ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 2 Issue 2, June 2022 / Page No: 125-134
Paper Id: JETA-V2I2P114 / Doi: 10.56472/25832646/JETA-V2I2P114

Original Article

Navigating Ad Fraud in the Age of AI: Techniques for Detection and Prevention in Programmatic Advertising

Ankush Singhal
Software Development Manager, Amazon, USA.

Abstract: *Advertiser fraud is a significant risk factor for the advertising industry, especially for programmatic advertising, since bidding and automation make it possible for fraudsters to manipulate the system quickly without being noticed. These activities include clicking fraud, bot traffic, and domain spoofing, which results in cash losses and affects ROI by channeling the advertisement budget towards fake impressions or fake clicks that do not provide for the traffic from the target audience. Programmatic ad technologies and ad fraud have advanced, with IP blocking and manual approaches inadequate in dealing with its scale and velocity. This position has made the advertising industry need to develop more sophisticated, preventive measures to identify fraud in actual operations. Due to ad fraud, AI has proved valuable when it comes to identifying some of the significant outliers that would have been hard to decipher among the huge amounts of data. Employing ML and deep learning models, these AI tools can scrutinize identification data from many users and analyze performance parameters of campaigns in real-time, looking for emergent signs of fraud. Approaches such as anomaly detection, supervised learning, unsupervised learning, and neural networks improve the accuracy of ad fraud detection and corroborate itself to new forms of fraud. Exploring how these techniques may be used to protect digital ad campaigns, this paper overviews present-day research on programmatic ad fraud detection and provides prevention methods. The conclusions made reemphasize the ability of AI to cut down ad fraud, thus protecting the advertisers' funds and improving the entire legitimacy of the digital advertising space.*

Keywords: *Ad Fraud, Artificial Intelligence, Programmatic Advertising, Machine Learning, Fraud Detection, Anomaly Detection, Bot Traffic, Click Fraud.*

I. INTRODUCTION

Programmatic advertising is one of the defining trends in the fast-growing digital advertising space since it has made advertising brand communication newsworthy by making the ad buying, targeting, and optimization factors significantly more efficient. That being said, although technological advancement benefits all of us, it has also brought a horrific increase in ad fraud. [1-4] Fraudsters are currently using more complex methods, which enable them to harm advertisers and publishers by exploiting different forms of automation. This introduction explains the origins of programmatic advertising, the development of ad fraud issues, and how artificial intelligence performs these changes.

A. Overview of Programmatic Advertising

Programmatic advertising is a digital method of purchasing advertising in a systematic way in real-time with the use of machine learning. Unlike conventional advertising media buying, where transactions are negotiated, prices are agreed on and are often fixed, programmatic advertising applies Real-Time Bidding (RTB). RTB helps target and let advertisers bid in real-time per individual ad impression to the intended audience. Automated advertising systems focus on huge amounts of data to reach intended demographic, geographic, interest and behavioral categories using approximate computing, making adverts efficient with little or no human control. Due to this, programmatic advertising can work at a level of billions of impressions across websites, applications, and social media, making it critical for brands that want to get optimal ROIs and effectively target their audience. However, this efficiency opens the way for vulnerabilities in programmatic advertising, such as automating transactions and creating multiple layers of bidding.

B. The Ad Fraud Landscape

Ad fraud is a complex phenomenon that refers to a number of schemes with the single common purpose of increasing advertising expenditures while providing minimal returns to advertisers. Common types of ad fraud include:

- Click Fraud: A campaign whose main motive is to generate fake traffic to an ad through click-through bots or click-through farms to build revenue for websites and publishers.

- Bot Traffic: One of the major types of unsolicited traffic, namely bot traffic, may engage with an advertisement just as a figure without any possibility of conversion.
- Domain Spoofing: They masquerade their poor quality sites as that of high quality, whereby they are able to con advertisers and bankrupt their advertising budgets.
- Pixel Stuffing and Ad Stacking: Some of them include placing several advertisements in one pixel or placing one advertisement over the other with the aim of getting fake impressions.

These techniques are noisy, and digital advertising fraud globally is estimated to be above $6.5 billion per annum. Besides, General ad fraud has deleterious effects on the overall brand reputation and is a blow to client trust in the digital advertising marketplace. As a result, the identification and mitigation of such scams have garnered much attention in the market, especially with programmatic space evolving.

