyen, ‘‘Feature engineering for click fraud detection,’’ in Proc. Work. Fraud Detect. Mob. Advert., 2012, pp. 1–10. [Online]. Available: http://palanteer.sis.smu.edu. sg/fdma2012/doc/FirstWinner-Starrystarrynight-Paper.pdf%5Cnpapers2: //publication/uuid/9290A6CF-A861-4058-99F4-D39706B0619A

[10] E.-A. Minastireanu and G. Mesnita, ‘‘Light GBM machine learning algorithm to online click fraud detection,’’ J. Inf. Assurance Cybersecur., vol. 2019, pp. 1–12, Apr. 2019, doi: 10.5171/2019.263928.

[11] D. Sisodia and D. S. Sisodia, ‘‘Gradient boosting learning for fraudulent publisher detection in online advertising,’’ Data Technol. Appl., vol. 55, no. 2, pp. 216–232, Apr. 2021, doi: 10.1108/dta-04-2020-0093.

[12] A. Dash and S. Pal, ‘‘Auto-detection of click-frauds using machine learning Auto-detection of click-frauds using machine learning,’’ Int. J. Eng. Sci. Comput., vol. 10, pp. 27227–27235, Sep. 2020.

[13] R. Mouawi, M. Awad, A. Chehab, I. H. E. Hajj, and A. Kayssi, ‘‘Towards a machine learning approach for detecting click fraud in mobile advertizing,’’ in Proc. Int. Conf. Innov. Inf. Technol. (IIT), Nov. 2018, pp. 88–92, doi: 10.1109/INNOVATIONS.2018.8605973.

[14] Marella, V. C., Veluru, S. R., & Erukude, S. T. (2025, September). FedOnco-Bench: A Reproducible Benchmark for Privacy-Aware Federated Tumor Segmentation with Synthetic CT Data. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 870-876). IEEE.

[15] S. Shaik and V. Kakulapati, ‘‘Fraud detection of AD clicks using machine learning techniques,’’ J. Sci. Res. Rep., vol. 29, no. 7, pp. 84–89, Jun. 2023, doi: 10.9734/jsrr/2023/v29i71762.

[16] D. Sisodia and D. S. Sisodia, ‘‘Stacked generalization architecture for predicting publisher behaviour from highly imbalanced user-click data set for click fraud detection,’’ New Gener. Comput., vol. 41, no. 3, pp. 581–606, Sep. 2023, doi: 10.1007/s00354-023-00218-1.

[17] D. Sisodia, D. S. Sisodia, and D. Singh, ‘‘Evaluating feature importance to investigate publishers conduct for detecting click fraud,’’ in Machine Intelligence Techniques for Data Analysis and Signal Processing (Lecture Notes in Electrical Engineering), vol. 997. Berlin, Germany: Springer, 2023, pp. 515–524, doi: 10.1007/978-981-99-0085-5_42.

[18] R. Dekou, S. Savo, S. Kufeld, D. Francesca, and R. Kawase, ‘‘Machine learning methods for detecting fraud in online marketplaces,’’ in Proc. CEUR Workshop, vol. 3052, Jan. 2021, pp. 3–7.