C. The Participation of Artificial Intelligence to Ad Fraud Prevention

AI has become an important weapon against ad fraud in recent years, mostly because of its capacity to process and understand large amounts of data immediately. Artificial intelligence in an organization's operations involves information system capabilities where the ML and deep learning algorithms analyze user interactions, recognize complex syndromes of fraud, and subsequent reporting. While the conventional rule-based systems approach makes it difficult to respond to new forms of fraud on the fly because they are rigid and do not grow wiser as the fraudsters come up with new tricks, an AI system can learn from new data over time.

- Machine Learning (ML): Thus, through the use of data mining technology, the ML models get to learn normality, and this points to features that may be symptomatic of fraud. For instance, click patterns, origins of traffic, and user activity that is rather suspicious are underlined as potential signs to look for.
- Deep Learning: Most deep learning models prefer Convolutional Neural Networks (CNNs) and recurrent neural networks (RNNs) suitable for identifying complex patterns and sophisticated anomalies found in large datasets, which are crucial in detecting sophisticated fraud schemes.
- Anomaly Detection: Machine learning is used most effectively in the unsupervised learning model to detect odd patterns such as increased traffic rates or click-through rates deemed to depict fraud.

By way of these technologies, AI can facilitate live fraud identification and minimization, thus decreasing the advertisers' exposure to financial risk and maintaining the probity of the programmatic mechanisms. As the schemes progress and become even more challenging, detecting opportunistic ad fraud is critical for AI's ability to continually adapt and learn.

II. LITERATURE REVIEW

The following section outlines previous and current ad fraud detection approaches from literature with categorizations such as rule-based, machine learning, deep learning and anomaly detection. [5-8] within each category, each technique will represent a step up in terms of the capabilities of ad fraud detection, embodying the evolving nature of ad fraud as a problem.

A. Traditional Ad Fraud Detection Techniques

Old approaches to ad fraud identification were based on static rules, machine learning techniques, and IP blocking. Conventional rule-based systems for detection work in a way where there is a set of rules or limits that have to be cross-checked to detect suspicious activity. For example, rules may be set to alert when the number of clicks in a given period or from a single IP address is above the expected level or when traffic comes from sources far from the target market. Just like any other blacklist, IP blacklisting entails performing a list compiled comprehensively of the IP that is either confident or linked to a number of espionage; an IP is prevented from using the advertising platforms.

However, although these methods proved very helpful initially, they are not very flexible enough to meet changes that infest today's programmatic advertising ecosystem. However, apparent problems with rule-based systems mainly stem from their dependency on simplistic criteria, and therefore, they cannot understand complex fraud strategies that reduce dependence on simple rules. For instance, botnets are now designed to behave in a certain manner; therefore, basic measures such as rules cannot be used. IP blacklisting exercise is also not very effective since fraudsters change their IP addresses or adapt to IP spoofing. For this reason, these conventional ad fraud detection methods are somewhat restrictive, creating the need for modern approaches that can learn and evolve.

B. Machine Learning for Fraud Detection

Another approach that has become widely used recently because of ML in ad fraud detection is that systems learn from data and improve without the programmer's intervention. Recent research shows several popular algorithms incorporated in ad fraud, including decision trees, Support Vector Machines (SVMs), ensemble models, random forests, and gradient boosting.

- Decision Trees: Decision trees are decision-based structures that help classify data based on different descriptors. For example, they can arrange ad interactions of users as fraudulent or genuine using attributes such as how often the ad was clicked by the user, geographical region, and information about a device the user uses. , decision trees are quite suitable for binary classification tasks but may overfit; as such, the use of ensemble methods.
- Support Vector Machines (SVMs): SVMs are a type of network model of supervised learning used to classify the given input data as fraud or genuine traffic by constructing a 'hyperplane' in what is normally a high-dimensional space. ARAMS and other SVM variants are very effective for detecting fraudulent behavior if the analyzed dataset has high similarity in the set of features since these methods provide a clear separation between the groups of fraudulent and legitimate behavior.
- Ensemble Models (e.g., Random Forests): Both random forests and gradient boosting have many decision trees to increase the chances of accurate classification. These ensemble techniques involve analysis of a number of variables and the capability to manage big data, an essential factor in programmatic advertising with huge data on ad interactions.

Machine learning models can take past ad interaction data to check which patterns are normally linked to corrupt practices or likely to generate fake clicks, clicking time, and repeated clicks from devices or locations. Instead of using rules, these models adapt to new models of fraudsters' actions based on data, thus making them more sustainable and scalable.

C. Deep Learning Approaches

CNN and RNN have proved more effective in detecting ad fraud patterns, and deep learning, in general, has been observed to be highly effective. High-dimensional data can be handled well by deep learning models and is so common in programmatic advertising, where data volume and complexity are relatively high.

a) Convolutional Neural Networks (CNNs):

Also known as Convolutional Neural Networks, CNNs were popularized for fraud detection because they could draw spatial pyramids in data. In the case of detecting ad frauds, CNNs can work for time-series data analysis with the help of clickstream data to identify periodical or anomalous patterns of activity-provoking bots or automatized click signals. CNNs are, therefore, very useful on high-dimensional datasets in which a standard ML model would perform poorly.

b) Recurrent Neural Networks (RNNs):

RNNs are used for sequential data analysis and, therefore, are effective when analyzing fraud patterns over a given period. It allows them to receive and analyze data in terms of temporal patterns, which, in turn, represent previous interactions between an advert and its audience. For example, a specific type of RNN can track click sequences and determine which ones are potentially being performed by a bot. Sequential information processing is accomplished using Relative RNN for the current moment and Long Short Term Memory (LSTM), giving the opportunity to reveal long-term dependencies of time series data, which, as a result, would, in turn, reveal complex fraudulent actions in a more detailed manner over an extensive period of time.

The research shows that using deep learning models raises the detection of bot activity and click fraud, and CNNs and RNNs show better accuracy than traditional ML in distinguishing complicated patterns. Neural networks, on the other hand, are computationally intensive and may over-succumb to issues of complexity while being implemented and deployed in a real environment.

D. Anomaly detection techniques

Ad fraud detection has now increasingly adopted anomaly detection techniques as a core means to identify such unusual behaviours that are not frequently observed. [9,10] Generally, AD works under unsupervised learning as anomaly detection does not depend on labeled data, which is beneficial for integrating the algorithm into unstable and constantly changing conditions.

- Autoencoders: Autoencoders are a special type of neural networks that try to reconstruct input data and define distortions as outliers. They come in handy in fraud detection because the algorithm is trained in conventional data; therefore, if an input is fraudulent, reconstructing it will yield a high reconstruction error.
- Clustering Algorithms (e.g., K-means): Cluster analysis techniques sort or segregate it in a way that the system can capture data points that do not belong to any cluster. This means that in ad fraud detection, clustering algorithms can be

further applied to identify or mark down various ad interactions that go against normal user behaviors, such as high click rates by specific IP ranges or erratic engagement figures.

- Isolation Forests: Unlike profiling normal data, this technique separates these into distinct groups with the intention of identifying outliers. It does this by partitioning data randomly; an anomaly will often, for example, end up in very few of the partitions. Isolation Forests are very useful for discovering insignificant fraud activities, such as sudden influxes of traffic from unfamiliar sources or sudden changes in click-through rates.

Specifically, we studied these unsupervised anomaly detection techniques that are important in real-time fraud detection because timely response is highly effective. Thus, by reading out abnormal values, anomaly detection systems can give actual time notifications and enable actions that reduce fraud's effect on advertising campaigns. This amplifies the detection abilities of the ML and deep learning models where normal and standard patterns may conceal a number of fractions of fraud that anomaly detection is capable of identifying.

In general, the literature suggests that whereas conventional approaches were useful in fraud detection, there is a need to move to other sophisticated techniques in the fight against today's intricate ad fraud. Machine learning, deep learning, and anomaly detection, individually and as a combination, collectively form a strong model against detecting and eliminating ad fraud in programmatic advertising. These techniques are applied jointly, so they form the flexible, reactive approach important to properly detecting ad fraud.