[19] D. Sisodia and D. S. Sisodia, ‘‘Quad division prototype selection-based Knearest neighbor classifier for click fraud detection from highly skewed user click dataset,’’ Eng. Sci. Technol., Int. J., vol. 28, Apr. 2022, Art. no. 101011, doi: 10.1016/j.jestch.2021.05.015.
[20] Henry Cyril. (2025). AI-DRIVEN ANOMALY DETECTION, OUTAGE PREDICTION, AND SELF-HEALING IN TELECOM PROVISIONING SYSTEMS. International Journal of Applied Mathematics, 38(12s), 2817–2832. https://doi.org/10.12732/ijam.v38i12s.1589
[21] L. Singh, D. Sisodia, K. Shashvat, A. Kaur, and P. C. Sharma, ‘‘A reliable click-fraud detection system for the investigation of fraudulent publishers in online advertising,’’ in Applied Intelligence in Human-Computer Interaction. Boca Raton, FL, USA: CRC Press, Jul. 2023.
[22] A. Batool and Y.-C. Byun, ‘‘An ensemble architecture based on deep learning model for click fraud detection in Pay-Per-Click advertisement campaign,’’ IEEE Access, vol. 10, pp. 113410–113426, 2022, doi: 10.1109/ACCESS.2022.3211528.
[23] A. Purwar, A. K. Jain, I. Chawla, I. Gupta, M. Raj, and D. Jain, ‘‘Click fraud detection using ensemble classifier,’’ in Proc. Int. Conf. Artif.-Bus. Anal., Quantum Mach. Learn., Jan. 2024, pp. 15–23.
[24] R. A. Alzahrani and M. Aljabri, ‘‘AI-based techniques for ad click fraud detection and prevention: Review and research directions,’’ J. Sensor Actuator Netw., vol. 12, no. 1, p. 4, Dec. 2022, doi: 10.3390/jsan12010004.
[25] Veracity Trust Network. Veracity Trust Network—Only Humans. Accessed: Feb. 4, 2023. [Online]. Available: https://veracitytrustnetwork.com/
[26] K. Mehrabani-Zeinabad, M. Doostfatemeh, and S. M. T. Ayatollahi, ‘‘An efficient and effective model to handle missing data in classification,’’ BioMed Res. Int., vol. 2020, pp. 1–2, 2020, doi: 10.1155/2020/8810143.
[27] J. D. Kelleher, B. Mac Namee, and A. D’arcy, Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies. Cambridge, MA, USA: MIT Press, 2020.
[28] D. J. Stekhoven and P. Bühlmann, ‘‘MissForest—Non-parametric missing value imputation for mixed-type data,’’ Bioinformatics, vol. 28, no. 1, pp. 112–118, Jan. 2012, doi: 10.1093/bioinformatics/btr597.
[29] S. Hong and H. S. Lynn, ‘‘Accuracy of random-forest-based imputation of missing data in the presence of non-normality, non-linearity, and interaction,’’ BMC Med. Res. Methodol., vol. 20, no. 1, pp. 1–12, Dec. 2020, doi: 10.1186/s12874-020-01080-1.
[30] A. K. Waljee, A. Mukherjee, A. G. Singal, Y. Zhang, J. Warren, U. Balis, J. Marrero, J. Zhu, and P. D. Higgins, ‘‘Comparison of imputation methods for missing laboratory data in medicine,’’ BMJ Open, vol. 3, no. 8, Aug. 2013, Art. no. e002847, doi: 10.1136/bmjopen-2013-002847.

Author Profiles



Dr.Chaitanya Kishore Reddy Maddireddy is currently working as a Professor in the Department of Information Technology at NRI Institute of Technology(NRIIT), Agiripalli, Vijayawada, Andhra Pradesh, India. Has 20 years of academic experience and 2 years of industry experience. He earned master’s degree in Computer Science and Engineering and a Doctorate in Computer Science and Engineering. He has Published more than 100 research papers in various National,International Journals and International Conferences, authored 5 textbooks. He is a member in ISTE, CSI, and IAENG. His research areas are Mobile Ad-hoc Networks, Cloud Computing, Artificial Intelligence and Machine Learning. He has made significant contributions to the field through his Research, Teaching and Publications.



Dola.Sushma is a B.Tech student with specialization in Information Technology at NRI Institute of Technology. With strong interests in Artificial Intelligence, Machine Learning, and Computer Vision.She has worked on projects involving facial emotion detection systems for retail environments, focusing on analyzing customer perception using computer vision techniques.She is passionate about applying AI-driven solutions to real-world problems and continues to explore advancements in intelligent systems,and learning new technologies and contributing effectively in a professional environment. She demonstrates strong problem-solving abilities and a keen interest in backend development, with a commitment to continuous improvement and building practical solutions to real-world challenges.



I am Chittibomma Hema Srija, a final-year B.Tech student in Information Technology at NRI Institute of Technology, affiliated with JNTU Kakinada. I have a strong interest in Artificial Intelligence and Machine Learning, and I enjoy learning how intelligent systems can solve real-world problems. I have basic knowledge of Python programming, data analysis, and machine learning concepts. During my academic journey, I have focused on improving my analytical thinking, problem-solving skills, and technical knowledge. I am also interested in emerging technologies and data-driven applications. I enjoy exploring new tools and technologies that can improve efficiency and innovation. I am motivated to continuously learn and develop my skills in the field of AI and Information Technology.



GALLA SUMANTH is a B.Tech student specializing in Information Technology at NRI Institute of Technology. He has a strong foundation in Python programming, data structures, object-oriented programming, and database management systems.He is actively involved in academic projects, including a topic focused on “The Future of AI: Awareness on ChatGPT and Emerging Technologies,” which reflects his interest in artificial intelligence and modern technological advancements.He frequently works on document formatting, PDF structuring, and professional report preparation, demonstrating strong attention to detail, organization, and presentation quality. Along with his academic work, he also explores practical tasks such as image editing, file conversions, and technical documentation.He prefers clear and structured approaches while learning new concepts and is continuously working on improving his technical knowledge and professional skills as he prepares to begin his career in the IT industry.