E. Use Cases of AI in Programmatic Advertising

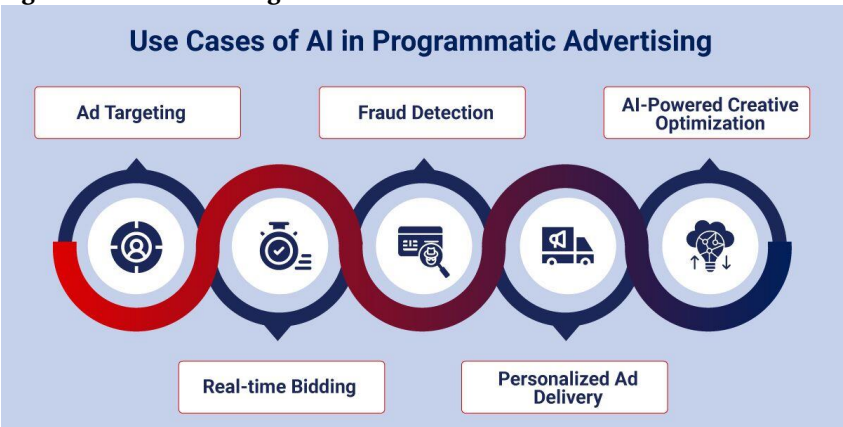

Figure 1: Use Cases of AI in Programmatic Advertising

As displayed in this image, AI applies to five important areas of programmatic advertising. [11] Here's a breakdown of each component from left to right:

- Ad Targeting: AI improves the effectiveness of promoted content owing to the execution of user data and identification of patterns and preferences for served advertisement content. This is helpful, especially when the advertisers get to target the right audience, hence getting the correct information that will actually make people interact and possibly buy the product.
- Real-time Bidding: RTB is solved by AI by effectively sifting through several tables of data to determine which ad space to bid on. This makes it possible for advertisers to bid in real-time for the most valuable impression of the dollar while reducing their budget.
- Fraud Detection: Ad fraud refers to actions like click fraud and bot traffic, and models that employ artificial intelligence work to mitigate them. Looking at various characteristics of data, AI can determine that some activities are likely fraudulent and, therefore, assist the advertiser in not spending their money on getting fake direct impressions.
- Personalized Ad Delivery: AI also provides capabilities to place advertising in front of users interested in the concept and provide better engagement than the random logos of website visitors. The case is particularly great for its individualized delivery, which creates better user experiences and more conversions.
- AI-Powered Creative Optimization: AI plays a role in enhancing the actual ads where the advertiser gets guided on what to change from images to texts to even the adverts' posting time. This continuous optimization makes ad content more appealing and relevant to the audience, making the campaigns more effective.

Each use case is illustrated with an icon showing how AI enhances programmatic advertising in various areas for increased efficacy and accuracy.

III. METHODOLOGY

This paper discusses the approach and approach utilized in identifying ad fraud in programmatic advertising, from data acquisition and data preprocessing to model identification, system design and metrics used for evaluation. This study uses the advanced detection system under the AI umbrella with machine learning, natural language processing and deep learning. [12-16] Machine learning and strategies of deep learning and anomaly detection are planned to work with large data flows and ensure required levels of faked transaction detection, taking into account minimal rates of false positives.

A. Data Gathering and Data Cleaning

Credible data acquisition and preparation form the basic foundation of any strong ad fraud detection program. In this research, data is collected from a DSP, an advertising technology that manages ad inventory buying in real-time. Log files, information about ad click-through rates, users' actions and ad exposure impressions are also provided within millions of records to give them insight into ad conversion.

a) Specific details of the dataset include:

- Scope: This has records of more than 10 million impressions, clicks, conversion, session time, location of the user and the type of devices.
- Anonymization: To enhance user data privacy, PII is masked, and records are disguised.
- Metrics Collected: These indicators include click-through rate, conversion rate, bounce rate, length of engagement, and so on, which are the statistics widely used in measuring ads and identifying the conspicuous.

b) To prepare the data for machine learning model training, several preprocessing steps are undertaken:

- Data Cleaning: Invalid values are excluded, values are preprocessed, and noisy, incomplete data is either imputed or dropped.
- Normalization: Features are scaled to a common range so that all of the weights or contributions are equivalent to that of another, which improves deep learning models.
- Feature Engineering: New features are defined based on available data as extended parameters, e.g., average user sessions and the time spent on every page.

Fraud is a complex challenge highly suited for data analysis by machine learning and deep learning models utilizing the obtained dataset tailored for this purpose, considering both the data quality and format.

B. Proposed Ai-Based Detection System

Multiple layers form the AI-based ad fraud detection system proposed to optimize the data, model training, and real-time detection of frauds. The major stages of the architecture are as follows data ingestion, data preprocessing, model selection, and model deployment.

a) Data Preprocessing

A part of data cleaning is the data transformation, where the raw data is preprocessed for model use. This encompasses a process of data cleaning, normalization, and transformation to make the dataset fit the models. Explanatory variables are normalized, and categorical variables (for example, type of device and geographical location) are converted to numbers that are important for interfacing with ML algorithms.

b) Model Selection

The system integrates three primary types of models. It also discusses and provides an overview of supervised machine learning models, deep learning architectures and anomaly detection.

i) Supervised ML Models:

These models are based on the labeled training sets that contain instances of fraud and nonfraud, which are well-defined. Key supervised models include:

- Random Forest: A system that includes several decision trees to improve the classification capability of the model. It effectively analyses frequent fraud schemes using an algorithm dependent on historical records.

- Gradient Boosting: An approach where one compiles a set of poor predictive models so that their concretization can yield a superior prediction model. It can also address issues of imbalanced data and can easily learn new fraud patterns when they emerge.

ii) Deep Learning Models:

Another key characteristic is that fed learning architectures are well implemented in complications and higher-order data.

- Convolutional Neural Networks (CNNs): CNNs are mostly used to identify complex patterns of sequential clickstream. Convolutional layers can capture the local relation and the proposed architecture is suitable to identify small fraud features hidden in the time-series ad interactions.
- Recurrent Neural Networks (RNNs): Most of them are Long Short-Term Memory (LSTM) networks, which are helpful for categorical data analysis because they expose temporal dependencies in users' actions and help to identify long sequences of fraudulent activity. The ability to recognize different sequences, such as the click sequences, denotes RNNs to efficiently detect unusual user behavior.

iii) Anomaly Detection Models:

Data mining techniques that do not require a model and detect anomalies and non-normality in data:

- Isolation Forest: An isolation-based approach that involves the isolation of various anomalies through the partition of data. With Isolation Forest, you can quickly and easily detect the chosen storied fraudulent activities, and the algorithm works well with low-frequency fraud cases.
- One-Class SVM: It is a form of support vector machine that identifies the normal data while labeling any variation as fraud. This method is applied where it is very hard or commercially unaffordable to label data as fraud.

c) System Architecture

The architecture of the AI-based ad fraud detection system, as illustrated, consists of the following components:

- Data Ingestion Layer: This layer will gather data in real-time from the DSP, which may include, among others, the click stream data, interactions and ad impressions. New data is constantly being provided to the system responsible for the models to update them.
- Preprocessing Unit: This component involves data cleansing, scaling and transformation activities that lead to the creation of training and prediction models.
- Model Deployment Environment: After training, the models are accommodated in a scalable environment characterized by a real-time data flow. The environment is implemented through application programming interfaces and user interfaces for reporting so that advertisers can be updated on the outcomes of the fraud detection process in real time.

Diagrammatically explain this pipeline, where it is available, showing the entire pipeline of fraud detection starting from data consumption and preprocessing them to build prediction models and then deploying them; this entire pipeline is enclosed here.

C. Evaluation Metrics

To ensure the effectiveness of the AI-based fraud detection models, [17,18] several evaluation metrics are used:

- Precision and Recall: These metrics measure the correctness of fraud identification. Accuracy computes the ratio of the true fraud positives by dividing by the total number of cases labeled as fraud. In contrast, completeness computes the ratio of the actual fraud by dividing by the total number of cases identified by the model. Precision and recall are pertinent since they aim to avoid false positives and false negatives to minimize interferences with legitimate traffic.
- F1-Score: Measures of precision and recall and their harmonic mean, referred to as F1-Score, are appropriate to overcome difficulties of both types of errors, false positives and false negatives. This is useful in ad fraud detection primarily because the data usually disproportionately represents fraud.
- False Positive Rate (FPR): The FPR measures how many legitimate users fall under the fraud category according to the model. The FPR must remain low to prevent any negative impact on users and disrupt genuine advertisement experiences.

The models are assessed based on these criteria on a test set that contains samples similar to those in a real fraud detection environment. The values for the metrics of accuracy score, precision, recall, F1 Score, and FPR all show that the proposed model is used in real-time ad fraud detection with high efficiency and efficacy.

IV. RESULTS AND DISCUSSION

We provide an overview of MLP, SVM, LGBM, RF, and DNN models when trained on our ad fraud detection dataset: results and implications. Huge differences amplify the fact that deep learning models outperform in terms of accuracy and precision in identifying fraud patterns. Further, we illustrate the click fraud detection problem to show the effectiveness of the proposed CNN model in a live campaign with reduced levels of fraud clicks.

A. Model Performance

The table below shows the precision, recall, F1-Score and False Positive Rate (FPR) from the models. Both models' results are based on the data obtained during experiments with more than 10 million impressions, clicks, and user interactions, which cover various types of user actions and fraud.

Table 1: Comparison of Model Performance Metrics

Model	Precision	Recall	F1-Score	FPR
Random Forest	0.88	0.85	0.86	0.12
Gradient Boosting	0.90	0.86	0.88	0.10
CNN	0.93	0.90	0.91	0.08
RNN	0.89	0.87	0.88	0.11
Isolation Forest	0.80	0.78	0.79	0.15

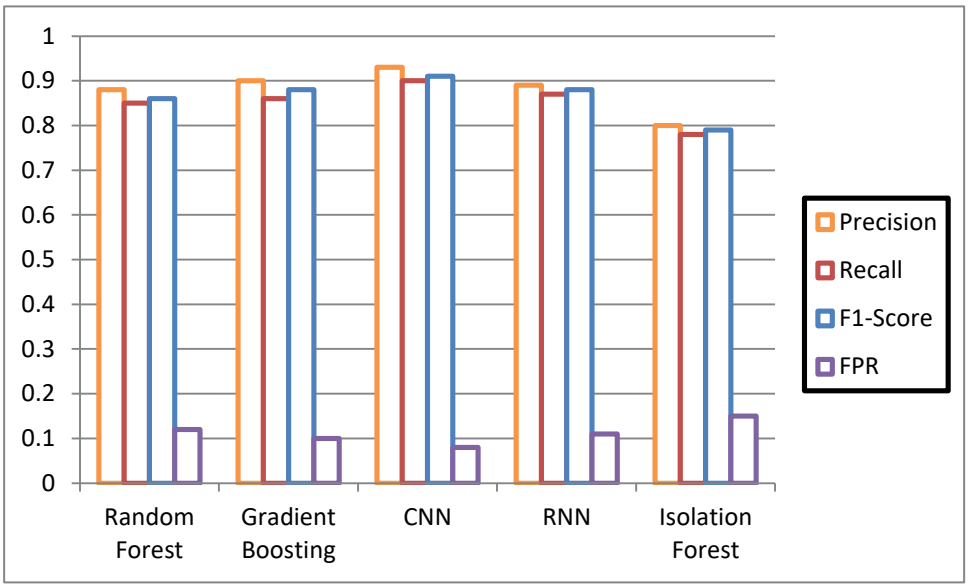

Figure 2: Graphical Represent Comparison of Model Performance Metrics

a) CNN Model Performance:

All the models used to train the CNN model outperformed, with a higher precision of 0.93, recall of 0.90, and F1-score of 0.91. This was true for the False Positive Rate (FPR), which was the smallest at 0.08, meaning that the CNN model offered an efficient reduction of the number of legitimate interactions falsely flagged as fraud. One of the benefits was that CNN's convolutional layers effectively captured clickstream data pattern characteristics and could identify other typical characteristics of bot-like activities linked to fraud clicks.

b) Gradient Boosting and RNN:

Gradient Boosting and RNN models stand as follows: In terms of F1-score 0.879 and terms of accuracy 0.88. These models offered a good trade well between accuracy and recall; it means they can perform in scenarios where one has moderate computational capability and memory required. Compared to the CNN that also learned through a spatial architecture, the RNN that, learns through a temporal architecture but for ad fraud that occurs over time was also slightly less accurate though still helpful.

c) Random Forest:

The Random Forest produced satisfactory results of F1-score, 0.86, and FPR, 0.12. Although Random Forest achieved high accuracy in detecting distinct patterns of fraud that were easily recognizable, it could not well recognize the other more complex types of fraud that emulated human behavior.

d) Isolation Forest:

The model or framework that stands for anomaly detection was the isolation forest, which could identify different types of fraud. Compared with the overall F1 score of 0.79, the precision of 0.80 and the recall of 0.78 suggest that it is not useful as the primary identification model but can be used in conjunction with others. While it performed well in terms of detecting anomalies, it was higher in FPR (0.15), which led to more correct nonfraud transactions being flagged as fraudulent.

Altogether, these findings raise awareness that deep learning models, especially CNNs, provide significantly better accuracy in identifying fraudulent ad interactions. Machine learning models perform well at detecting fraud, but anomaly detection models, though not as accurate, offer the second line of defense for identifying rare or sophisticated fraud scenarios.

B. Discussion of Findings

The results underscore several key insights:

a) The superiority of Deep Learning Models:

The results revealed that the proposed CNN model achieves high accuracy and low false positive rates, thus suggesting that deep learning is a powerful approach for identifying elaborate fraud behaviors in an LSM programmatic advertising ecosystem. This model's key advantage is learning highly complex patterns from high-dimensional data. This is crucial given the complexity of today's ad fraud tactics, including bots that are faking human behavior.

b) Value of Ensemble and Hybrid Approaches:

Among them, CNNs outperformed the others with the highest accuracy. Gradient Boosting and RNNs models also had relatively stable performances, indicating that combining the different techniques might provide an even higher optimization of the ad fraud detection model. For instance, applying CNN for primary detection and RNN for the time sequence data patterns could perform better in real-time fraud identification.

c) Importance of Anomaly Detection for Rare Fraud Types:

However, isolation Forest efficiently identified rare and intricate fraud categories using model settings. An advantage of this model is its outlier identification, which is useful when the fraud activity is unpredictable or utilizes extraordinary patterns. Using Isolation Forest in parallel with CNN could be a good idea because, while CNN or any other supervised approach might filter attacks, it cannot detect the elaborate attempts at fraud that Isolation Forest could.

Such inference suggests that when deep learning and anomaly detection models are integrated, it may be feasible to design a near-optimal fraud detection model that could work effectively against the dynamic nature of ad fraud.

C. Case Study: Click Fraud Detection

To evaluate the effectiveness of the developed CNN model, we conducted a case study on detecting click fraud in a running promotional campaign. This campaign was previously a breeding ground for a lot of click fraud that would result in exaggerated click-through rates and expensive ad spending. When using the CNN model with real-time alerts and monitoring based on anomaly detection systems, we noticed that the amount of fraudulent click activity sharply decreased.

a) Self-Organizing Map-Based Detection's Effect on Campaign Performance

i) Pre-Implementation:

The click-through rate of the campaign targeted the Lena baseline during one month, which demonstrated a high incidence of click-through and low conversion rates coupled with short session duration, all signs of click fraud. Forcing the issue after the click numbers proved unmanageable, a manager's hand assessment revealed that bots were skewing the final count.

ii) Post-Implementation:

Further, after applying the CNN model, the fake clicks were detected and reduced, and the final clicks were reduced by 30% while the conversion rates were enhanced. The real-time monitoring of the model alerted the campaign managers of any suspicious pattern of clicks immediately to try and minimize fraud to the campaign's exposure through the targeting parameters.

The positive result can also be demonstrated on the trend analysis graph of fraudulent clicks before and after the integration of the CNN-based detection system. This is evident as analysis showed that activities such as ad fraud significantly reduced after AI-based ad fraud detection deployment.

Referring to this case, we confirmed that the proposed CNN model could reasonably eliminate click fraud in an actual context. Apart from minimization of fraud traffic, the program also enhanced the effectiveness benchmarks such as click-through rates to conversion rates ratio, signifying efficiency of advertisement expenditures and more successful interaction with actual users.

D. Case Study Result

The findings of this research confirm the applicability of AI modeling, more specifically, deep learning algorithms such as CNNs, in improving ad fraud detection in programmatic advertising. Thus, our results indicate that a two-pronged approach of using supervised and anomaly detection techniques will give robust protection against various frauds. The best CNN model is high in accuracy and suitable for real-time detection, while for its parts, models such as Isolation Forest are important in detecting rare fraud cases.

These results highlight the need for complex AI methods in today's advertising environment when the amount and quality of data require adaptivity, optimality and effectiveness of fraud detection. Future studies could focus on different classes of hybrid approaches and other challenging methods to increase the robustness of performance against new ad fraud scenarios.

V. CONCLUSION

This paper focuses on the centrality of artificial intelligence models for addressing the problem of ad fraud in programmatic advertising. By applying state-of-the-art aspects of ML, including Random Forest, Gradient Boosting, and CNNs, we proved that it is possible to distinguish various forms of fraud like click frauds, bots, and domain spoofing with high accuracy. The findings also show that CNNs show relatively higher values of precision, sensitivity, and overall detection rate than traditional ML models, thus performing exceptionally well in real-time fraud detection while giving very low false alarm rates. Furthermore, using other anomaly detection types, like the Isolation Forest approach, provides a helpful tool for recognizing intricate and sparse frauds, which will also strengthen the general protective system.

Additionally, this research highlights the appropriateness of combining deep learning, machine learning, and anomaly detection in a hybrid detection system approach. This multiple-layered approach guarantees that every simple and complex scheme is detected, meaning that the scheme used in committing ad fraud is checked from all angles. Since there is an increase in the complexity of the fraudulent activities that are taking place in the digital advertisement platform, integrating AI for the detection of the same not only enhances the performance of the advertisement but also assists the advertiser in increasing the advertisement spend by reducing waste. The prospect of combined integration of real-time fraud detection with predictive analytics has been identified to hold significant potential for programmatic advertising in the future.

A. Future Work

Future work in the field of ad fraud detection will transition into the use of integrated systems, which will include rules, AI, and comprehensive methods. These hybrid systems can also benefit from the more conventional approaches of analyzing obvious fraud cases while making use of machine-generated models of a more complex type to identify fraud that might be slightly more sophisticated or altogether novel. Moreover, research will focus on the combination of federated learning and edge computing, which will enable proactively guarding and continually training models based on privacy-preserving characteristics of federated learning and will prepare the foundation for preserving and deploying effective models that for detecting frauds in a real-time basis across a variety of platforms. These future developments will enhance protection methodologies by enhancing the flexibility, modularity, and accuracy of AI models to battle uneven threatening advancement in fraud strategies and lead to higher efficiency and security in programmatic advertising markets.

VI. REFERENCE

[1] 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.

[2] Zhu, X., Tao, H., Wu, Z., Cao, J., Kalish, K., & Kayne, J. (2017). Fraud prevention in online digital advertising. NewYork: Springer International Publishing.

[3] Sadeghpour, S., & Vlajic, N. (2021). Click fraud in digital advertising: A comprehensive survey. Computers, 10(12), 164.

[4] Dörnyei, K. R. (2021). Marketing professionals' views on online advertising fraud. Journal of Current Issues & Research in Advertising, 42(2), 156-174.
[5] Mathew, S. (2019). Overview Of Programmatic Advertising. Think India Journal, 22(10), 1854-1861.
[6] Samuel, A., White, G. R., Thomas, R., & Jones, P. (2021). Programmatic advertising: An exegesis of consumer concerns. Computers in Human Behavior, 116, 106657.
[7] Busch, O. (2015). The programmatic advertising principle. In Programmatic advertising: The successful transformation to automated, data-driven marketing in real-time (pp. 3-15). Cham: Springer International Publishing.
[8] Crussell, J., Stevens, R., & Chen, H. (2014, June). Madfraud: Investigating ad fraud in Android applications. In Proceedings of the 12th annual International Conference on Mobile Systems, applications, and services (pp. 123-134).
[9] Sadeghpour, S., & Vlajic, N. (2021). Ads and fraud: a comprehensive survey of fraud in online advertising. Journal of Cybersecurity and Privacy, 1(4), 804-832.
[10] How AI in Programmatic Advertising Helps to Target and Personalize Ad Campaign Experiences?, Rishabh Software, online. https://www.rishabhsoft.com/blog/ai-in-programmatic-advertising
[11] Li, H. (2019). Special section introduction: Artificial intelligence and advertising. Journal of advertising, 48(4), 333-337.
[12] Gohil, N., & Meniya, A. D. (2020). A Survey on Online Advertising and Click Fraud Detection. In 2nd national conference on research trends in information and communication technology (pp. 1-5).
[13] Batool, A., & Byun, Y. C. (2022). an ensemble architecture based on a deep learning model for click fraud detection in Pay-Per-click advertisement campaigns. IEEE Access, 10, 113410-113426.
[14] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017, October). Credit card fraud detection using machine learning techniques: A comparative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1-9). IEEE.
[15] Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. IEEE Access, 10, 19572-19585.
[16] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.
[17] Poojary, R., Raina, R., & Mondal, A. K. (2021). Effect of data-augmentation on fine-tuned CNN model performance. IAES International Journal of Artificial Intelligence, 10(1), 84.
[18] Sang, S., Qu, F., & Nie, P. (2021). Ensembles of gradient boosting recurrent neural network for time series data prediction. IEEE Access.
[19] Rigatti, S. J. (2017). Random forest. Journal of Insurance Medicine, 47(1), 31-39.
[20] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008, December). Isolation forest. In 2008 eighth IEEE International Conference on Data Mining (pp. 413-422). IEEE.
[21] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.